

Internet Week 2003
IP Meeting 2003 パネルディスカッション
配布資料 2003年12月4日

インターネットにおける IDとトレーサビリティ

独立行政法人産業技術総合研究所
グリッド研究センター セキュアプログラミングチーム

高木 浩光

<http://staff.aist.go.jp/takagi.hiromitsu/>

追跡可能性の用途

- 食品トレーサビリティ
 - 消費者が、生産者を知る
- サプライチェーンマネジメント (SCM)
 - 生産、流通、小売が商品を追跡する
- カスタマーリレーションシップマネジメント (CRM)
 - 小売が消費者の購買動向を追跡する
- 廃棄物リサイクル
 - 生産者、廃棄物処理業者がマテリアルを追跡する
- 犯罪捜査
 - 法執行機関による追跡および開示請求

匿名性と顕名性

- 表現の匿名性
 - 言論・表現活動における著者・演者等を秘匿する
 - デフォルト: 非匿名
 - インターネットがもたらした変化
 - 匿名での表現が容易に
- 存在の匿名性
 - 消費活動において消費者名を明らかにしない
 - デフォルト: 匿名
 - インターネットがもたらした変化
 - 消費行動が非匿名(顕名)化
 - 技術的必然性によって結果的に
 - マーケティング手法のIT活用による進化によって

インターネットの発展と変化

年代	生活との関わり	IPアドレス
1994年 ごろまで	表現の場	固定(組織)
1998年 ごろまで	表現の場	固定(組織) ダイヤルアップ(家庭)
2001年 ごろまで	表現の場 消費生活の場	固定(組織) ダイヤルアップ(家庭)
～現在	表現の場 消費生活の場	固定(組織) 固定(家庭) +ダイヤルアップ

将来像は？

～現在	表現の場 消費生活の場	固定(組織) 固定(家庭) <small>+ダイヤルアップ</small>
-----	----------------	--

将来 A	表現の場 消費生活の場	固定(組織) 固定(家庭)
------	----------------	------------------

A: 存在の顕名化により消費生活の場としての利用が衰退？

将来 B	表現の場 消費生活の場	固定(組織) 流動的(家庭)
------	----------------	-------------------

B: 存在の匿名性の確保により消費生活の場としてさらに発展

固定IDすなわち共通ID

- cookieのドメイン独立性と第三者cookie
 - cookieはドメイン毎に名前空間が独立(設計による)
 - 第三者cookieとは
 - インライン画像等へのアクセスで発行されるcookie
 - HTMLと異なるドメインに置かれた画像へのリンク
 - サイト横断的なcookie発行の多用
 - バナー広告会社が、閲覧者に無期限IDを発行
- 広範なドメインにまたがった第三者cookie
 - 「共通ID」化
 - 大半のドメインに共通のユーザ識別番号
- 固定IPアドレス(からのアクセス) = 共通ID
 - 時間的にも空間的にも固定のID

共通ID化の回避

- 共通IDの回避はグローバルスタンダード
 - P3P導入によるcookieの設計改善
 - (コンパクトプライバシーポリシー提示のない) 第三者cookieのデフォルト拒否化
 - Internet Explorer 6, Netscape 7
 - IPv6 に対する RFC 3041 の導入
 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6
 - Windows Media PlayerのプレイヤーID拒否可能化
 - 「一意のプレイヤーIDをコンテンツのプロバイダに送信する」設定
 - Pentium IIIのPSN (Processor Serial Number) の中止
 - Liberty Alliance の “Federated ID”
 - 住基台帳法による住民票コードの民間利用の禁止

到達性と追跡性

- 到達性のあるIDだけがプライバシー情報 ではない
 - 到達性のあるID
 - 電話番号, 住所, メールアドレス, IPアドレス
 - ID主が連絡をもらうためのID (情報を返信してもらうためのID)
 - 到達性のないID
 - 住民票コード, cookie, RFIDタグ
 - 発行者が管理目的で使うためのID
- 追跡性
 - 2つの非追跡性
 - Anonymity: それは何(誰)であるかわからないこと
 - Unlinkability: それが他の何かと同じだとわからないこと (「同定可能」でない)

IDと個人情報保護法

- 個人情報保護法における個人情報の定義
 - 住所氏名を含まないIDは「個人情報」ではない
 - この法律において「個人情報」とは、生存する個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。
- IDにひも付けされたあらゆる情報（私事性のある情報を含む）の記録、蓄積、売買は合法？
 - 住所氏名さえ含まなければ
 - IDが共通IDであっても
 - IDが「他の情報と容易に照合することができ」ないなら
 - 「容易に」とは？

懸念される事態

- 私事性情報蓄積の動機(現実)
 - FSP (Frequent Shoppers Program) や One to One マーケティングといったCRMのため、顧客の消費動向パターンを知りたい
 - 現に磁気カード式ポイントカードなどで行われている
- 氏名住所を含まないIDによる私事性情報の安易な蓄積(現実)
 - 個人情報ではないので管理が厳重でなくてすむし、売却しても合法
 - 無記名式ポイントカードはローカルなIDで管理されている
- 無記名私事性情報の共有の動機(仮定)
 - 自社が取り扱わない商品の消費動向が得られれば、自社商品のマーケティングに活かせるという考えから、業種を超えた提携が求められる
- 共通IDによる私事性情報データベースの共有化(技術的に可能)
 - 共通IDで購買行動を記録することで、事業者を越えた私事性情報の共有が可能
 - ポイントカードではできない(カードを共有化しないと)
- 他のIDを目的外使用することで購買行動を記録(技術的に可能)
 - 固定IPアドレスやRFIDタグのIDを、共通IDとして記録に利用できるようになる(?)
 - ポイントカードがなくても、ポイントカードを作ってくれない客でも、有効
- 蓄積された私事性情報の目的外使用や検索サービスの提供、または漏えい
 - 別の手段で知った、知人のIDから、過去に遡って当人の行動履歴を検索