研究計画書
無線タグのプライバシ保護機構に関する研究

慶應義塾大学環境情報学部　学籍番号 70057323

自署：_____

平成 15 年 10 月 16 日

概要

近年、RFID をはじめとする個体識別技術により、本や洋服などの非計算機を含めたオブジェクトを、ネットワークを介して管理する試みがなされている。特に RFID 技術により、オブジェクトに固有の ID を割り振り、持ち物の管理などオブジェクトを管理できるようになる。しかし、ID を読み取ることで製品の種類がわかるだけでなく、洋服のサイズや趣味・嗜好に関するプライバシが第三者に漏洩する危険性がある。

本研究は、RFID 技術によりオブジェクトの管理が行われるようになった際に、私的なオブジェクトの情報の第三者への漏洩を防止することを目的とする。まず、現状の RFID のオブジェクト管理技術の問題点を整理する。その上で、RFID 技術におけるプライバシ問題を解決するためのモデルとして、RFID タグを暗号化・隠蔽し、プライバシの漏洩を防止するモデルを提案する。さらに、システムの設計・構築を行う。

1　はじめに

近年、RFID(Radio Frequency IDentification) をはじめとした個体識別技術を用いることで、コンピュータだけでなく非計算機を含めた全てのオブジェクトをネットワークを介して管理する技術が実現されようとしている。これにより、ネットワークを介してのオブジェクトの位置情報などの状態が取得可能となる。本研究では、オブジェクトを ID により個体識別可能な物体、と定義する。

流通においては、オブジェクトの位置情報や属性を管理することで、個々のオブジェクトの位置情報を把握でき、在庫管理・貨物配送を効率化できる。しかし、現在のコンピュータは「自分のまわりに何があるのか、それはどのような状態にあるのか」など、周囲の物の存在や状態を「感知する」ことはできない。RFID とセンサを用いれば、コンピュータは自分の周囲の情報を収集・管理・処理できるようになる。非計算機に RFID タグを貼付することにより、端末が計算機であることを前提とするインターネット上で非計算機を扱えるようになる。

RFID 技術を用いて流通を管理する手法として、AIDC (Automatic Identification and Data Capture) がある。AIDC には、RFID タグ自体がオブジェクトの情報を保持するものと、RFID タグは ID のみを保持し、オブジェクトの情報は ID と関連づけられ、ネットワーク上に保持するものに分類できる。プライバシの漏洩防止をする際、前者の場合は暗号化や認証機能付きの高機能な RFID タグを用いることにより実現できるが、後者はネットワーク上にある情報のアクセス制御を伴うため、技術的に困難である。具体的には、タグの読み取りの認証だけでなく、ネットワーク上のサーバの認証や安全な通信路の確保など、考慮すべき点が多くなる。

オブジェクトの情報をネットワーク上に保持するものの例として、MIT(マサチューセッツ工科大学) や慶應義塾大学が中心となって研究開発を行っている Auto-ID Center[1] が注目を集めている。Auto-ID Center では RFID 技術をバーコードに代わるオブジェクト認識技術として位置づけ、製品の製造・流通・在庫管理・販売・決済に至るまでを一貫して管理することを目指している。

Auto-ID Center のアーキテクチャでは、全てのオブジェクトに固有の ID を割り振った RFID タグを取り付けて識別するため、製造から流通、小売に至るまでだけでなく、家庭内などさまざまな状況でオブジェクトを一元的に管理できる。これにより、自分の買った商品が、「いつどこで作られ、どのような流通経路をたどってきたのか」といった情報が容易に取得できる可能性を提供する。

また、鞄の中や自分の部屋などの私的な空間において、RFID 技術を用いて所有物を管理することにより、所有している本などの情報を、いつどこにいても管理できる。例えば、自分の部屋に存在する本の情報を参照することにより、書店において「どの本を購入するか」の判断の指標にできる。

しかし、さまざまな製品に RFID タグを貼付することで、私的な所有物に関する情報が第三者に取得される恐れがある。誰がどのような製品を所有しているかという情報から、個人の趣味嗜好が推測できてしまい、プライバシの点から問題となる。

2　研究目的

現在の Auto-ID Center で提案されているシステムモデルをはじめ、既存の RFID 技術の多くは、リーダを持っていれば誰でも RFID タグの情報を取得できてしまう。RFID タグの ID が漏洩することにより、RFID タグの ID だけでなく、RFID タグの ID と関連づけられたオブジェクトの情報までもが、第三者に容易に取得されてしまう。

現在の Auto-ID システムでは SCM(Supply Chain Management) での利用を中心に考慮されており、小売店以降 (家庭) での利用をあまり考慮していない。本研究では、RFID タグの ID とそれに関連づけられた情報をプライバシと定義し、所有者が自分のオブジェクトを管理することに焦点を当て、プライバシの漏洩を防止することを目的とする。

本研究では、RFID 技術を用いる際のプライバシの漏洩を防止するための技術的な問題を整理し、システムモデルを提案する。それらに基づき、プロトタイプを設計し、構築する。

図 1: Auto-ID システムのアーキテクチャ概要図

図 2: 本研究で想定する利用環境

3 Auto-ID Center

本章では、現在 Auto-ID Center で提案されているシステムモデル (Auto-ID システムと呼ぶ) について述べる。

現在提案されている Auto-ID システムの概要を図 1 に示す。Auto-ID システムは EPC(Electronic Product Code)[2] タグ、EPC リーダ、Savant[3]、ONS(Object Name Service) Server[4]、PML(Physical Markup Language) Server[5][6] によって構成される。それぞれについて、以下に詳述する。

- **EPC タグ、EPC リーダ**
  オブジェクトに EPC タグという RFID タグを取り付け、それを EPC リーダを通じて自動的に検出する。
- **Savant**
  Savant は、検出された EPC および、その EPC の PML をもとにしたサービスを提供する。EPC をもとにオブジェクトの属性を得る際には、ONS Server に対して PML Server の IP アドレスを問い合わせる。その IP アドレスをもとに、PML Server から PML を取得し、オブジェクトの属性情報を得る。
- **ONS Server**
  ONS Server は、EPC を受け取ると、EPC と対応する PML Server の IP アドレスに変換する。
- **PML Server**
  PML Server は、EPC の属性を保持するコンテンツサーバである。Savant からの要求に対し、EPC に対応する PML を送信する。

Auto-ID システムではオブジェクトの識別子として、EPC を用いる。EPC には、全体で 64 ビット・96 ビット・256 ビットの 3 種類のコード体系があり、3 種類とも 4 つのコード部分に分けられる。先頭から順番に、Header(ヘッダ)、EPC Manager(ベンダコード)、Object Class(製品コード)、Serial Number となっている。

EPC はオブジェクトの ID のみを表現する。そこで、EPC と関連づけて、オブジェクトの属性を管理する機構が必要になる。オブジェクトの属性とは、製造年月日・流通経路・位置情報など、様々なサービスに必要になる情報である。このようなオブジェクトの属性を記述するための言語が PML である。PML を用いることで、オブジェクトの状態に応じた柔軟な属性の記述が可能となる。

4 本研究で想定する利用環境

本章では本研究で想定する利用環境について述べる。本研究では、全てのオブジェクトに、工場出荷の状態で EPC が取り付けられていることを前提とする。そして流通の過程や、その後の家庭での使用に際し EPC を用いて管理することを想定する。

図 2 では工場や、運送業者、商店ではリーダを用いて EPC から個体 ID を取得可能であり、在庫管理や流通管理に EPC を用いている。そして、家庭では購入後のオブジェクトの管理に EPC を用いている。購入後のオブジェクトの管理には家庭内のリーダだけでなく、例えば駅や店頭など、公共の場にあるリーダの利用も想定する。

4.1 要求事項

以上を踏まえ、以下の視点から Auto-ID システムを家庭で利用する際のオブジェクトのプライバシ漏洩防止システムの要求事項を洗い出す。

- **オブジェクトの取得**
  オブジェクトが店頭に並んでいるときや、店の倉庫にあるときは、店がオブジェクトの管理のためにオブジェクトの ID を取得できる必要がある。しかし、客が店でオブジェクトを購入すると、オブジェクトの所有者が店側から客側に移る。一度オブジェクトが客のものになれば、そのオブジェクトの ID が店側に取得できる必要はなく、オブジェクトの ID は客だけが取得できれば良い。そのためには、オブジェクトのオーナを設定し、オーナ以外の人のオブジェクトの ID の取得を禁止する必要がある。
- **オブジェクトの管理**
  オブジェクトの位置情報や状態を、ネットワーク経由で取得できる。しかし、この情報は所有者以外の第三者から取得されてはならない。
- **オブジェクトの放棄**
  オブジェクトは、最終的には廃棄物として処理される。廃棄したオブジェクトの ID をリーダで読み取られることにより、個人の持ち物などから生活内容や趣味嗜好が漏洩しないようにしなければならない。そのためには、オブジェクトを廃棄する際、オーナが ID を破棄できるようにしなければならない。

4.2 現在の Auto-ID システムの問題点

以上の要求事項を踏まえ、現在の Auto-ID システムには以下の 3 点が問題点として挙げられる。

- 第三者による EPC の読み取りによる個人情報の漏洩
- EPC を容易に推測可能
- EPC をもとにオブジェクトの情報を取得可能

現在の Auto-ID システムには所有権の概念がないため、EPC リーダを持つだけで、誰でもオブジェクトの ID を取

得できるようになる。EPC は製品名だけでなく、個々のオブジェクトの識別子を保持するため、第三者に EPC を読み取られると、そのオブジェクトの持ち主のプライバシが漏洩する可能性は高い。例えば、鞄をリーダで読み取ると、鞄の ID だけでなく、鞄の中に入っている全てのオブジェクトの ID を取得できる。結果、鞄の中に何が入っているのかという情報が、第三者に漏洩してしまう可能性がある。

さらに、EPC は、EPC Manager、Object Class、Serial Number で構成されているため、特定のメーカの製品の EPC がわかると、その EPC をもとに他のオブジェクトの製品名やメーカ名を推測できる。

5 既存研究

本章では、RFID 技術においてプライバシの漏洩を防止する既存技術について述べる。

5.1 RFID のセキュリティとプライバシ

Auto-ID Center が提案する技術に、RFID のセキュリティに関するものがある [7]。この技術は、RFID においてセキュリティを守るための技術として、単一方向ハッシュを用いるというものである。これは、RFID タグの ID を書き換えられるという前提で、EPC をロックすることにより、リーダから RFID タグの読み取りを制限するというものである。RFID タグは自身がロックされると、リーダに対し EPC を応答しない。RFID タグが公開されているときは、誰でもその RFID タグの情報を読み取り可能である。

RFID タグをロックするためには、所有者は任意の鍵のハッシュ値を計算し、ハッシュキーとして RFID タグに書き込む。RFID タグの情報を読み取るためには、リーダが RFID タグに鍵を送信する必要がある。RFID タグはそれをハッシュし、RFID タグ内に保存されているデータと比較し、合致した場合のみ RFID タグ情報を提供する。

この手法の問題点して以下の 2 点が挙げられる。

- リーダが鍵を管理するため、オブジェクトの所有者が変わっても、同じリーダを用いることにより、第三者に RFID タグの情報を取得される恐れがある。
- 無線通信を用いて、RFID タグとリーダが認証を行うため、通信を傍受することにより、第三者に RFID タグの情報を取得される恐れがある。

5.2 EPC の暗号化・隠蔽

現在、EPC の暗号化には以下のようなものが提案されている [8]。

- **Anonymous EPC**
  Anonymous EPC は、EPC の Object Class と Serial Number の代わりに、信頼された証明書会社によって提供されるランダムコードを使用する。これにより第三者から EPC を隠蔽できる。
- **Encrypted EPC**
  Encrypted EPC では、EPC が暗号化される。EPC 内に公開鍵を持ち、認証済みクライアントから要求があると、サーバに登録されている秘密鍵を用いて復号化する。Anonymous EPC との違いは、翻訳用のデータベースを持つ必要がないことである。

これらの提案は EPC の隠蔽・暗号化手法のみの提案であり、これらを実現するためのアーキテクチャは提案されていない。また、所有権の概念が存在しないため、所有権の移譲が発生した際に、以前のオーナが ID やオブジェクトの情報を取得できてしまう可能性がある。

6 問題点解決へのアプローチ

本章では、問題点解決をする際に考えられるアプローチをについて述べ、本研究で用いる問題点解決へのアプローチについて述べる。

6.1 考えられるアプローチ

EPC の読み取りによる第三者へのプライバシの漏洩を防止する方法として、以下の 2 通りのものが考えられる。

- PML サーバでのアクセス制御
- EPC の暗号化

前者の PML サーバでのアクセス制御とは、PML サーバに対してオブジェクトの情報を取得する際にオーナの認証を行い、認証されていないオーナに対してはオブジェクトの情報を提供しない、というものである。しかし、EPC の構造は変わらないため、EPC からオブジェクトの EPC Manager、や Object Class を判別・推測できてしまう恐れがある。

後者の EPC の暗号化とは、EPC を暗号化し、認証されたオーナ以外は復号化できなくするというものである。暗号化された EPC は、ONS サーバに問い合わせてもエントリが存在しないため、PML サーバの IP アドレスを取得できず、オブジェクトの情報を取得することができない。認証されたオーナのみ、復号化された EPC を取得でき、オブジェクトの情報を取得できる。これにより、第三者の EPC の読み取りによるプライバシの漏洩を防止できる。

6.2 本研究でのアプローチ

本研究では、第三者へのプライバシ漏洩問題解決へのアプローチとして、EPC を暗号化する。さらに、全ての暗号化や認証の機能を管理するために、EPC Authentication Server(EPCAS と呼ぶ) という認証サーバを用意する。EPCAS ではオーナの認証、EPC の復号化、オーナの管理、鍵の管理を行う。EPCAS でオーナ認証されたオーナのみが復号化された EPC を取得できる。これにより、例えば公共の場所にあるリーダを用いても、オーナは自分の持ち物のは認識できる。

6.3 機能要件

本研究を進める上で、以下の機能が機能要件として挙げられる。それぞれについて以下に詳述する。

EPC の暗号化・隠蔽:
第三者からの EPC の読み取りによるプライバシの漏洩を防止するため、EPC を暗号化する。オブジェクトに貼付された EPC は工場出荷時には暗号化されておらず、所有者が任意の時点で自分の秘密鍵を用いて暗号化できるようにする。

前章で述べた様に、既存の RFID タグの暗号化に関する研究は、ID の隠蔽・暗号化手法のみの提案であり、これらを実現するためのアーキテクチャは提案されていない。本研究で提案するアーキテクチャを利用することにより、これらの隠蔽、暗号化手法が実現可能となる。

安全な通信:
復号化後の EPC を傍受されることを防止するため、SSL や IPsec などを用いて安全な通信路を確保する。

図 3: 本研究で提案するシステムアーキテクチャ概要図

鍵管理:

リーダで鍵の管理を行った場合、オブジェクトのオーナが更新しても、リーダの中に鍵が残存する。そのため、オーナ変更後に第三者が同じリーダを用いることにより、第三者に EPC の情報を取得されてしまう可能性がある。これを防止するため、認証を行うサーバ上で秘密鍵を管理する必要がある。

また、Encrypted EPC を使用する際、秘密鍵をネットワーク上に流すことは安全性の点から望ましくない。そのため、認証サーバ上で復号化を行うことが必要である。

オーナ管理・認証:

オブジェクトは商品として市場に流通するため、その所有者は変遷する。所有者が変わる際に、以前の所有者がそのオブジェクトの情報にアクセスすることを制限する必要がある。そのため、オブジェクトに付加属性として、現在の所有者を示す「オーナ」を 1 人設定する。オーナ属性を 1 つだけに限定し、オーナの認証を行うことにより、オーナ以外の人からのアクセスを制限する。

オブジェクトの所有者が複数に存在する場合は、オーナ属性に特定の個人ではなくグループを指定することにより、対応可能である。また、プライバシを保護する必要のないオブジェクトや情報を公開したいオブジェクトは、オーナを設定しないことにより、第三者からのアクセスを可能とする。

6.4 システムアーキテクチャ

図 3 に、本研究で提案するシステムアーキテクチャを示す。現在の Auto-ID システムのシステムモデルに加える変更点を、以下に詳述する。

- **Savant**
  本研究では、Savant 上に、暗号化された EPC を受け取った際、認証サーバに対してオーナ認証、および EPC の復号化を要求する機能を実現する。現在の Savant は、暗号化された EPC を受け取った際、その EPC を正しく処理することができない。また、Savant はリーダとインターネットを介さずに、シリアルケーブルなどで直接接続されており、一般的には使用する人を特定できる。Savant に使用者を特定する情報 (OwnerID) を入力することにより、認証サーバに自動的に送信する。
- **EPCAS**
  本研究では、認証サーバとして EPCAS を追加する。EPCAS は Savant から認証要求があった際に、オーナ認証を行う。オーナの認証がされると、EPCAS は EPC の復号化を行い、暗号化された伝送路を用いて、Savant に送信する。
- **Owner Management Client**
  Owner Management Client はオーナの変更が生じた際に、EPC のオーナ情報を登録、更新するためのものである。オーナの変更は、そのオブジェクトのオーナのみが実行可能で、第三者による不正なオーナ変更を防止する。第三者によるオーナ情報改竄を防止するため、オーナ情報の更新の際にはオーナ認証を行う。
- **Key Registry Client**
  Key Registry Client は ID を暗号化する際に、秘密鍵を登録するためのものである。オーナが鍵を変更し ID を暗号化しなおす際や、オーナの変更が生じた際にも、Key Registry Client による鍵の登録が必要となる。

図 4: 認証サーバ上のモジュール相関図

6.5 動作概要

図 4 は、本研究で提案する EPCAS のモジュール相関図である。それぞれのモジュールの動作について、処理の流れを詳述する。

認証・復号化:

Savant から EPCAS へのオーナ認証・EPC 復号化要求を処理するのが、オーナ認証モジュールと EPC 復号化モジュールである。

オーナ認証モジュールは (1)Savant からの認証要求を受け取ると、(2) オーナ管理データベースに対して EPC に対応するオーナ情報を要求する。(3) オーナ管理データベースから受け取ったオーナ ID と、Savant からのオーナ ID が一致すると、(4)EPC 復号化モジュールに処理が移る。EPC 復号化モジュールは、(5)Savant から受け取った EPC をもとに (6) 鍵管理データベースから秘密鍵を受け取り、復号化し、(7)Savant に送信する。

オーナ登録・更新:

EPC のオーナ情報に変更が生じた際、Owner Management Client は EPCAS に、登録・更新を要求する。

オーナ登録モジュールは、(a)Owner Management Client からの登録・更新要求をオーナ登録モジュールが受け取ると、(b) 受け取った EPC と OwnerID を、オーナ情報管理データベースに登録・更新する。

鍵登録・更新:

EPC Manager が、工場出荷時にオブジェクトに EPC タグをつける際には ID は暗号化されていない。オーナが商品を購入後、暗号化する際に EPCAS に秘密鍵を登録す

る必要があるが、その際に鍵登録モジュールを使用する。

また、オーナが鍵を変更し暗号化する際や、オーナの変更時に新しいオーナが暗号化する際にも秘密鍵の登録が必要となり、同様に鍵登録モジュールを使用する。

鍵登録モジュールは、(I)Key Registry Client からの鍵登録要求を受け取ると、(II) 受け取った EPC と Key を、鍵情報管理データベースに登録・更新する。

6.6 Auto-ID システムとの相違点と共存性

本研究では、全ての EPC を隠蔽または暗号化し、Auto-ID システムに、認証サーバとして EPCAS を追加する。また、認証サーバに対応するように Savant に変更を加える。さらに、認証サーバに対し、オーナの登録・更新を行う Owner Management Client と、EPC Manager が秘密鍵を登録・更新する Key Registry Client を追加する。ONS Server・PML Server・EPC リーダには全く変更を加えることなく、本研究で提案するモデルを実現できる。

6.7 考慮すべき点

膨大な数の EPC が世の中に存在するため、世界中の EPC の認証を、1 台の認証サーバで行うことはできない。世界中の Savant からの認証要求をどのようにして分散させるのか、システムのスケーラビリティについて、検討しなければならない。

EPC の中に、認証サーバを指定する ID を埋め込むことによって、負荷分散を実現する手法が考えられる。また、家庭内に認証サーバを設置し、オーナ (もしくはグループ) ごとに使用する認証サーバを分けることにより、負荷分散を実現することも考えられる。

しかし、1 台の認証サーバでどの程度の RFID タグの情報を管理できるのか、評価実験を行う必要がある。そのため、スケーラビリティに関しては、評価実験の後に設計を見直すことで対応する。

7 研究の進め方

Auto-ID Center Japan は、慶應義塾大学 SFC 研究所内に設立される。本研究ではこの研究基盤を利用し、システムの設計、実装、評価を行う。

8 期待される成果

本研究の成果として、まず Auto-ID Center に対する本システムの提案を行う。暗号化された EPC が本研究で提案するシステムには必要であるので、暗号化 EPC の仕様を作成し、併せて Auto-ID Center に対して提案を行う。さらに EPCAS・Owner Management Client・Key Registry Client の実装、および、Savant を EPCAS へ対応させるための実装を行う。これにより Auto-ID システムで用いられる RFID のプライバシが保護される。

9 これまでの研究活動

私は学部 2 年次より慶應義塾大学村井研究室に所属し、多くの先端技術にふれながらネットワークに関する研究活動を行ってきた。

RFID タグを用いて人の位置情報の履歴を記録し、それをもとにテレビ電話を開始やメールの送信をするアプリケーションを作成した (研究実績 1)。学部 3 年次には、無線 LAN 基地局の混雑状況を視覚的に地図に表示するアプリケーション (AP Monitor) を作成した (研究実績 2)。

その中で私は位置情報をネットワーク上で扱うことに興味を持ち、RFID タグを用いて検出した位置情報をもとに、自動的にインスタントメッセンジャのスクリーンネームを決定するシステムを作成した。このシステムは DICOMO2003 シンポジウム [9] のデモセッションにてデモンストレーションを行った (研究実績 3)。

また、同時に WIDE プロジェクト [10] の icars ワーキンググループ (現 SPEARS ワーキンググループ) に参加してきた。この活動を通じ、4 回にわたる WIDE 合宿における実証実験に携わり、実空間ネットワーキングの実証実験システムの構築に参加し、2003 年 9 月には RFID タグの暗号化の実験を行った (研究実績 4)。

10 政策・メディア研究科に進学を希望する理由

現在 Auto-ID Center が提唱するモデルは、SCM を中心にターゲットとしている。また、このモデルはプライバシの漏洩の危険性があるため、家庭への応用は難しい。本研究なくしては、Auto-ID システムの家庭への応用はできない。本研究を進めていく上で、SFC にある Auto-ID Center Japan と共同研究をしていくことは必要不可欠である。

また、政策・メディア研究科では技術のみならず、実際のビジネスや法整備を見据えた研究活動を行っている。RFID タグのプライバシ漏洩防止を推進する際に、技術開発のみならず、法整備による規制も必要になってくる。

さらに、慶應義塾大学は WIDE プロジェクトへ積極的に参加している。WIDE プロジェクトは、Auto-ID Center をはじめ多くの対外プロジェクトを推進しており、技術開発だけでなく、その応用や運用、標準化を見据えた研究がなされている。

このように政策・メディア研究科は、私の研究を進める上で必要な環境が全て整っている。以上の理由から、私は政策・メディア研究科への入学を強く希望する。

参考文献

[1] Auto-ID Center, http://www.autoidcenter.org/, 2003/10/01

[2] David L. Brock,“ The Electronic Product Code (EPC) A Naming Scheme For Physical Objects ”, 2001/1/1

[3] Oat Systems, MIT AutoID Center, “ The Savant - Version 0.1 (Alpha) Oat Systems & MIT Auto-ID Center ”, 2002/2/1/

[4] Oat Systems, MIT AutoID Center, “ The Object Name Service - Version 0.5 (Beta) Oat Systems & MIT Auto-ID Center ”, 2002/2/1

[5] David L. Brock, “ The Physical Markup Language - A Universal Language for Physical Objects”, 2001/2/1

[6] Mark Harrison, Duncan McFarlane, “ Development of a Prototype PML Server for an Auto-ID Enabled Robotic Manufacturing Environment ”, 2003/2/1

[7] Sanjay E. Sarma, Stephen A. Weis, Daniel W. Engels, “ RFID Systems, Security & Privacy Implications ”, 2002/11/1

[8] 日経 BP IT Pro 記事, “ Anonymous EPC, Encrypted EPC ”, http://itpro.nikkeibp.co.jp/free/NBY/NEWS/20030425/2/, 2003/04/25

[9] **成瀬大亮**, “ 階層的位置情報を用いた位置情報広告機構 ”, DICOMO2003 シンポジウム デモンストレーション, http://www.dicomo.org/

[10] WIDE Project, http://www.wide.ad.jp/, 2003/10/01