

無断リンク禁止と儀礼的無関心、 不正アクセス禁止法、 プライバシーアーキテクチャと 匿名性

高木 浩光

前回までから

- 倫理研第3回共同討議より
公共圏の確立から「私的領域の確保」へむけて
- 東: まさにそうですね。情報社会以前では、予告状を直に送りつけでもしなければ威力業務妨害にはならなかったところが、いまは、比喩的に言えば、自宅の壁に書いてもそうになってしまう(笑)。自分のウェブ日記で「中国大使館を爆破したい」と書けば捕まってしまう。自分の日記だからいいんじゃないの、という論理は通じない。
- 倫理研第4回共同討議より
アクセス・コントロールによる私的領域の確保は処方箋となるか
- 東: 「繋がりの社会性」を欲望しているユーザーにとっては、アクセス・コントロールは実はなんの意味もない。そして、日本のネット文化を支えているのは繋がりの社会性であるのだから、アクセス・コントロールは本質的に対策たりえない。

目次

- 前半
 - 前回までからのつながり
 - 私的領域と公的領域を区別できるか
 - 無断リンクを禁止する人たちとあえて無視する人たち
 - 反無断リンク禁止派の求めるところ
 - 不正アクセス禁止法がもたらしたものととの共通性
- 後半
 - 新たな話題
 - プライバシー侵害アーキテクチャ
 - ダメアーキテクチャの普及を阻止することができるか
 - Webのプライバシー懸念が実世界に拡大する
 - 表現の/存在の匿名性/顕名性の倫理と設計

不正アクセス禁止法

- 不正アクセス行為とは、次の各号の一に該当する行為をいう。
 - 一 アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該**アクセス制御機能により制限されている特定利用をし得る状態にさせる行為**(略)
 - 二 アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該**アクセス制御機能による特定利用の制限を免れることができる情報**(識別符号であるものを除く。)又は**指令**を入力して当該特定電子計算機を作動させ、**その制限されている特定利用をし得る状態にさせる行為**(略)
 - 三 (略)

制限されていなければ自由

- 不正アクセス禁止法施行が確立させた倫理観
 - 「アクセス制御機能により利用が制限されていない利用であればアクセスは自由である」
- 「顧客情報ファイル丸出し漏えい」事件の続発
 - 2002年1月～
 - 2ちゃんねるで暴露する行為が続発
 - 丸見えになっているファイルやディレクトリのURLを書き込む行為
 - 「不正アクセスだろ!」という声が毎回まき起こったが、制限されていない利用なのだから不正アクセスではないという議論が毎度繰り返され、そうした考え方が広まり固まっていき、丸見えの場所が堂々と晒されるようになっていった。

「道端に置くのと同じ」

- 中日新聞 2002年7月4日 相次ぐ個人情報流出
“お寒い”企業の危機管理 監視庁「道に置くのと同じ」
より引用
 - (略)ハッカー被害との見方も出たが、背景を探ると多くは「サーバーの設定ミス」(専門家)などで、知識や注意不足が原因。情報技術(IT)社会のお寒い情報セキュリティ事情が浮かび上がる。
(略)
道端に名簿を置いていたのと同じ。 - 原哲也 **監視庁ハイテク犯罪対策総合センター所長の説明**は明快だ。一連の流出情報はサーバーの公開部分に置かれ、誰でも見られた。最低限の防御もしていないケースが多く、企業の相談で「法的に不正アクセスと判断できるものはない」という。

議論の混乱

- 無断リンクが当然をデフォルトにしないといけない
 - 新聞社や官公庁の無断リンク禁止ポリシーを見た一般人が、自分の個人サイトでも無断リンクを禁止するのが妥当だと考えるようになるという構造
 - 「新聞は無断リンク禁止だよ、許諾を得ましたか?」とか余計なお世話を書き込む人
- 議論の混乱
 - 新聞社や官公庁の話と個人サイトの話をごちゃ混ぜにする人々もいる
 - 官公庁の無断リンク禁止に対する撲滅運動の意義は、個人サイトの場合には当てはまらない

「儀礼的無関心」

- リンクは本当に自由なのか
- そっとしておいてあげる?
- 「リンクには許可が必要」という倫理観が形成される可能性
 - そうするとどうなる?
- 技術的手段による公的領域と私的領域の区分けは可能か?
- 望まないアクセスを「不正アクセス」ということにしたい人たちと、無断でリンクされることを望まない人たちの共通性

アクセスコントロール

- Webにおける私的領域の確保
 - 「アクセス・コントロールによる私的領域の確保は処方箋となるか」 倫理研第4回より
 - 「繋がりの社会性」を欲望しているユーザーにとっては、アクセス・コントロールは実はなんの意味もない。そして、日本のネット文化を支えているのは繋がりの社会性であるのだから、アクセス・コントロールは本質的に対策たれない。
- 技術による解決
 - 普及したとき何が起きるか
 - 自分の嗜好を偽ったり、アクセスを繰り返すなどして、仲間と判定されるように積極的に仕向け、目的のものを読むという行為が流行るか。
 - 面倒ならしないということ解決するか。

脆弱性届出制度

- IPA,脆弱性関連情報に関する届出について
<http://www.ipa.go.jp/security/vuln/report/>
 - 2004年7月より開始
 - ソフトウェア等脆弱性関連情報取扱基準, 平成16年経済産業省告示第235号
 - IV. 本基準の適用範囲
本基準は、以下に掲げるものの脆弱性であって、その脆弱性に起因する被害が不特定多数の者に影響を及ぼし得るものに適用する。
- 当事者に修正を促すことができるようになった
 - ファイル丸見え漏えいを告発するためとして(不正アクセス禁止法違反ではないことをいいことに)掲示板で暴露する行為は減り、それによって被害が出るという事態は減ったと推察される

それは欠陥?

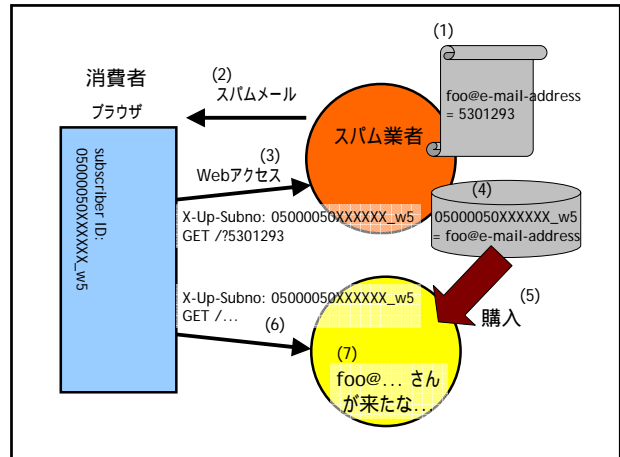
- 明らかな欠陥は直させることができるようになった
 - ソフトウェアの欠陥は、100パーセントの再現性があることが多く、一人の指摘者によって欠陥を認めさせられる可能性を持っているという特殊性
- オープンソース vs プロプライエタリ
- ほどほどに問題となるようなものについては、誰も直させる力を持ってない
 - 事例:固定の固有IDによるアクセス者の特定

固定の固有IDのプライバシー問題

- 英語圏ではこの問題はよく理解されている
 - WebブラウザにはIDが埋め込まれていない。
 - Intel Pentium III のPSN (Processor Serial Number)問題
ボイコット運動が起きて活用を断念
 - パナー広告会社が発行する「第三者cookie」に対する批判
DoubleClick社に対する訴訟、そして和解
P3P (Platform for Privacy Preferences) という技術による解決
 - Windows Media Playerに固有IDが埋め込まれており、JavaScriptで取得できることが「Super Cookies」であるとして批判され、Microsoftはその機能をデフォルトでオフに仕様変更
 - 最近でも、スパイウェア検知ソフトが追跡型のcookieを検出することをめぐって、これはスパイなのかそうでないのかという議論がある

携帯電話のID

- KDDIとVodafoneのサブスクライバID
 - 公式サイト以外にも常時送信される固定の契約者ID
 - どのサイトにWebアクセスしても同じIDが送信される
 - 設定で止めることはできる
 - KDDIでは2005年4月から
 - au, サブスクライバIDの通知・非通知を選択可能に、ケータイWatch
http://k-tai.impress.co.jp/cda/article/news_toppage/23345.html
- 何が問題か
 - プライバシーが損なわれる
 - 危険性と言えるような具体例
 - ワンクリック不当請求で、アクセス者を特定される



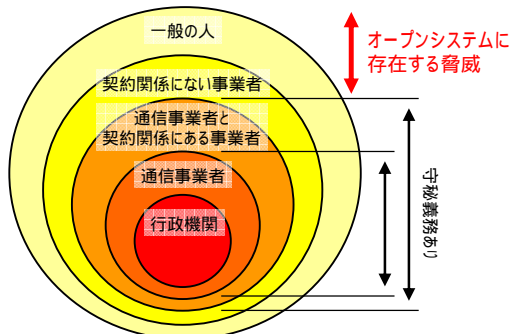
不当料金請求の手口

- 総務省総合通信基盤局電気通信事業部消費者行政課
「メールに記載されたURLへの不用意なアクセスについて
(不当料金請求の新しい手口にご注意ください)」(2004年4月)
http://www.soumu.go.jp/s-news/2004/040421_3.html
- 1 最近の手口
メールに記載されたURLをクリックして、高額な会費を請求される事例における最も典型的なパターンは、以下のとおりです。
1. 受信者ごとに異なる識別番号を含むURLが記載された迷惑メールを送りつけ、サイトにアクセスされるのを待つ。
例えば、090 の電話番号宛てのメールに、この電話番号に対応した識別番号(下のイメージ図では、321 a25c)を含むURLを記載し、受信者がこのURLをクリックしてサイトにアクセスしてきた場合、送信者は、当該電話番号の所有者がこのサイトにアクセスしてきたことを確認できます。
こうしたメールは、英数字を用いたメールアドレス宛てではなく、**携帯電話のショートメッセージサービス**(携帯電話事業者が提供する、電話番号宛てにメールを送ることができるサービス)を利用して送りつけられることが多くなっていますが、これは、**アクセスしてきた者の電話番号を把握できるため**、後日、入金の督促を電話で行うことができることがその原因と考えられます。

開放的 vs 閉鎖的

- 閉鎖的システム(昔の電話など)
 - プライバシーは一定の水準で保たれる
- 開放的システム(インターネットなど)
 - 誰でも自由に新たな事業に参入できるため、急速な発展を遂げる可能性を持つ
 - プライバシーを確保するための仕組みが必要
- ハイブリッドなシステム(近頃の携帯電話)
 - 開放システムに要求されるプライバシー確保の仕組みが必要であるにもかかわらず、誤って、閉鎖的システムの発想で作られる危険性

守秘義務の有無とオープンシステム

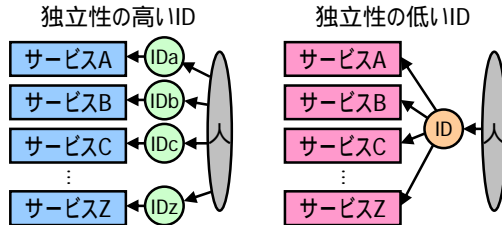


IDと個人情報保護法

- 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(直ちに)「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**(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(私人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?

IDの有効ドメイン範囲

- ID空間のサービス独立性
 - 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



修正させられるか

- 2002年8月にこの問題を訴えたが、声が届かないどころか、匿名で誹謗中傷されるほどの反発あり
 - 2003年5月からはたなダイアリーで地道に問題点を解説していくことによって、ようやく広く認識されるようになっていった
- 固定の固有IDを使った方法がプライバシーの問題を起こすことは、暗号応用研究コミュニティでは古くからの常識
 - 「unlinkability」を確保する技術の研究が進められてきた
 - たとえば、電子マネー
- なぜダメなアーキテクチャが普及してしまうのか
 - 研究と事業化
- 一旦普及させてしまったものは取り返しがつかないのか

ネットから実世界へ

- 高度「コピキタス社会」の推進
 - RFIDが人の持ち物などに取り付けられるサブスクリバード相当のものが実世界へ拡大
 - 実世界でも「アクセス」(存在)のトレースを可能にしてしまう
- プライバシー問題を回避できるか
 - IDだけでは個人情報保護法による個人情報に該当しないため、取り扱いがぞんざいとなり、また、どんな目的に使用しても合法となるおそれ
 - 技術的な解決策はいまひとつ希望を持ってない
 - ICカードと異なりICタグは低価格が優先されているため
 - 長距離の読み取りが期待されているため、消費電力を抑える必要があり、暗号演算回路を搭載することができず、プライバシー対策ができない

懸念される事態の例

- 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IID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すむし、売却しても合法
 - 無記名式が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、事業者を超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)
- 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

推進派の無理解

- 日経IT Proの記事「消費者に理解されていない「ICタグ」」
2003年8月
<http://itpro.nikkeibp.co.jp/free/ITPro/OPINION/20030806/1/>
- 「ICタグに個人情報を入れなければ問題ない」というインチキな主張
 - 本気でそう思っている人もいる
 - 意図的に問題をすり替えている?
- 実際には問題点AとBがあるにもかかわらず、Aの問題だけを取り上げて、Aは解決済みであり、それを理解しない消費者が騒ぐだけ というやり方
- プライバシー問題を指摘する反対派(「プライバシー擁護派」)は、米国の狂った人たちだけの主張だろう という思い込み

プライバシー懸念要因の区別

- 以下は分けて議論する必要がある
 - システム欠陥が原因で守られるべきプライバシー情報が事故で漏えいしたり、故意に盗み出されたりする
 - 内通者が情報を外部に持ち出したり、従業員の実ミスで漏えいさせる
 - 事業者が情報を外部に提供する予定がある場合に、それを消費者が承知しているかの問題
 - 事業者を信頼してよいかの判断が、普通の消費者にはたして可能なのか
 - 消費者に事業者の選択の余地がなくなる懸念
 - 共通(固有)ID方式という識別アーキテクチャの問題

胡散臭い標語「安心・安全」

- 「安心」とは?
 - 真に安全でなくても、安全だと思込まれることによる安心感?
- 安心・安全のためとして、小学生の行動をIDで追跡可能にする動き
 - ランドセルにRFIDを取り付けて追跡する実験が、立て続けに
 - 繰り返される実験の報道
 - 経済部記者によるもの
 - なぜ?
- 技術的には、かえって危険が増すという問題点の指摘

「ICタグで子どもの安全を」?

- アクティブ型RFIDタグをランドセルに取り付けて.....



NHK総合、ニュース10、2004年9月27日22時55分ごろより

キャスターB:「これがその、子供達がランドセルに付けていたICタグなんですけども、ずいぶんとこ小さくて軽いんですねー」
 キャスターA:「そうですねえ、なくした場合ちょっと心配かと思うんですけども、この中にはですね、児童ひとりひとりに割り当てられた数字と文字しか入ってなくて、名前ですとか住所とかは、流出することがないんだそうです。大丈夫なんだそうです。」

別の番組では...



讀賣テレビ「ワークアップ!」
 2004年10月9日午前9時2分8秒より引用

利便性の過大評価

- 「安全のため」として導入される「監視」技術
 - プライバシーが犠牲になるかもしれないにしても、「安全のためなのだから」とされることは多い
- しかし
 - 実はたいして安全にならない場合
 - 実はかえって新たな危険性も生ずる場合
- 子供をダシにした実験
 - 保護者への事前説明でリスクは開示されているか
 - 業界関係者の反応
 - 「全部が悪いかのようなイメージを招く不用意な実験は迷惑だ」

真の目的を隠すための利便性?

- ICタグで連れの客の所在確認・阪急百貨店で実験、日本経済新聞、2004年11月9日朝刊
<http://it.nikkei.co.jp/it/newssp/ictag.cfm?i=2004110810133wf>
 - 店内に設置した表示装置に客がICタグをかざすと、別行動している連れの客の居場所が表示される。家族やグループで来店した客が、それぞれ自由に買い物しやすくなる(略)。
- ICタグで居場所ビタリ 阪急百貨店が実験へ 別々の買い物自由に、大阪読売新聞夕刊、2004年11月10日
 - 「十六歳以上の来店客に、二人一組でICタグ(縦約五センチ、横約三センチ)をそれぞれ持ち、別々に買い物してもらい、タグから発信された電波は、各階に六か所あるアンテナがとらえる。
- 客へ実験の目的がどう説明されたか?
- 些細な利便性を提供して見えない真の目的を達成する

匿名性に対する懸念

- 「安心・安全インターネット推進協議会」
<http://www.scat.or.jp/stnf/> 設立趣意書より:
 - しかしながら、現在のインターネットでは、利用者の個人情報が漏洩したり、身に覚えのない請求が届いたり、といった事件が頻繁に発生しており、ネットワークの利用に関する不安が増しています。これは、匿名性や、必要最小限の通信機能のみを提供するといったインターネットの特徴を悪用したものであります。ネットワークビジネスを一層活性化し、国民誰もが安心・安全に参加できるネットワーク社会を実現するためには、現在のインターネットは不十分であり、すべてのセキュリティ対策を端末で行うのではなく、ネットワーク側でセキュリティを確保し、利用者がネットワークにアクセスした瞬間に安心・安全なコミュニケーションの場に参加できるネットワーク環境の構築が強く待望されています。
- インターネットのLモード化構想か?

匿名性に関する混乱

- 表現の匿名性と存在の匿名性
- 混乱
 - 表現の匿名性の弊害を主張することによって、存在の匿名性を失わせるアーキテクチャを導入しようとする人たち
 - 両者は区別して理解するべきであり、そうすれば、存在の匿名性の必要性について反対する人はいない
 - 存在の匿名性を確保しつつ、表現の匿名性を制限することは可能
 - 常に表現の匿名性を排除せよという話と、場合によって制限するという話は別であることにも注意

表現 / 存在の、匿名性 / 顕名性

- 東浩紀, 情報自由論(9) 表現の匿名性と存在の匿名性, 中央公論2003年4月号より
- 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

IPアドレスの固定化

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) <small>+ダイヤルアップ</small>

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

実名でのネット活用促す

- 実名でのネット活用促す 総務省「悪の温床」化防止、共同通信、2005年6月27日
 - 総務省は27日、自殺サイトなど「有害情報の温床」ともいわれるインターネットを健全に利用するために、ネットが持つ匿名性を排除し、実名でのネット利用を促す取り組みに着手する方針を固めた。匿名性が低いとされるブログ(日記風サイト)やSNS(ソーシャル・ネットワーキング・サイト)を小中学校の教育で活用するよう求め、文部科学省などと具体策を詰める。今週初めに発表する総務省の「情報フロンティア研究会」の最終報告書に盛り込む。
- 「ネットに匿名性は不可欠」 総務省、ITmedia、2005年7月1日
 - 「総務省がネットの匿名性を排除しようとしている」とある報道を発端に批判が広がった。総務省は、ネットの実名性を高める必要はあるとしながらも、匿名性を排除するつもりは全くないと弁明する。「ネットの匿名性を排除すべき」とは言っていないのだが、総務省情報通信政策課の内藤茂雄課長補佐は、一部報道をきっかけにブログ界で盛り上がった「政府がネット利用の実名化を推進しようとしている」という議論に頭を抱えた。

顕名Webアーキテクチャの可能性

- Webに顕名システムを作る
 - 事前に本人確認した者のみにIDを与え、必ずそのIDでblogなどを書く仕組み(小倉秀夫さんのこのところのご提案)
- 存在意義
 - たしかに、Webでは実名による議論は簡単でない
 - メーリングリストなどに比較して
 - 特定のサービス事業者で閉じたIDではなく、事業者をまたがって同一性が保証されるIDシステム
 - シングルサインオンのようなもの(ログインが自動である必要はない)
 - コメントの氏名欄に「小倉」と書かれていて、それは誰なのかという問題の解決
- すべての表現システムに適用する必要はない
 - 始まるとその後どうなるか?