堀部政男情報法研究会 共通番号制度と国民ID時代に向けた
プライバシー・個人情報保護法制のあり方 <課題と提言>
第3回シンポジウム
2010年12月19日 後日配布版

インターネットにおけるID利用の現状とプライバシーの課題

独立行政法人産業技術総合研究所
情報セキュリティ研究センター
高木 浩光

http://staff.aist.go.jp/takagi.hiromitsu/paper/horibemasao-201012-takagi-dist.pdf

講演趣旨

- インターネット上で進むID利用を題材に
- プライバシーと衝突してきた10年史
- IDで何をしたい人たちがいるのか
- 何が懸念されてきたのか
- 技術者たちが取り組んできたこと
- 技術的な落とし所はどこにあるか
- 日本の携帯電話で起きている独自の状況
- 日本で問題が解決されない具体的事例の数々
- 日本の法制度上の不備は何か

インターネットにおけるID

- IPアドレス
  - 通信相手を識別するために必然的に存在
  - IPv4では動的に再割り当てされるため時々変化する
  - 利用者を識別するIDとしては機能しない
- HTTP cookie
  - サーバ側がブラウザ側に覚えさせる任意の値
  - 乱数によりIDを与えて利用者を識別するために用いられる
  - 拒否や削除が可能
- 他には
  - HTTP cookie以外の同等手段が近年いくつか
  - 日本では「ケータイID」が2008年3月から
  - スマートフォンの端末IDが乱用される兆候

匿名で閲覧する権利

- 書くときの匿名性と読むときの匿名性
  - 公開される発言を書き込むときに期待する匿名性
    - 必ずしも広く求められるわけではない
  - 読むときに期待する匿名性
    - 誰が何を読んでいるかは秘匿されることが一般的には期待される
- 匿名性のレベル
  - 公開される
  - 第三者に開示される
  - 第一者が使用する
  - 記録するが使用しない
  - 令状によるものに限って開示
  - 記録しない
  - 識別しない

特定と識別

- 識別して個人を特定する
  - 個人情報保護法「特定の個人を識別する…」
  - 各個人情報保護法令の対象
- 識別するが個人を特定しない
  - 特定の個人を識別することがなくても、何らかを識別
    - Webブラウザを識別、携帯電話端末を識別、契約利用者を識別
      - 識別対象と個人とが事実上一対一対応したりする
  - 識別手段
    - cookieとして発行された乱数値、端末ID、RFID、MACアドレス等
- 特定可能性
  - 個人を特定しないで識別したものが、後に、個人を特定するために使用（できる場合、できない場合）

IDで何をしたいか

- Web閲覧のトラッキング
  - 行動ターゲティング広告、アクセス解析
    - 個人を特定せず乱数発行IDで視聴者を識別
- 「お一人様一回だけ」の実現
  - mixi等の利用者登録時にケータイIDを使用
    - 個人に比較的強く結びついた既存のIDを使用
- 「強固な」利用者認証
  - 個人に強く結びついた既存のIDの使用により実現？
    - これは技術的な誤解に基づいた単なる幻想
- 本人確認
  - 韓国の掲示板等での例
    - 住民登録番号のWeb利用（直接入力、i-PIN方式）

行動ターゲティング広告

- 行動履歴を蓄積して嗜好に合わせた広告を配信
- 行動履歴蓄積の実現手段
  - サイト内完結型
    - 大手ポータルサイトでは、サイト内での閲覧履歴から、利用者の行動を蓄積できる
  - 広告ネットワーク型
    - 広告を表示すると同時に、そのサイトを閲覧したことを記録
    - 同じ広告会社から配信される広告を表示しているサイト群を対象に、それらのサイトを閲覧したという行動を記録
  - DPI (Deep Packet Inspection) 方式
    - ISP（インターネット接続プロバイダ）に設置したDPI機器によって、通信内容を傍受して、趣味嗜好を分析しながら記録
  - その他
    - 「楽天ad4U」：IDを使用しない（が別の問題あり）

補足

- 行動ターゲティング広告とは
  - 購買行動につながる聴衆向けに広告を表示
    - 化粧品の広告は、女性を中心に見せたい
    - 分譲住宅の広告は、住宅を探している人に見せたい
    - 育毛剤の広告は、薄毛を気にしている人に見せたい
  - 聴衆一人一人の趣味嗜好に合わせた広告を選ぶ
    - 閲覧者の一人一人を識別し、
    - 閲覧者の行動記録を蓄積し、
    - 閲覧者の趣味嗜好を分析する

cookieの種類

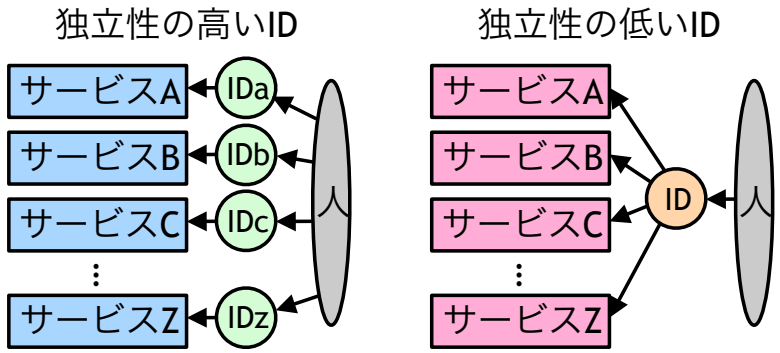
- 第一者cookie
  - 閲覧中画面のサイト自身が発行するcookie
    - そのサイトしかそのcookieを取得できない
  - アクセス解析、サイト内完結型行動ターゲティングには十分
- 第三者cookie
  - 閲覧中画面に埋め込まれた別サイトコンテンツ発行のcookie
    - 別サイトコンテンツの例：広告画像、ビーコン画像等
    - その別サイトしかそのcookieを取得できない
  - 広告ネットワーク型の行動ターゲティングに必要
- スーパーcookie（仮称）
  - すべてのサイトで共通に使える値
    - 行動ターゲティングには不要
    - 日本の「ケータイID」

Googleの取組みの例

- アクセス解析「Google Analytics」の場合
  - 第一者cookieで実現している（第三者cookie不使用）
  - Analyticsは第三者サイトに置かれているが、JavaScriptがcookieをセットするため、第一者cookieで実現できる
    - 技術的な創意工夫
      - <script src="第三者サイト"> （第一者サイト上にインクルードする）
      - document.cookie=乱数値（第一者サイト上で実行される）
- 広告「Adsense」の場合
  - 行動ターゲティングしない広告
    - 広告の貼付けられた画面上のコンテンツに相応しい広告を配信
      - 画面上のコンテンツを分析
  - 第一者cookieのみで実現

IDのサービス独立性

- IDの空間的連続性（サービス独立性）
  - 独立性の低いID（共通ID）は、匿名前提で蓄積された属性情報を、匿名でなくする危険性を高める



必要最小限の原則

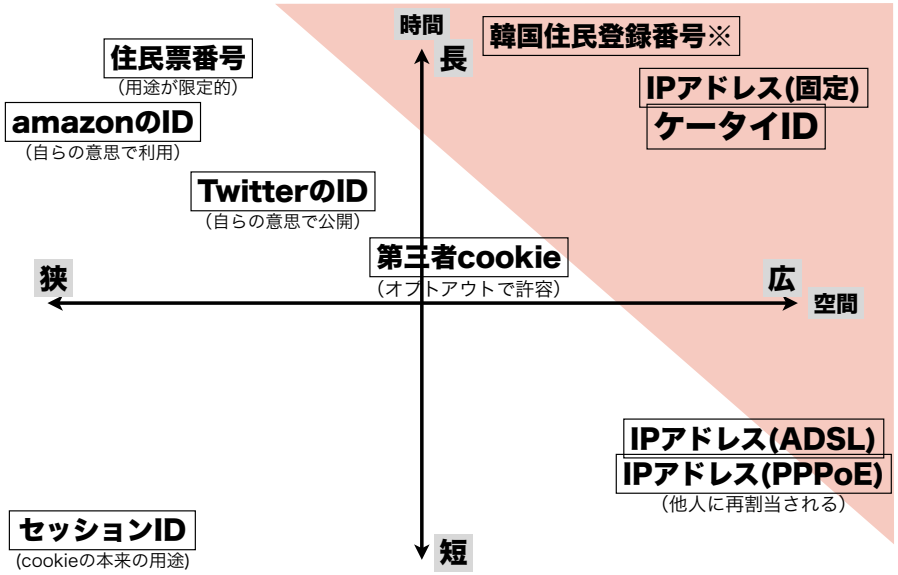
- 目的達成に必要最小限の技術を用いる
- プライバシーとの両立のため
- その技術的な実現手段が存在する場合がある

- 存在を知らなければこの考え方に至らない
  - 両立し得ないと誤解
  - （ビジネス上の都合によりあえて無視の場合も？）
- 誰も求めないなら配慮されない
  - プライバシー法令による圧力
  - 市民からの圧力

一方、日本では

- 行動ターゲティング用途にスーパーcookie使用
  - ケータイIDは「スーパーcookie」相当
  - ケータイIDが元々あるから（2008年3月以降）
    - docomoの旧機種（2009年春以前）にはcookie機能がなかったから
- プライバシー影響度最大の技術方式が、必要でないのに使用されている
- ケータイIDについてはこちら
  - 今こそケータイID問題の解決に向けて（2010年6月）
    http://takagi-hiromitsu.jp/diary/20100619.html

IDの時間的・空間的連続性



日本のプライバシー保護

- 通信の秘密
  - 個人が識別されるかに関係なく厳格に保護
- 個人情報保護法令
  - 特定の個人を識別する情報の取り扱い
- 欠けているもの
  - 個人を特定せず識別して蓄積されるプライバシー情報の保護
- 日本のプライバシー権
  - 個々のプライバシー侵害事案に対する法的措置は可能
- 欠けているもの
  - 社会インフラの信頼を確保する観点からの、個人を特定せず識別してプライバシー情報を蓄積するシステムに対する何らか

今日のニュース

- 共同通信「アプリから個人情報流出か スマートフォンで米紙調査」（2010年12月19日）
  - 「米紙ウォールストリート・ジャーナルは18日（略）iPhoneや（略）アンドロイド（略）101種類のアプリを調べた。このうち56種が、利用者の許諾を得ずに携帯電話固有の識別番号を外部の会社に送信。47種が位置情報を、5種は年齢や性別を送っていたという。」
- 一方日本は
  - 全機種が携帯電話固有の識別番号を無差別に常時送信中!!
  - なぜ問題にしない?
  - 「米国有力紙が問題視するんだから問題なんだろう」って？

日本だけ取り残された事案

- ケータイID問題
  - 諸外国ではこの方式は（ほぼ）使われていない
- Googleストリートビュー問題
  - そもそも…
- Google無線LAN電波傍受蓄積問題
  - 電波法では傍受だけなら合法

日本で起きた問題

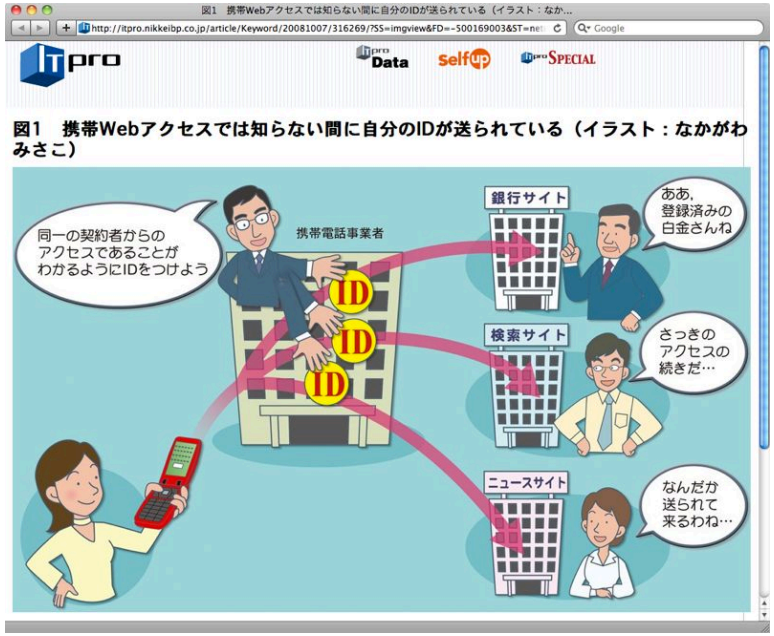
- これまでに問題となった事案
  - ケータイID 総務省研究会で問題に 2001年
  - Googleストリートビュー 2008年8月各社報道
  - 「楽天ad4U」 2008年10月、2009年3月産経新聞
  - 総務省諸問題研究会第一次提言
  - 総務省諸問題研究会第二次提言
  - DPI広告 2010年5月朝日新聞
  - Google無線LAN傍受問題 2010年報道なし
  - 総務省SIMロック解除ガイドライン
- 問題対処への法的根拠がない
  - マスコミによる世論喚起という手段しかない

履歴売買が始まる?

- 識別番号に紐付けた履歴を売買する構想
  - 日経産業新聞2010年8月16日「サイト閲覧履歴、取引仲介」「個人特定せず利用者を識別」「広告効果向上を支援」「サイト間で閲覧履歴をやりとりして別サイトの広告掲載に生かす手法は米国などで一般化しつつあるという」
    - 「Data Exchanger」と呼ばれる比較的新しい事業形態
- 合法か？
  - 番号自体は個人情報ではないとする総務省解釈をうけて
  - 「配慮原則」さえ守ればよい?
    - 総務省研究会の提言が一人歩きしつつあるのでは
  - 日本では法的に止めることができない
    - 米国で始まりつつある方式を、広告システム事業者が仕組みを一部誤解して、米国でも許されない方式を日本に導入してしまうおそれ

履歴売買で何が問題か

- 広告会社らの主張
  - 識別番号からそれが誰かはわからないので問題ない
  - 広告会社自身が個人を特定することはしないと約束
- その識別番号を住所氏名と紐付けできる者が、履歴情報を取得する場合が問題
  - 第三者cookieを用いた方式の場合、広告会社のシステム設計しだいでは、照合できる場合がある
    - 日本の広告会社は（誤解により）これを始めてしまうおそれあり
    - 広告会社側で個人を特定できない履歴情報を、ネットショップ等に提供する場合が問題となる（米国ではそのような提供をしない）
  - ケータイIDを用いた方式の場合、容易に照合できる
    - 広告事業者のみならず、ならず者たちにも悪用される危険がある



http://itpro.nikkeibp.co.jp/article/Keyword/20081007/316269/
日経BP社 日経NETWORK「契約者固有IDとは」より

http://itpro.nikkeibp.co.jp/article/Keyword/20081007/316269/
日経BP社 日経NETWORK「契約者固有IDとは」より

総務省 第二次提言「配慮原則」

- 広報、普及・啓発活動の推進
  - 利用者のリテラシーの向上や不安感や不快感の払拭に資するべく、対象情報を活用したサービスの仕組みや、本配慮原則に基づく取組について、広報その他の啓発活動に努める
- 透明性の確保
- 利用者関与の機会の確保
  - オプトアウトできるようにせよという意味
- 適正な手段による取得の確保
- 適切な安全管理の確保
- 苦情・質問への対応体制の確保

配慮原則「透明性の確保」

- 少なくとも以下について利用者に通知し、又は知り得る状態に置くことが望ましい
  - ア. 取得の事実
  - イ. 対象情報を取得する事業者の氏名又は名称
  - ウ. 取得される情報の項目
  - エ. 取得方法
  - オ. 第三者提供の事実
  - カ. 提供を受ける者の範囲
  - キ. 提供される情報の項目
  - ク. 利用目的
  - ケ. 保存期間
  - コ. 利用者関与の手段

私の考え

- ターゲティング広告自体を否定するものではない
- 悪いシステムを普及させてはいけない
  - 良いシステムと悪いシステムがある
- 個別に許容できるか否かを判断する必要がある
  - 技術的に越えてはならない一線がどこかを明らかにする
- ダメなシステム
  - ケータイID（全サイト共通番号）方式
  - 第三者cookieと第一者cookieを連携させる手法の一部
  - ……

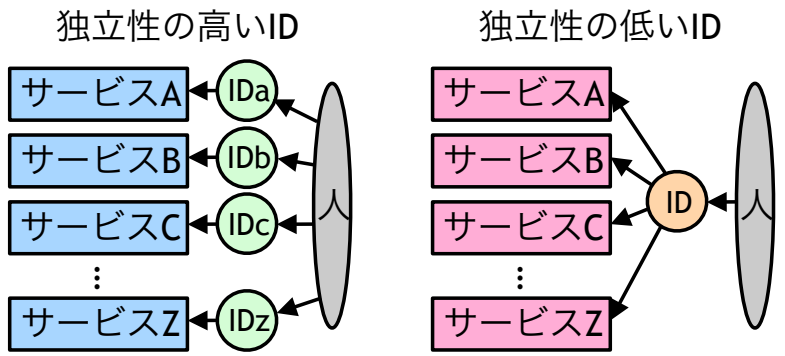
政府機関の無策

- Google Analytics使用問題
  - 日本の中央官庁や地方自治体がGoogle Analyticsを使用
  - 使用していることを表示していない
    - Google Analyticsの利用規約に違反
      - 「All website owners using Google Analytics are required to have a privacy policy that fully discloses the use of Google Analytics.」
  - 行政機関個人情報保護法、各地個人情報保護条例的にはどうか
  - 加えて言えば
    - 個別履歴のみならず、国民の政府サイト閲覧の動向が外国に常時送信される仕組みを政府が構築していること自体、いかがなものか
- 一方米国では
  - 合衆国行政管理予算局（OMB）が2000年からルール化
    - M-00-13: Privacy Policies and Data Collection on Federal Web Sites
    - M-10-22: Guidance for Online Use of Web Measurement and Customization Technologies

米国では

- ICAM 「Federal Identity, Credentialing, and Access Management OpenID 2.0 Profile」(2009)
  - 2.3.6 Pseudonymous Identifiers
    - Unique identifiers, especially those shared with multiple RPs, are considered personally identifiable information (PII). … To avoid the unnecessary exchange of PII, … The first is the Private Personal Identifier (PPID), which is a pair-wise pseudonym used to uniquely identify an end user at each RP they visit.
- eGoverment Act of 2002
  - (3) RESPONSIBILITIES OF THE DIRECTOR.
    - (A) develop policies and guidelines for agencies on the conduct of privacy impact assessments; (B) oversee the implementation of the privacy impact assessment process throughout the Government; and (C) require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form as the Director determines appropriate.

再掲



ひどいエピソード

- 飛騨市図書館個人情報流出事件で
  - 飛騨市発表文（2010年11月22日）
    - 「情報の内容：当館に登録されている利用者の情報の一部でデータの内容は、利用者氏名（漢字）、利用者氏名（カタカナ）、住所、生年月日、郵便番号等であった。」
  - 図書の書名も漏れたはずなのにそれが書かれていない
    - 電話で取材したところ「書名も含まれている」
  - 「なぜそれを書かないのか？」に対し図書館長曰く「住所氏名等が個人情報だから」
    - 住所氏名に紐付けられた書名自体は個人情報でない？
- 個人情報保護法での定義
  - …個人に関する情報であって、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…

キーだけが個人情報?

個人情報??

- 個人情報保護法での定義
  - …個人に関する情報であって、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…

日本はIDで何をするの?

- Web閲覧のトラッキング
  - 行動ターゲティング広告、アクセス解析
    - 個人を特定せず乱数発行IDで視聴者を識別
- 「お一人様一回だけ」の実現
  - mixi等の利用者登録時にケータイIDを使用
    - 個人に比較的強く結びついた既存のIDを使用
- 「強固な」利用者認証
  - 個人に強く結びついた既存のIDの使用により実現？
    - これは技術的な誤解に基づいた単なる幻想
- 本人確認
  - 韓国の掲示板等での例
    - 住民登録番号のWeb利用（直接入力、i-PIN方式）

まとめ

- 実現したいものとプライバシーの両立
  - 両立させる技術方式が存在することを知る
  - 技術方式上の落としどころがどこか
- そもそも何を実現したいのか
- 適切な技術方式を採用させるよう促す法制度
  - システムとしてのプライバシーリスクへの対応
    - 個別のプライバシー侵害事案に対する保護だけでなく社会のプライバシーリスクを軽減する措置が必要
  - 第三者機関の創設
    - 欧州各国のプライバシーコミッショナー等
    - 専門家集団によるプライバシー影響評価
    - 行政機関に対してだけでなく民間に対しても監督
    - せめて調査権だけでも与えて公開の場での議論を