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

2005－MBL－32（9）
2005－UBI－　7（9）
2005／3／17

サービス利用判定におけるプライバシー漏洩を防ぐ判定方式

上野 正巳† 末田 欣子† 八木 哲† 瀧口 浩義† 北見 広和† 小林 透†

†NTT 情報流通プラットフォーム研究所 〒180-8585 東京都武蔵野市緑町 3-9-11

E-mail: †{ueno.masami, sueda.yoshiko, yagi.satoshi, takiguchi.hiroyoshi, kitami.hirokazu, kobayashi.toru}@lab.ntt.co.jp

あらまし 個人のコンピューティング環境を出先のユビキタス資源を組み合せて簡単かつ安全に実現するユビキタス環境ローミングのコンセプトを紹介し、それを実現する機能のうち、ユビキタス・コンピューティング環境で提供される種々の資源の利用可否を判定する際に，プライバシー情報漏えいを防ぎつつ，高速に判定を行う方式を提案する。そしてその方式を実装した評価システムに基づき評価した結果を報告する。

キーワード プライバシー，保護，ユビキタス，条件判定

Privacy protected judgment method in ubiquitous service use

Masami UENO† Yoshiko SUEDA† Satoshi YAGI† Hiroyoshi TAKIGUCHI† Hirokazu KITAMI† and Toru KOBAYASHI†

†NTT Information Sharing Platform Laboratories 3-9-11 Midori-cho, Musashino-shi, Tokyo, 180-8585 Japan

E-mail: †{ ueno.masami, sueda.yoshiko, yagi.satoshi, takiguchi.hiroyoshi, kitami.hirokazu, kobayashi.toru }@lab.ntt.co.jp

Abstract: We introduce the concept of the Personal Network Environmental roaming which realizes personal computing environment simply and safely combining external computing resources. Personal network environmental roaming consists of many functions. We pay our attention to the function to judge the use propriety of the various resources offered in a ubiquitous computing environment among those functions, and we propose the method which judges at high speed, and it preventing a privacy information leak. And we report the evaluation system which used the method.

Keyword: Privacy protection, Ubiquitous Computing, and Condition judging

1. はじめに

ADSL や光回線の普及と、無線 LAN アクセスポイントの普及により、PC を持ち歩いていれば出先の環境で職場や家庭の機器にアクセスし、利用できる状況になりつつある。利用者が所有する PC を持ち歩いていれば、比較的柔軟にそのような種々のサービスを利用可能であるが、各々のサービスを利用するためには、そのサービスに応じた設定が必要であったり専用のソフトウェアが必要であったりと専門的な知識が必要である。一方、例えばネットカフェ等に設置された共用の端末を利用する場合には比較的専門知識は必要としないが、セキュリティ面の配慮のために自由にアプリケーションを起動できない等、制限が設けられ、安全かつ容易に職場や家庭の機器にアクセスすることは難しい。

今後様々な機器にコンピューティング資源が与えられるようになったとしても、それぞれのサービスを使いこなすためには現在のように専門知識が必要なままであれば、ユビキタス・コンピューティング環境も一般の人々に利用されず、普及は難しい。

本稿ではこれらの問題を解消するために、どこにいても誰でも簡単にその場の資源と遠隔の資源を組み合

せて利用可能にする「ユビキタス環境ローミング」のコンセプトを提示し、それを実現する技術のうち個別資源の利用判定における問題点の明確化と、解決方法の検討を行い、実際に動作するプロトタイプを作成しその評価を報告する。

2. ユビキタス環境ローミング

2.1. コンセプト

我々が想定する「ユビキタス環境ローミング」とは、利用者個人が普段家庭やオフィスで利用している自分のコンピューティング環境を、どこに行ってもその場にある資源を一時的に利用して再構築する事が出来る事が基本コンセプトになっている。図 1に、この基本コンセプトを示した。

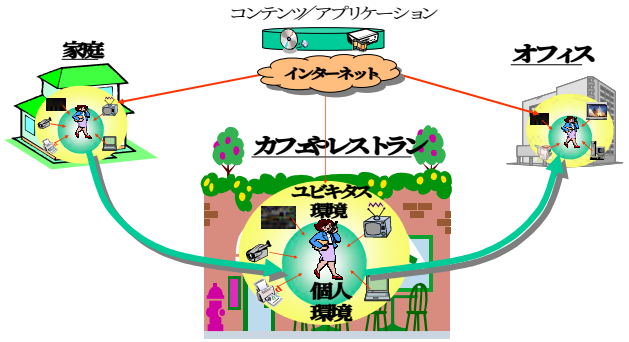

図 1 ユビキタス環境ローミングのイメージ

このようなコンセプトを実現するために、我々は次のような特徴を実現するべきものとして設定した。

（1）安全であること

まず、利用者にとって安全であること。サービスを利用するためにプライバシーや個人情報が漏洩しないという点。

そして、もう一つはサービス提供者にとっても安全にサービスを提供できるということ。これは利用者とサービス提供機器の双方が相手の認証や、サービス品質の確認を行うことが出来ること。

（2）パーソナルな環境

利用者毎に異なる家庭やオフィスのコンピューティング環境を、どこに行っても再現できるように、利用者が居る場所にある機器と組み合せて利用できること。

（3）簡単な操作

モバイル環境におけるサービスの遠隔利用は既にいろいろな分野で実現されているが、利用するためには専門的な知識が必要である。そこで、統一的かつ簡便なユーザ・インターフェースを提供し、専門知識を持たない利用者でも簡単に複数のサービスや機器を組み合せて利用できること。

2.2. アクターと信頼モデル

コンセプトを実現するために、登場するアクターとアクター間の信頼モデルについて整理した。外出先等で提供される資源を利用するためには、まず利用者と、個々の資源をサービスとして提供するサービス提供者（以下 SP と略記）が必要になる。更にユビキタス環境ローミングの仕組みを提供するプラットフォーム事業者が必要になる。

プラットフォーム（以下 PF）提供事業者：ユビキタス環境ローミングを実現する。プラットフォームに関る通信方式、データ定義、共通機能を保証する。サービス提供事業者及び利用者に対してシステム内で有効な鍵と証明書と PF を配布する。

サービス提供事業者（以下 SP）：各種サービスを提供する。PF 提供事業者に登録し、利用者にサービス（資源）を提供する。

利用者：PF 提供事業者に登録することで、SP の提供する様々なサービスを利用し、ユビキタス環境ローミングサービスを受けられる。サービスの提供形態によっては SP にも登録を行う場合がある。

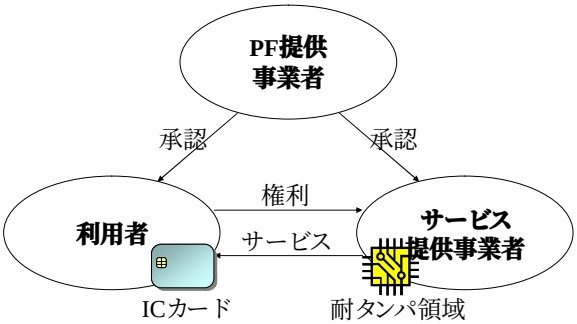

図 2 アクターとその関係

3. 利用判定方式の提案

ユビキタス環境ローミングを実現するためには、複数のユビキタス資源を組み合せて利用する必要がある。ユビキタス資源を利用する際の基本的な機能要素としては、

（1）資源を検知する機能

（2）資源の検索・選択する機能

（3）資源利用可否の判定を行う機能

（4）資源の利用を制御する機能

が必要である。本稿ではこれらのうち（3）資源利用可否の判定を行う機能を中心に論じる。

3.1. 三つの判定処理

ユビキタス環境ローミングでは、資源を組み合せて利用する前提があるために、資源を利用する際の判定として、以下に示す三階層の判定を行う必要がある。

（1） 個別の資源に対する利用可否の判定

個別の資源をその利用者が利用可能か、それぞれの資源のポリシーに応じて、利用者属性、資源属性の双方を見て判定を行う。

（2） 複数資源の組み合せ可否判定

資源どうしを組み合せようとしたときに、その組合せが可能であるかどうかを判定する。具体的には該当する資源が取り扱うことの出来る、プロトコルやデータフォーマット、サーバ／中継／クライアント等の種別により、適合性を判断する。

（3） 利用開始可能判定

例えば、サーバ資源がネットワーク資源を経由してクライアント資源まで接続すればサービスを開始できるが、どれかが欠けた状態ではサービスを開始できない。このように、サービスが開始可能な組み合せに達しているかどうかの判定を行う。

3.2. 個別資源の利用可否判定法

3.2.1. 集中判定法

3.1で示した３つの判定処理のうち、個別資源の利用可否を判定する部分に関して、我々は資源に対する利用権というものを設定し、判定するというアプローチで研究を行ってきた。本稿でも、この個別資源の利用可否判定の部分に焦点を当てて検討を行う。

(1) MUSA

我々はユビキタス環境における資源の利用可否を判定する仕組みとして、MUSA(Model based Ubiquitous Service Architecture)の検討を行ってきた[1][2][3]。MUSA では、利用者が所持する IC カードの中に利用者の属性や、サービスの提供を受けるためのポリシーが XACML[4]で記述された「利用権」が格納されている。このポリシーには利用者に対する条件に加え、利用するサービスや装置に関する条件も記載されている。またサービスを提供する機器の中のセキュア領域にその機器の属性が格納されており、判定処理はポリシーが記述された利用権と双方の属性情報を、サービス提供を行うサーバに集め、そこで判定を行うという「集中判定型モデル」を採っていた。このため、あるポリシーに対して、利用者はサービスに対する条件を設定でき、ＳＰは利用者に対する条件を設定できる。双方に対する条件を判定した上で、サービスを提供する事で、双方が安心してサービスの提供／利用を行う事が出来る。

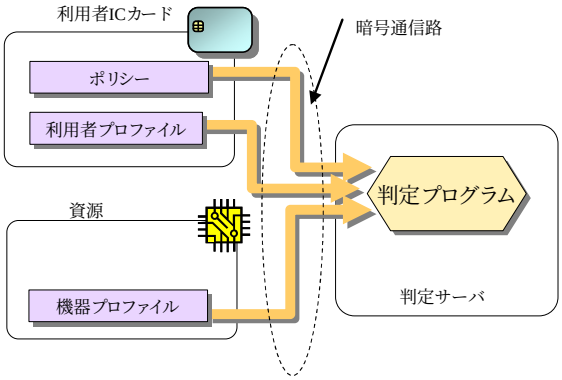

図 3 集中判定モデル

しかし、図 3に示すような集中判定型モデルでは利用者や機器の属性情報といった外部に漏れて欲しくない情報を外部のサーバに集中させるために、IC カードや機器のセキュア領域と、判定を行うサーバの間を暗号通信路で結ぶ必要があった。汎用のアクセスポリシ

ー記述言語である XACML を用いたため、サービス提供の判定を行うに当たって複合的で柔軟な条件判定はできるようになったものの、IC カードなどの処理能力の低いデバイスでの暗号処理が負荷となり、速度的に高い性能は出せなかった。

②集中判定法の問題点

「ユビキタス環境ローミング」を実現するに当たって、3章冒頭で示した（3）の資源利用可否を判定する部分の高速化が必要と考え、MUSA で検討した判定方式を高速化するために現状の分析を行った。集中判定型モデルでは、IC カードと判定を行うサーバとの間で、ポリシーや属性情報をやり取りする際に、相互認証を行った上で暗号通信路を形成して通信を行っている。集中判定型モデルでの判定処理において処理時間の内訳を測定したところ、暗号通信路形成に関する部分が大部分を占め、処理能力の低いＩＣカード上での暗号処理を減らす必要があることが分かった。

次いで、通信データ量に応じて変化するデータ通信時間が大きく、データ量自体も削減する必要があることが分かった。

3.2.2. 分散判定法

（1）条件判定の物理的な分散

ここで、資源利用のために設定されるポリシーのなかに設定される条件を分類すると、以下の３つのものに分類できる。

(ア) 利用者条件： サービスの提供者が利用者に対して設ける条件。利用者の属性情報を元に判定される。例えば利用者の年齢や性別。

(イ) 提供者条件： サービスの利用者が提供者や、提供するサービスに対して設ける条件。サービスを提供する資源内の属性情報にて判定される。例えば、カラー印刷可能など。

(ウ) 環境条件： 上記以外の環境の情報によって判定される条件。例えば現在の時刻など。

それぞれの条件は対応する属性の定義されている場所で判定すれば、属性情報を外部に漏らさずに判定が可能になる。そこで、図 4に示すように利用者の属性情報が格納されている IC カードや資源の属性が格納されている耐タンパエリア内に判定プログラムを導入し、資源利用のためのポリシーのうち、利用者条件は利用者の IC カード内で判定し、提供者条件は資源内の耐タンパエリア内で判定し、環境条件は仲介装置内で判定を行う、分散判定モデルを採用した。各耐タンパエリア内で判定された結果は判定保証書として仲介装置である UAG に集められ、総合的な判定を行う。この場合、プライバシー情報である属性情報はそれぞれの耐タンパエリアから出ないために、判定保証書の改ざん対策だけを行えばよく、暗号通信路を作成する必要がなくなる。

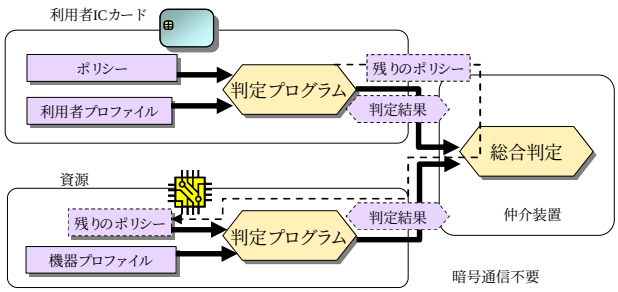

図 4 分散判定モデル

（2）条件判定の時間的な分散

更に、資源利用に関するポリシーのライフサイクルを検討すると、サービスを利用する前に、ポリシーを購入するなど、IC カードにダウンロードするタイミングがある。従来はサービスを利用する際に IC カード内の利用者属性情報を利用した判定も行っていた。しかし、利用者の属性情報は容易には変化しないので、この判定をポリシーの購入／ダウンロード時に事前に行い判定保証書（証明書）の形で作成しておく事で、サービス利用時の判定処理を減らす事が出来る。利用時判定と、購入時判定のフローの違いを図 5に示す。

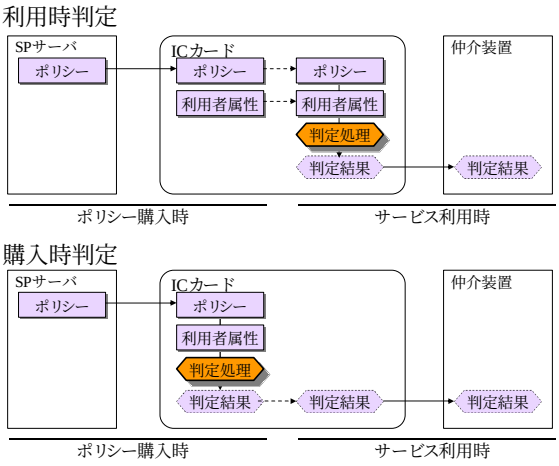

図 5 利用時判定と購入時判定

この方法をとった場合には、判定後に利用者の属性情報が変化する場合があるために、判定保証書に適切な有効期限を設定したり、属性に関するオペレーションが行われた場合に、判定保証書の作り直しを行う等の対応が必要になる。

3.2.3. 条件記述の圧縮による判定の高速化

MUSA ではXACML を用いて資源の利用ポリシーを定義していた。XACML は XML ベースであるため、可読で柔軟な条件記述が可能である。反面、3.2.1でも述べたようにテキストデータであるためにデータ量が大きくなってしまうデメリットがある。分散判定モデルでは、このポリシーも IC カードと判定サーバとの間でやりとりしていたために、大量のデータ通信が発生していた。本システムでは、ポリシー記述のベースを XACML としながらも、XACML の関数およびパラメータを符号化し記述を逆ポーランド記法を用いてバイナリ化を行い圧縮した。IC カード内の条件判定には、この圧縮したデータを解釈して判定結果を出力する処理を実装した。

4. 試作システムの概要

ここまで述べた資源の利用条件判定を実装し、試作システムを作成し、評価を行った。

4.1. 試作システムの構成

システムは、利用者の操作を受け持つ操作端末、する複数の資源に加え、あるエリア内の資源を管理し、利用条件判定の仲介を行う装置として UAG (Ubiquitous Area Gateway) を設けた。

（1） 操作端末： 利用者を認証するための属性情報やサービスのポリシーが格納された IC カードを読み書きする IC カード通信アプリケーションを内蔵している。また、サービスの組合せ利用を行うための操作を行う操作アプリケーションを内蔵する。また UAG との連携を行うためにプラットフォーム機能を内蔵している。

（2） IC カード： カード内に、利用者の属性情報を管理する機能、サービスのポリシーが記述された利用権を管理する機能、ポリシーを判定する機能、判定結果を受け渡す機能等を持つ。

（3） UAG： プラットフォーム機能として、環境条件の判定機能、資源と操作端末のポリシー判定の仲介機能と総合判定の機能、資源の状態管理機能、資源の起動制御の機能等を持つ。

（4） 資源：サービスを提供する機能、プラットフォーム機能として、UAG と連携し内蔵する耐タンパエリアのアプリケーションと通信する機能を持つ。耐タンパエリアのアプリケーションとしては、資源の属性管理、ポリシーを受け取り提供条件の判定を行う機能を持つ。

装置及び機能の構成を図 6に示す。

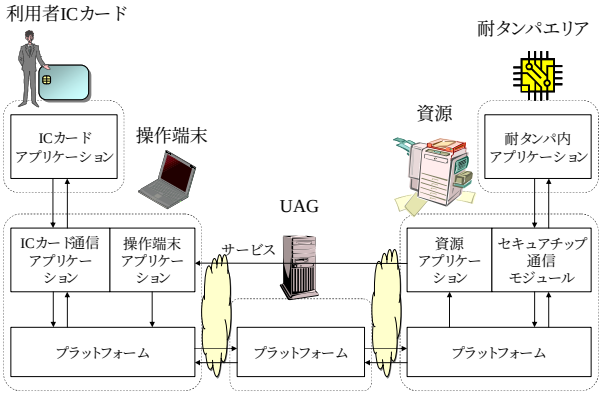

図 6 装置構成および機能構成

4.2. セキュリティポリシー

試作システムでは、高速化の観点から不用な暗号化通信は行わない方針を採った。このため次のようにポ

リシーを設定し、セキュリティの設計を行った。

(1) 不正利用が防止できること

IC カード内の権利が不当に増減されないこと、または権利内に規定されたサービスポリシーに適合した判定結果が正しく得られること。

(2)プライバシー保護

利用者のプライバシー情報である属性情報が不当な第三者に漏洩しないこと。

5. 評価

5.1. セキュリティ評価

(1)不正利用防止

権利を消費し減数する処理について、評価システムでは乱数を含んだ署名の生成と検証によって命令の送信者を認証し不正な増減を防いでいる。また、条件判定に関わるポリシーや判定結果の情報については、発信元を認証した上で署名を作成・検証することで改竄となりすましを防止し、ポリシーにそった条件判定が行われることを担保している。

(2) プライバシー保護

評価システムでは利用者のプライバシー情報は利用者の IC カード等の耐タンパ装置に格納されたあとは外に出ることがないため、耐タンパを破られない限りはプライバシー情報が直接漏洩することはない。

5.2. 性能評価

分散判定モデルを用いた評価システムでは、判定処理を物理的に分散し、更に時間的にも分散させて、利用者がサービスを利用する利用権行使のタイミングでの処理量を減らすことができた。更に、判定処理を分散させ、プライバシー情報を耐タンパエリアから出さずに判定が行えるようにしたことで各アクター間の通信に暗号化通信を行わなくて済むようになった。これらによって、利用権行使のタイミングで必要とする処理の時間を大幅に削減でき、一般の Web アクセスと同レベルの感覚で利用できる速度を達成できた。

6. あとがき

本稿ではユビキタス環境ローミングのコンセプトを提示し、これを実現する機能のうち、資源の利用可否を判定する方式において、物理的、時間的に処理を分散させるとこで、効率的に利用権行使の判定が行えることを示した。

物理的に判定を分散させるために、元々一つであったポリシーも分割させたが、ポリシーによっては複数の場所に格納されている属性情報同士の比較などの演算が必要になる場合があり、このような場合には対応できていない。また、本モデルでは属性情報が真に分散している状況を想定しているために、分散した情報をいかに正しく管理していくかという課題も今後検討する必要がある。

文　献

[1] 神戸雅一，伊藤誠吾，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”，信学技報,KBSE2002-23 ,December.2002.

[2] 神戸雅一，上野正巳，伊藤誠吾，瀧口浩義，小林透，近藤好次，“IC カードを用いた利用権管理手法の考察”，信学技報, KBSE2003-48, pp.13-18, March.2004.

[3] 上野，神戸，伊藤，瀧口，小林，近藤，“属性情報を用いた利用権管理手法のコンテンツ利用制御への適用”信学技報, KBSE2003-49, pp.19-24, March.2004.

[4] OASIS eXtensible Access Control Markup Language (XACML) TC http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml