Model-based Ubiquitous Service Architecture における利用権動的管理技術

伊藤誠悟 神戸雅一 上野正巳 瀧口浩義 小林透

今後，あらゆる場所で機器やサービスが利用できるユビキタスコンピューティング環境が整備されていくに従い，従来のように個人または組織が機器やサービスを所有するという概念に代わり，機器やサービスを利用する権利，すなわち利用権が必要に応じて動的に付与されるという概念が定着すると予想される．我々は上記のようなユビキタス環境実現に向けたアーキテクチャ Model-based Ubiquitous Service Architecture を提案している．本稿では MUSA における利用権条件記述方式について既存の標準アクセス制御記述言語である XACML (eXtensibleAccess Control Markup Language) とこれを基本とした条件判定モデルの適用時の問題点を明らかにし，利用権管理に向けた最適なモデルについて提案する．

Managing permission to use for computing and service resources on MUSA

Seigo ITO　Masakazu KANBE　Masami UENO　Hiroyoshi TAKIGUCHI　Toru KOBAYASHI

As ubiquitous computing technology (ex. services and resources can use everywhere) increasingly becomes a part of our daily life, we predict a change uses of services and resources from possession to utilization on demand. In this paper we present MUSA, a Model-based Ubiquitous Service Architecture system for managing and circulating permission to use. MUSA operates by dynamic decisioning and collecting permission to use information. We present results of verification that demonstrate the ability of MUSA's decision model to manage permission to use with eXtensible Access Control Markup Language (XACML)

1　はじめに

近年，Ubiquitous Computing [1]，Pervasive Computing, Nomadic Computing 等，様々なコンセプトの元に次世代の情報環境の構築に向けた研究が活発に行われている．例えば，Easy Living [2] (Microsoft)，Pervasive Computing [3] (IBM)，Cool Town [4](Hewlett-Packard)，FEEL (SONY)，OXYGEN [5] (MIT)，Sentient Computing[6] (AT&T)，STONE [7](東大)，Smart Space[8] (慶大)等，多くのプロジェクトが進行中であり，位置情報や環境情報などのセンサーの研究から様々なデバイス上でのサービス連携まで研究の対象は非常に多岐にわたっている．このような研究が実用化されるに従って，ネットワーク上に存在するあらゆるコンテンツやアプリケーションといったコンピューティング資源や実世界におけるモノがいつでもどこでも利用可能となりつつある．

NTT 情報流通プラットフォーム研究所
NTT Information Sharing Platform Laboratories

2　利用権管理技術

2.1　利用権管理技術の必要性

今後，誰もがさまざまな場所で，機器やサービス等のコンピューティング資源が利用可能となるユビキタス環境が実現されるに従い，従来のように個人または組織が機器やサービスに対する所有権を取得し利用するという概念に代わり，機器やサービスに対する利用権を必要に応じて取得し利用するという概念が定着すると我々は考える（図 1）．例えば，ユーザは出張先のビルに設置されている無線 LAN や公衆 PC 等の利用権を一時的に取得することにより，出張先でのコンピューティング資源の利用が可能となる．また，駅・空港において時間の余裕がある場合に，運行

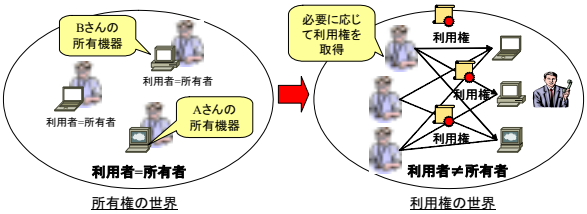

図1:所有から利用へのパラダイムシフト

チケットを保持するユーザには一時的にディスプレイやターミナルでの Web 閲覧を許可するといった利用シーンが考えられる．我々はこれを「所有から利用へのパラダイムシフト」と呼んでいる．これら利用権管理技術の試みとして昨年度，「利用権垂直統合システム[9]」について検討と試作を行い，コンピューティング資源の動的な利用を行う際の要件として「Join & Use，Exclusive Access Control」を明らかにしてきた．現在，我々は「所有から利用へのパラダイムシフト」への流れを起こすことを目的とし，Model-Based Ubiquitous Service Architecture [1013] (MUSA)を提案し検討を進めている．

2.2 既存の利用権利管理システム

ネットワーク上に存在するコンピューティング資源や，実世界における資源の利用権を流通させる利用権管理のための既存関連システムとして，Flex Ticket[11](NTT)や Light Holder[12](NEC)がある．これらのシステムは主に以下の機能を実現している．

- **一意性を持つ権利の管理基盤機能**
  一意性をもつ権利を　，権利定義情報や属性定義情報を付与して利用するための権利管理基盤機能．例えば「コンサート C 席のチケット」「動物園入場のためのチケット」等の特定の意味を持つ権利を定義し管理･利用する．
- **携帯デバイスによる権利流通機能**
  IC カードや携帯電話などに電子的な権利を格納し，ユーザが権利を持ち歩き，さまざま場所で権利を行使できる機能．

これら既存の利用権管理システムが提供する機能に加えて，我々は次の機能を想定している．

- **環境やユーザの状態に応じた権利**
  利用権管理プラットフォームにより発行された権利が，行使される際の環境情報，ユーザ情報，その他デバイスの情報の変化に応じて，利用可能な権利の範囲が動的に変化し，それらを制御する機能．例えば新幹線の自由席の利用権を例に考えると「自由席の利用権は，乗車率が 100%以下の場合，当該新幹線の自由席に乗車することが出来るが，100%以上の場合は当該車両に乗車することは出来ず，他の列車で利用権を行使しなければならない．」という例となる．この利用権は権利が行使される際のプロファイルや環境情報の状態に応じて，ユーザが許可される行為が変わる．この例では新幹線の乗車率の状態に応じて利用権の行使可否が変化している．
- **利用権の組み合わせ**
  必要に応じて個別の利用権を取得しそれらを組み合わせることによるアドホックな連携サービス機能．例えば「一時的に出張先の会議室を利用する場合に，会議室の利用という利用権には，備え付け計算機利用のための利用権，プロジェクタの利用権，プリンタの利用権といったそれぞれのモノを利用するための利用権や，会議室の利用履歴参照，会議室のストレージサービス，会議室の無線 LAN 利用といったそれぞれのサービスを利用するための利用権が含まれている．」といった利用権の水平統合の例がある．
- **ユビキタス資源の管理**
  ネットワーク，コンテンツ，アプリケーションといったコンピューティング資源に関する利用権管理だけではなく，実際の物理的なモノやヒトとのインタラクション方式や検知方式を含めた，ユビキタス資源管理のための共通フレームワーク機能

このような機能を想定して，現在我々が開発しているシステム，MUSA について説明する．

2.3 MUSA

MUSA [13] (Model-based Ubiquitous Service Architecture)とは，ユーザ，コンピューティング資源，モノ，その他環境情報等のプロファイル情報の状態に応じて，資源利用権の行使判定を動的に行い，権利を管理する，利用権管理のためのアーキテクチャである．MUSA では Web サービス，コンテンツ，アプリケーション，ネットワークといった従来のコンピューティング資源利用権管理だけではなく，RFID 等を活用し実世界のモノ，ヒトも含めたユビキタス環境における利用権管理も想定している． MUSA は汎用的な利用権管理のためのアーキテクチャであるため権利を管理するあらゆる場面で利用することができる．図 2 は MUSA が対象とする利用権管理の概要図である．図 2 においてユーザはネットワーク，コン

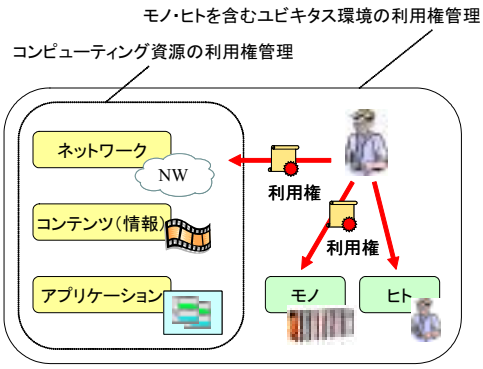

図2：MUSAが対象とする利用権管理

テンツ，アプリケーションといったコンピューティング資源，モノ等の利用を行う場合は必要に応じて利用権を取得する．例えばモノの利用権を行使する際には，機器に埋め込まれた認証用のセキュア IC チップによる機器プロファイル情報，ユーザの正当性を保証する IC カードによるユーザプロファイル情報，その他環境情報，それぞれを利用し機器認証，ユーザ認証，利用権行使判定を行う．

MUSA における利用権行使判定モデルを表したものが図 3 である．利用権の中の利用権条件部の条件情報に従い利用権の行使時に，動的に利用判定を行う．MUSA において 2.2 節の要求条件機能を実現する際の課題として以下のものが挙げられる．

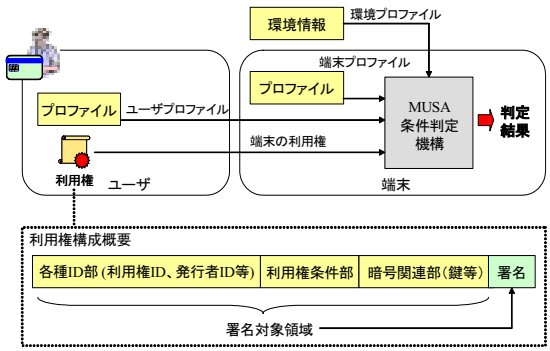

図3：利用権行使モデルと利用権構成図

- 利用条件記述方式
  利用条件（利用権）に関する統一的な記述方式．
- 利用条件判定方式
  あらゆる場所において利用権が行使される可能性のある利用権管理システムにおける利用条件判定方式．
- モノ管理方式
  利用権が行使されるモノについて，モノとのインタラクションや，実際のモノの探知方式を含めたモノ管理方式．

上記課題のうち，本稿では「利用条件記述方式」「利用条件判定方式」を対象とする．モノ管理方式については，RFID 技術用の適用を想定する．

3　利用権管理における利用条件記述

我々は利用権の利用条件判定のための枠組みとして，アクセス制御記述の標準仕様である eXtensible Access Control Markup Language (XACML)適用を想定している．XACML は 2003 年 2 月に標準化団体 OASYS の標準として勧告されており，図 4 のように既存標準技術と非常に深い関係がある．また，XACML は複雑な条件判断を容易に実現でき拡張性も高い．例えば，通常 OS などが提供しているアクセス制御ではユーザやグループに対して読み・書き・実行の許可・不許可程度の制御のみであるのに対し XACML では条件判定に用いる要素の指定や，要素の値を比較する演算方法，対象動作などをポリシとして記述し指定することが出来る．このため MUSA のようにプロファイルの状態に応じてさまざまな条件判定を行う枠組みに非常に適しているため XACML を採用した．利用権に関する条件判定部を XACML で記述した場合の例を図 5 に示す．

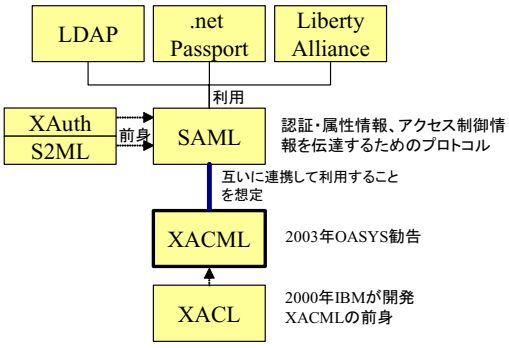

図4：XACMLと関連技術

他の代表的な権利記述関連の枠組みとしては IETF で標準化されている VTS[14]（Voucher Trading System）がある．VTS では個々の価値流通システム独自のプロトコルを隠蔽して統一した API を定義し，主に GVL （Generic Voucher Language）による権利自身の情報の記述方式と権利流通のプロトコルについて深く検討されている．しかし，MUSA のようなプロファイルベースによる利用権条件判定を行う場合，条件判定式

をポリシとして容易に記述できる XACML がより妥当であると考えたため今回は XACML を用いた.

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:pflab:scdrm:xacml:policy:test:T001"
        RuleCombiningAlgId="urn:oasis:xacml:1.0:rule-combining-algorithm:deny-overrides">
 <Description>利用権の記述例</Description>
 <Target>
  <Subject>対象主体の指定</Subject>
  <Resource>対象資源の指定</Resource>
  <Action>対象動作の指定</Action>
 </Target>                                              利用権の対象を指定
 <Condition>動作主体・対象資源・対象動作以外の環境情報等の条件記述</Condition>
 <Rule RuleId="urn:pflab:xacml:test:0001:rule" Effect="Permit">
  <Target>ルール1に関する動作主体・対象資源・対象動作の指定</Target>
  ・・・（ルール1に関する判定ロジック・対象要素・演算方法等の指定）・・・・・
 </Rule>                                                利用権に関する条件判定のロジックを指定
 <Rule RuleId="urn:pflab:xacml:test:0002:rule" Effect="Deny">
  <Target>ルール2に関する動作主体・対象資源・対象動作の指定</Target>
  ・・・・・（ルール1に関する判定ロジック・対象要素・演算方法等の指定）・・・・・
 </Rule>
</Policy>
```

図5：XACMLによる利用権記述

3.1 XACML の概要

XACML [15] [16] (eXtensible Access Control Markup Language)とは，ネットワーク上の多様な資源に対する柔軟で拡張性のあるポリシ記述仕様等を定めたXMLタグセットである. XACMLのモデルは以下の動作主体より構成される.

- PDP (Policy Decision Point)
  定められたポリシに従い，示されたアクセス要求が正しい権限を持つものかを判断をし，アクセス要求に対する許可不許可を判断する主体
- PEP (Policy Enforcement Point)
  アクセス要求者からのアクセス要求を受けてPDP に対象リソースへのアクセス判断を依頼し，PDP が判定した結果に応じてアクセス制御を実行する主体
- PAP (Policy Administration Point)
  リソースに対するポリシやポリシセットを生成し PDP へ提供する主体
- PIP (Policy Information Point)
  リソースやリクエスト主体等に関する属性情報を提供する主体

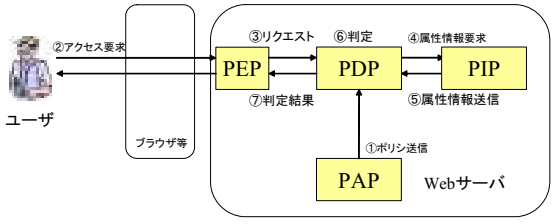

図6:Web文書におけるXACMLアクセス制御フロー

これらの動作主体の基本動作のデータフローが図 6 である．XACML の基本的な枠組みを，我々が想定している利用権流通へ適用した場合にはいくつかの課題がある．XACML が想定しているアクセス制御モデルでは，主に Web サーバ上の資源に対するアクセス制御を目的としており，アクセス制御を行うサーバとアクセス要求を行うクライアントが明確に分かれているモデルである．クライアントはユーザ情報等のプロファイル情報をユーザから取得し，サーバ上に存在する資源への要求をプロファイル情報とともにリクエスト文として送信する．サーバ側ではクライアントより受信したリクエスト文と自身が保持するポリシ文を評価し判定結果を返信する.

4 利用権流通における利用権条件判定方式と課題

我々が想定する利用権管理システムは，どこでもユーザが移動する先々で，コテンツ・アプリケーションといったコンピューティング資源，サービス，ネットワーク，モノを利用できるユビキタス環境を想定しており，利用権条件判定はサーバ上だけとは限らずあらゆるローカル端末上で行われる．ある程度正当性が保証されているサーバと違い全てのローカル端末上での条件判定は危険である．このように利用権管理システムにおいては，端末・サーバ問わずあらゆる場所で利用権条件判定を行うので，条件判定のための環境情報や個人情報等のプロファイル情報が端末等へ抽出されるのはプライバシー保護上好ましくない.

4.1 利用権管理の条件判定アーキテクチャ

4.1.1 条件判定アーキテクチャの要件

図 6 に示した従来アーキテクチャの場合，サーバ上で条件判定を行うためサーバもしくは端末へプロファイル情報等を送信する必要がある．前述の課題を考慮すると，利用権管理における利用権条件判定は，ユーザや端末に関するプロファイル情報を扱うので，不必要な主体へ情報を提供することなく，ユーザが保持する耐タンパ領域で条件判定等の処理を行うことが望ましい．利用権管理においてユーザはさまざまな場所に移動して，移動した先々でローカルまたはオンラインで利用権を行使する．このため可搬性が高くハードウェア耐タンパ機能を持つICカードやMOPSS[17]カード等の中に利用権条件判定用のモジュールを配置した利用権条件判定モデルを提案する.

4.1.2 提案モデル

図 7 は IC-Chip 上で利用権条件判定を行うモデルの概要図である．基本アイデアは簡潔なものであり「利用権条件判定のための要素情報は必要のない場合は，基本的に耐タンパ領域の外部へ出さない」というものである．図 7 では Rights Management Point (RMP) 機構を追加している．RMP はそれぞれの耐タンパ領域で判断しなければいけない条件を解析し，判断されるべき場所へリクエストをディスパッチする．その後，各 RMP より返信された判断結果を統合し最終的な条件判定を行う機構である．基本フローは以下のようになる．

① ユーザは固有 AP（PEP）からリクエストを RMP へ送信する．
② RMP はユーザのカード内で判断するべき条件についてはカード内での判断を PDP へ依頼する．
③ RMP は他の耐タンパ領域で判断される条件については他の RMP へディスパッチし，返信される判定結果を統合する．
④ 全ての RMP の判定結果により最終的な利用条件判定結果を PEP に返信する．

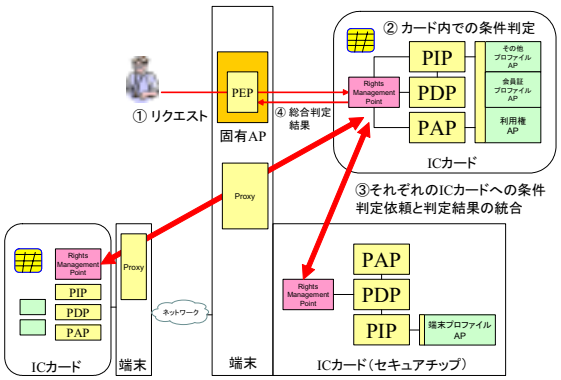

図7 利用権管理における条件判定アーキテクチャ

このように端末へ要素情報を抽出せず，ハードウェア耐タンパ装置内にて必要な処理を完結させ処理結果のみを耐タンパデバイスより返信するという構成の既存システムとしては「指紋認証の処理を IC カード内で行い照合判定結果のみを返信するシステム[18]」「セキュアマルチメディアカード[19]（ケータイ de ミュージックサービス用コンテンツ格納ハードウェア）」などが存在しているが，利用権管理の観点から行っているものは知られていない．

4.1.3 利用権条件判定モデル

提案モデルを含む既存利用権条件判定モデルを以下に示す．モデルとしては，どの主体が利用権の条件判定を行うかにより分類を行い，「サーバ判定モデル」「端末判定モデル」「IC-Chip 判定モデル」の 3 種類のモデルに分類することが出来る．

- モデル 1：サーバ判定モデル

ユーザが保持する IC カードからユーザに関するプロファイル情報，機器から機器に関するプロファイル情報を取得し，ネットワークを介してサーバ側に送信する．各主体より送信されたプロファイル情報と利用権の条件情報を元にサーバ側で利用権の条件判定を行い，利用権の行使可否判断を行うモデル．（図 8）．

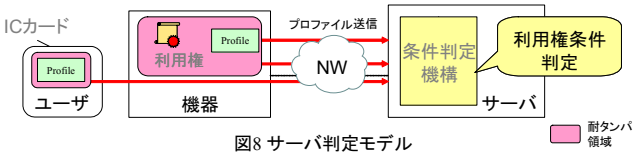

図8 サーバ判定モデル

- モデル 2：端末判定モデル

ユーザのプロファイル情報 ，機器のプロファイル情報を IC カードと機器からそれぞれ取得し，サービスを実行する端末上に送信する．サービスを実行する端末上で，利用権の情報を基に利用権の条件判定を行い，利用権の行使可否判断を行うモデル．（図 9）

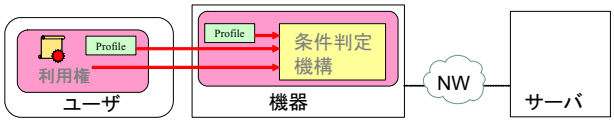

図9 端末判定モデル

- モデル 3：IC-Chip 判定モデル

条件判定のためのユーザのプロファイル情報や機器のプロファイル情報は端末・サーバ上に送信せず，プロファイルを保持するそれぞれ主体上で条件判定を行う．各主体間では条件判定結果のみの通信を行い，判定結果を統合し利用権の行使可否判断を行うモデル．（図 10）

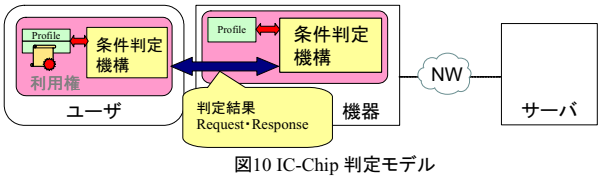

図10 IC-Chip 判定モデル

5　評価

5.1　利用権条件判定モデルの比較

4.1.3 節にて分類をおこなったサーバで利用権条件判定を行うモデル 1（図 8），端末で条件判定を行うモデル 2（図 9），IC-Chip 上で条件判定を行うモデル 3（図 10）に対して比較評価を行った（図 11）．オンラインでの利用権条件判定はどのモデルでも行うことが可能である．オフラインにおける条件判定についてはモデル 1 では条件判定を全てサーバで担っているため行うことが出来ない．条件判定の処理速度性能と実行メモリ容量に関してはモデル 1 モデル 2 が PC 上で行うのに対しモデル 3 では IC-Chip 上で行うため他のモデルより性能面で劣る．プロファイル情報の保護に関してモデル 3 は利用権条件判定のための要素情報を外部へ出さない．このためプロファイル保護に関して有効である．

表11 : 各モデルの比較

	モデル1 (図6) サーバ判定モデル	モデル2 (図9) 端末判定モデル	モデル3(図7) IC-Chip判定モデル
オンライン条件判定	○	○	○
オフライン条件判定	×	○	○
条件判定の処理速度性能	○	○	△
実行メモリ容量	○	○	△
プロファイル保護	△	△	○
適用領域	一元判定	エリア判定	個別判定
現段階での実現性	○	○	△

5.2　利用権管理のためのモジュール

XACML 関連の実装として現在利用可能なモジュールは，Sun Microsystems による Sun's XACML Implementation[20]と Jiffy Software が提供する Jiffy XACML[21]がある．しかし，これらの実装はともに PDP の部分しか実装されておらず，PIP，PAP 他の部分に関しては提供されていない．これらの PDP に対してポリシとリクエストを与えて条件判定を行わせた場合，判定結果としては「Permit（許可），Deny（不許可），NotApplicable（適用ルールなし），Indeterminate（不確定）」のいずれかが選択される．Web におけるアクセス制御の場合は，この 4 つの判定結果により表示・非表示，実行許可，不許可等のみを行えばよい．しかし，利用権管理においては，Deny 判定の場合でも，どんな理由で不許可であり，次にどういう行動を起こせば許可になるか，ユーザに示すことがユーザ支援の観点から重要である．このようなことを考慮した場合 XACML パーサが持つ解析結果の意味情報を提示することが必要である．

6　まとめ

本稿では，利用権流通における利用権条件判定方式についての既存モデルとの比較・検討を行い，現在の実装状況について述べた．今後の予定として，IC カード上の条件判定機構について，ハードウェア的制約等を考慮しながら図 10 のモデルの実装を行う予定である．

参考文献

[1] Mark Weiser. "The Computer for the 21st Century", Scientific American 265(3):94-104, September 1991.
[2] Easy Living : http://research.microsoft.com/easyliving/
[3] IBM Pervasive Computing : http://www-3.ibm.com/software/pervasive/
[4] Cool Town : http://cooltown.hp.com/cooltownhome/
[5] MIT Project OXYGEN : http://oxygen.lcs.mit.edu/
[6] Sentient Computing Project : http://www.uk.research.att.com/spirit/
[7] Service Synthesizer on the Net(STONE) : http://www.mlab.t.u-tokyo.ac.jp/
[8] Smart Space Lab : http://www.ht.sfc.keio.ac.jp/SSLab/
[9] 伊藤誠悟，神戸雅一，直井邦彰「モデルベースユビキタスサービスアーキテクチャにおける資源利用権管理方式」電子情報通信学会，全国大会, D9-13 , March. 2003.
[10] 神戸雅一，伊藤誠悟，直井邦彰，小林透.「コンピューティング資源の利用権管理方法についての検討」電子情報通信学会技術研究報告, KBSE2002-23, December. 2002.
[11] Flex Ticket : http://info.isl.ntt.co.jp/flexticket/
[12] Light Holder : http://www.sw.nec.co.jp/cced/lightholder/
[13] 庭野栄一，神戸雅一，瀧野修，山本修一郎.「MUSA : モデルベースユビキタスサービスアーキテクチャ」電子情報通信学会技術研究報告, KBSE2001-74, March. 2001.
[14] Voucher Trading System (VTS) : http://www.faqs.org/rfcs/rfc3506.html
[15] eXtensible Access Control Markup Language (XACML) http://www.oasis-open.org/
[16] 工藤道治，羽田知史.「拡張可能アクセス制御ポリシー記述言語:XACML」暗号と情報セキュリティシンポジウム, SCIS2003 12B-2, January. 2003.
[17] Mobile Passport (MOPASS) : http://www.mopass.info/
[18] IC カードと指紋認証技術を組み合わせた認証システム http://www.nttdata.co.jp/release/2001/0308.html
[19] ケータイ de ミュージック : http://www.keitaide-music.org/
[20] Sun's XACML Implementation : http://sunxacml.sourceforge.net/
[21] Jiffy XACML : http://www.jiffysoftware.com/