追跡される私たち

行動履歴のトラッキング
高度化かつ巧妙化する技術

大東文化大学 経営学科
水谷正大

政府も　貴方を監視したい　犯罪を防ぎたい

企業も　貴方用のサービスをしたい

他人も　先駆けたい　心配だから

すご〜く

あなたのことに関心がある

貴方が思ってもみない
ようなことに

怖い？
不安？
嬉しい？

なぜ私に関心があるの？

日頃の言動や行動を知れば、貴方の欲求や不満、
行動計画がわかるから

間接的調査（尾行）の大いなる手間を掛けずに、直接の売込（捕獲）が可能

分かりやすく単純な（暴力的）世界へと移行？

行動履歴の追跡 tracking

誰が何に関心があるのか（検索エンジン）
誰がどのWebページをどんな順で何を見たか
誰がいつメールを読んだか
誰がどんなマウス操作をしたか

見知らぬ人に覗かれながら生活している？

http://www.asahi.com/digital/av/images/TKY200808190128.jpg

trackingという覗き込み

？

第三者に開示できる？
ユーザの許可は不要？
事前告知は必要？

さらに。。。

twitterの発言やFacebookで知らせた内容

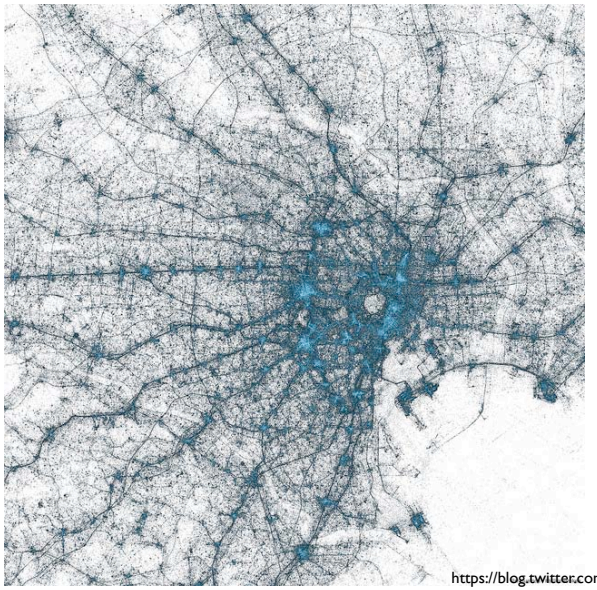
＋

そこから知人を辿り、その発言や写真など

から、貴方についての情報が一層補強される

ありがとう、貴方がtwitterで教えてくれました

2009年からのtweetした場所



https://blog.twitter.com/2013/geography-tweets-3

twitterの位置情報設定

iPhoneで撮影したGeo-Taged写真

[設定][プライバシー]
[位置情報サービス]はON
撮影アプリをOFF撮影すればGeoTagはつかない

GeoTag GPS機能を利用して写真に付加されるExif情報

iPotoで見てみると位置情報が表示される

写真整理や記録にはきわめて便利 (^^)

You should know about GeoTag

GeoTagがついたままで写真をメールしたりSNSで公開すると撮影場所がわかる・詐称可

画像投稿機能がついたアプリケーションで要注意
（iPhoneのメール送信してアップロードした写真はiPhoneがGeoTagを削除して送信する）

GeoTagを含むExif情報

GeoTagは写真撮影の記録としては非常に重宝

＋

不用意なGeoTag付き写真は高度なプライバシー露出

写真のExif (Exchangeable image file format)情報を編集加工できるソフトやアプリが沢山ある

本来の撮影場所とはまったく無関係な任意のジオタグ情報を追加して**場所や日付の詐称も可能**

iPhoneの位置情報設定

Facebook情報設定

http://jp.techcrunch.com/2013/06/14/20130613smile-hackers-can-silently-access-your-webcam-right-through-the-browser-again/

知らない間にハッカーがWebカメラであなたの写真を撮ってしまうかもしれない

GREG KUMPARAK

2013年6月14日 コメント

ラップトップのWebカメラにテープを貼って、外部からののぞき見を防いでいる人がいるよね。でもそれは、妥当な行為なのだ。

今日（米国時間6/13）登場したハッキングのデモは、ブラウザからWebカメラを操作してユーザの写真を撮る（そして盗る）。もちろんユーザの承認なしで。

実際にはユーザは承認をしているのだが、そのことを自分で知らないだけだ。

セキュリティコンサルタントのEgor Homakovが概要を説明しているが、このハックはいくつかの昔からあるトリックを駆使してFlashの事前承認要件を回避し、ユーザの明示的な許可なしでカメラやマイクにアクセスする。

簡単に言うとそのデモは、CSS/HTMLの高度なトリックを多重に使って、Flashの許可プロンプトを透明な層の上に表示し、その今や見えない"Allow"（許可する）ボタンの上にユーザがクリックしそうなもの…ビデオの"Play"ボタンなど…を置く。

このテクニックそのものは、クリックジャック(clickjacking)と呼ばれ、前からある。ぼくはこれまで、そういうものについて書くことを避けてきたが、それは、知る人が少なければ被害の広まりも少なくて、実害を受けるまえに対策も可能だ、と思うからだ。でもクリ

クリックジャック

断片的なことがらだけでも

多数集めて総合すると

ジグソーパズルのように

貴方のことが浮かび上がってくる

それらを自動化する**高度な技術**、それを可能にする**強大なコンピューティングパワー**がある

治安、政治、軍事問題はここでは触れない

インターネット利用を拡大し豊富にしてきた源泉

政府の公共部門

税金による資金提供

民間資金（市場原理）

広告収支モデル

技術・知識のオープン性

贈与の経済モデル

互いに協調
融合してきた

教育と知の在り方は我々の未来にもっとも重要な課題

消費者庁インターネット消費者取引連絡会

インターネット広告の概況と健全化の取り組み

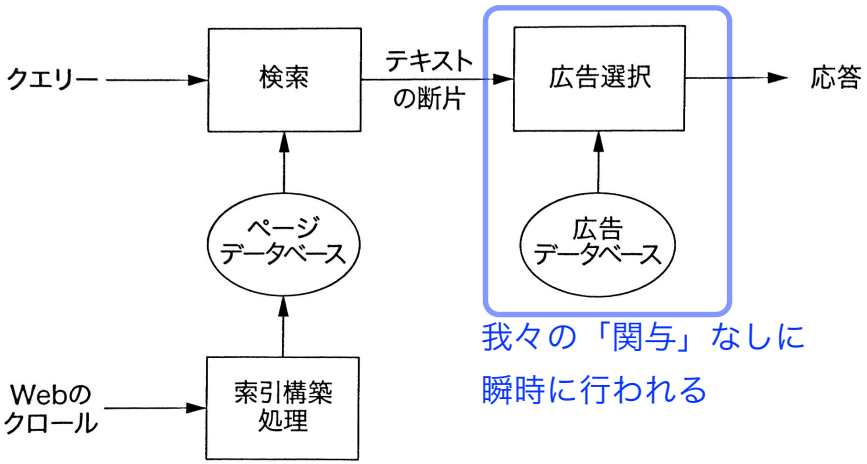
http://www.caa.go.jp/adjustments/pdf/130306shiryo1_1.pdf

〈参考〉インターネット広告の種類と取引契約形態

デバイス	種類	手法	取引契約形態
パソコン --- スマートデバイス スマートフォン タブレット --- モバイル フィーチャーフォン	ディスプレイ広告 ウェブ上に表示される画像による広告（いわゆるバナー広告など） テキスト広告 ウェブ上に表示される文字（テキスト）による広告 タイアップ広告 媒体サイト内に専用ページとして設けられる広告 インターネットCM 映像や音声による動画広告 ペイドリスティング 検索キーワードやウェブコンテンツに連動して表示される広告 メール広告 電子メール内に表示される広告（メールマガジン挿入型やDM型など）	枠売り --- 運用型	期間保証型 媒体が設定する一定期間の広告掲載を保証 掲載期間に対して課金される インプレッション保証型 広告が露出される回数(インプレッション)を保証 1回あたりの露出に対して課金される インプレッション課金型 露出回数、期間、クリック数等は保証されない 1回あたりの露出に対して課金される クリック保証型 広告がクリックされる回数を保証 1回あたりのクリックに対して課金される クリック課金型 露出回数、期間、クリック数等は保証されない 1回あたりのクリックに対して課金される 成果報酬型 露出回数、期間、クリック数等は保証されない 広告を通した任意の成果(売上額や契約数など)に対して課金される 枠指定型 配信数保証型

7

Web検索と広告配信の仕組み



我々の「関与」なしに
瞬時に行われる

デジタル作法 ～ カーニハン先生の「情報教室」　p260　オーム社（平成25年）

広告配信の行為よりも

ターゲット広告

貴方にどのような広告が蠱惑的か

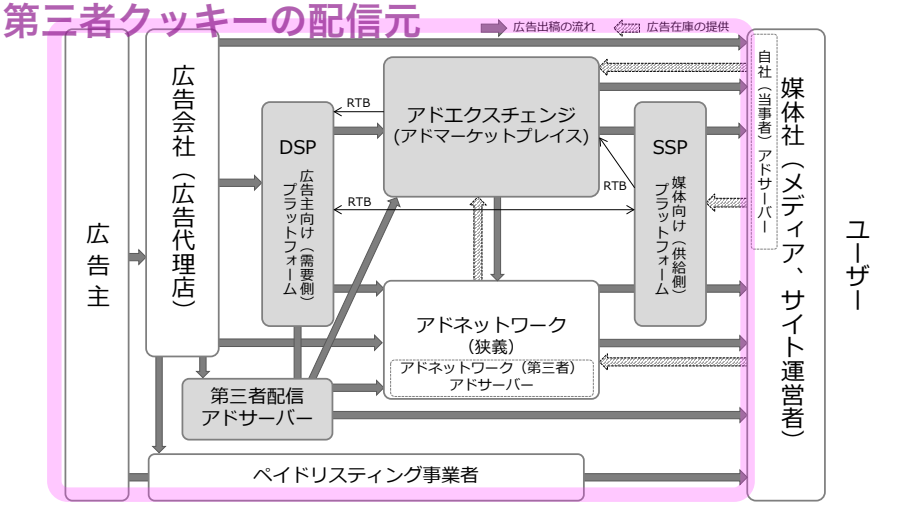
のための情報収集の方法それ自身に問題がある

消費者庁インターネット消費者取引連絡会

インターネット広告の概況と健全化の取り組み

http://www.caa.go.jp/adjustments/pdf/130306shiryo1_1.pdf

〈参考〉インターネット広告取引のフロー概念図



媒体社への広告掲載までのフローには、国内・海外の多数のプレイヤーが複雑・多様に関連している

HTMLメールの受信

歌舞伎美人

<img src="http://www.kabuki-bito.jp/news/newsletter/img/header_title200803.gif" alt="歌舞伎美人" border="0" width="316" height="56">

このメールはたいへん「良心的」です

<img>タグの画像を読み出すと配信元に
オプション情報と共にログが記録される

<img src="http://www.kabuki-bito.jp/news/img/mm/2013/342_3.jpg" width="250" height="157" border="0" alt="仁左衛門が語る「七月大歌舞伎」">

You should know about HTMLメール

画像の読み出しのたびに、送付先の特定メールアドレスでメールが閲覧されているかをオプション情報と合わせて確認可能

Webビーコン

もし画像が透明なら、**利用者に知られることなく**行動確認できる
スパムHTMLメールなら読むだけでスパムメールの送り手に情報提供してしまう spamビーコン

HTMLメールにはイメージブロック設定を！

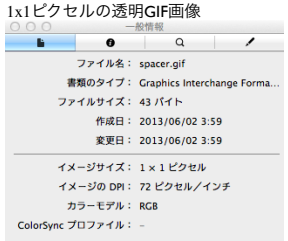
Webビーコン（Webバグ）

http://ja.wikipedia.org/wiki/ウェブビーコン

メールに埋め込まれた<img>要素を解釈・表示する際はサーバへのリクエストが生ずるが、付加された符号もそのリクエストとともにサーバに伝達される。それにより、サーバ側ではどの受信者がそのメールを表示したかを知ることができる。HTMLメールを送信したサーバ側に受信者の個人情報があれば、特定の個人の行動(メール閲覧)を把握することも技術的には可能である。

WebビーコンはJavaScriptをOffにしていても画像読み込みだけで追跡可能

1x1ピクセルの透明GIF画像



Webメールに埋め込まれたWebビーコン例

メール送信元からのWebビーコン

<img src="http://m3.rakuten.co.jp/open.phtml/-/45u0/992fd/aigj0" width="1" height="1" border="0">

いまや大抵のHTMLメールに仕込まれている

透明画像にすることによって受信者にはこの仕掛けは直ちには分からない

メール送信元とは異なる**ページビューを追跡する専門企業**からのWebビーコン

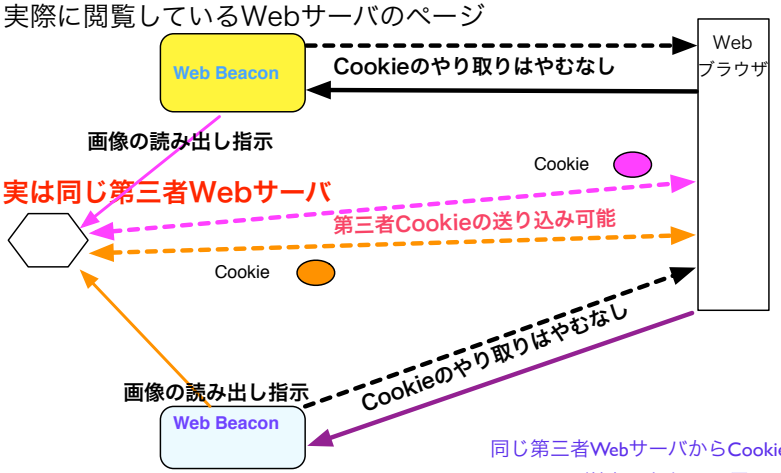
<img src="http://a248.e.akamai.net/f/248/47562/14d/ig.rsys4.net/responsysimages/lejpn/NL891_130601/nl891/spacer.gif" alt="" width="15" height="1">

Cookieを届けられるのは要求があったWebサーバだけから

Web ビーコン

画像読み出しのために第三者Webサーバに要求をだしてCookieを受領する環境を強いる

実際に閲覧しているWebサーバのページ



別途閲覧するWebサーバのページ

同じ第三者WebサーバからCookieを受け取るとユーザ情報の把握は一層正確になる

Webビーコンで収集できるデータ

Web閲覧者には高々小さな画像を読み込んだ程度の認識しかない。
しかし、Webビーコンは画像の振りをしたcgiやphpプログラムとして動作可能である。

収集可能データ

- IPアドレス、プロバイダホスト名、
- 閲覧時刻
- 閲覧経過時間
- 閲覧したURL
- リファラ（そのページの参照元）。検索ワードも調査可能。
- Cookieの発行も可能
- JavaScriptを併用すると
  - 利用しているブラウザの種類
  - モニタの解像度

収集不可データ

- 利用者の氏名とか正確な住所
- メールアドレス（工夫すれば可能）
- 電話番号

あるIPアドレスのユーザーはどんな時間に、どんなページを見ているかは完全に分かる

問題点

いかなるデータの収集に際して事前の**警告や説明は一切なし**。自分のデータが第三者に勝手に収集され、さらに別の業者に渡って分析され得ることは**正当なのか**？

Gmailはイメージブロックする

特定の送信者からの画像を表示する

外部画像へのリンクが含まれているメールを受信しても、通常、Gmail ではそのような画像は自動的には表示されません。これはプライバシーを保護するための対策です。画像が自動的に表示されると、画像が取得されたことがメールの送信者に通知され、いつメールを読んだか知られてしまう可能性があります。

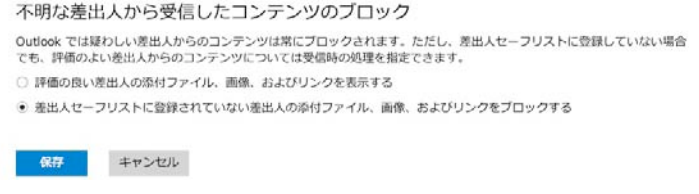
ただし、少なくとも 2 回メールを送信した相手から画像入りのメールが届いた場合、そのグループのユーザーは信頼できるとみなされ、デフォルトで画像が表示されます。認証されたメール内の画像しか表示されないので、送信者の名前やアドレスを偽装したなりすましメール内の画像が表示される心配はありません。このグループのメンバーからの画像がデフォルトで表示されないように設定を変更することもできます。方法は次のとおりです。

1. 右上にある歯車のアイコンをクリックし、**[Gmail 設定]** を選択します。
2. **[外部コンテンツ]** セクションで **[外部コンテンツを表示する前に確認する]** を選択します。
3. **[変更を保存]** をクリックします。

設定: Outlook.comでイメージブロックする

[mailの詳細設定]

[迷惑メール処理レベルの選択]



[受信されたHTMLメールの様子]

アクティブコンテンツ

Webからダウンロードしたコードを実行するように
促すページ（動的・インタラクティブなページ）

http://technet.microsoft.com/ja-jp/library/cc722487.aspx

10 Immutable Laws of Security

Law #1: If a bad guy can persuade you to run his program on your computer, it's not your computer anymore

悪い奴が貴方のコンピュータでプログラムを動かすことができたら、それはもはや貴方のコンピュータではない

.exe/.vbsファイル　極悪　Windowsの実行形式。軽々に実行しては絶対ダメ

ActiveX　リスク高し　Internet Explorerにコードをロードしてそのまま実行する機能
任意のWindows命令を実行できコンピュータを完全制御できる。供給元を信頼する
しかない。IEをデフォルトブラウザにするのは避け、最後の手段にするのがbetter。

Plug-in/拡張機能　リスクあり　ブラウザと協調して動作するプログラム。
QuickTime, Adobe Flash, Silverlight など。供給元を信頼するしかない。

JavaScript　ある程度は制御可能　ほとんどのWebページに含まれているコード
巧妙にユーザ情報をトラッキング可能。Alas... 不可避なのか？

追跡状態を知りブロックする

Ghostery http://www.ghostery.com

Disconnect http://disconnect.me

NoScript http://noscript.net