

平成22年9月9日

FIT2010 LOIS研究会 講演資料

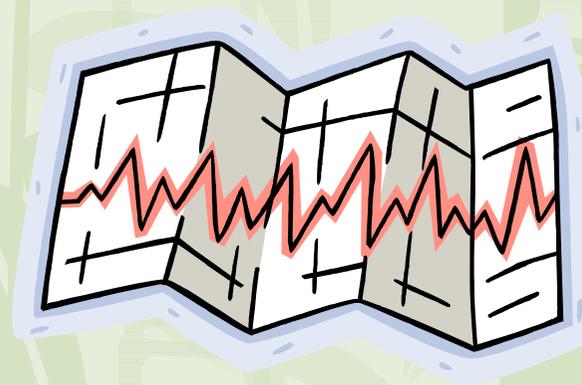
～ライフログ活用サービスのために個人情報管理～

ライフログのための個人情報管理と法

大阪成蹊大学/大阪市立大学大学院

松田 貴典

広範なライフログとその活用方向



1. 広範なライフログ

ライフログ(Life Log:生活行動記録)は、「蓄積された個人の行動記録」であり、非常に広範な個人の蓄積情報をさす[2]。以下事例である。

■ POSによるCRM情報:

百貨店, CVS(コンビニエンスストア), 小売店舗, スーパーマーケット, レストラン等での購買・決済記録

■ インターネットによる電子商取引, 決済記録等:

■ クレジット, 電子マネー等の利用状況:

Edy, nanaco等の電子マネー使用記録。Suica, ICOCA, PASMO, PiTaPa等の交通電子マネー等による交通ルート・購買決済記録等

■ 閲覧履歴:

ウェブのアクセス記録, 検索語句, 訪問先URLや滞在時間等

■ 位置情報とその周辺映像:

携帯端末のGPS機能により把握された行動記録, 道路周辺映像, 街頭カメラ映像を解析したもの等

■ SNSに書き込まれた趣味・嗜好・交友記録等

■ 医療情報(病歴, 投薬等), 人間ドッグ情報, 健康管理のための生体データ等

2. ライフログの活用の方向性

ライフログの活用方向性には、大きく二つある [2]。

どのような活用の方向性があるのか、検討する必要がある。それはライフログの方向性とその活用方法、収集情報により、法的な問題は変わる。

1. 収集された情報が自分のアシストのために提供される方向性である。

ユーザの行動履歴からユーザが求められると思われる情報を配信するサービスであり、行動ターゲティング広告と行動支援サービスがある

① 行動ターゲティング広告

Webの閲覧記録や電子商取引サイトからの購入履歴から、利用者の趣味、嗜好からクラスター分析をして、広告を出し分けるサービス。

例：オークション事業者が、利用者の購入履歴にもとづき、携帯サイトへのアクセス時に嗜好品の広告表示等

② 行動支援サービス

ユーザが使用するGPS機能付の携帯電話からの位置情報や、購買情報から、趣味嗜好を分析して、ユーザのタイムリーな情報を提供するサービス

例：携帯電話の利用者の位置情報から、との地域局所の天気予報を提供する等

2. 個人の行動履歴が外部に統計情報として情報提供される方向性である。

GPS機能付の携帯電話からの位置情報を所有者情報(性別、年齢等)とを組み合わせる詳細な統計情報の作成し販売する等

ライフログの法的脆弱性



1. ライフログと法的脆弱性

現代のICT (Information Communication and Technology) の飛躍的な進展は、携帯端末は単なる情報発信機能から情報閲覧機能や生活を支援する高機能(電子決済や地図情報の提供等)まで持つようになってきた。

しかし、そこから発信される、購買情報やサイト閲覧情報、行動情報等は、ライフログとして収集されることになる。ライフログが収集されることで、利用者にとって属性情報に応じたコンテンツや広告の提供を受けるサービスにして進展してきている。

ICTの「効用」を求めれば、その対峙関係にある「脆弱性」が潜在化する。

『情報システムの脆弱性は、ICTの本質的な特性に起因して、情報化に伴い、そこから得られる「効用」に比して不可避免的に発生・拡大化し、潜在化する欠陥』である。脆弱性には、ICTの本質的な脆弱性を基底に、「**組織・管理的側面の脆弱性**」、「**国際・社会的側面の脆弱性**」、「**法・論理的側面の脆弱性(以降、法的脆弱性という)**」があり、相互に密接に関連する。

2. ライフログの法的脆弱性の背景

ライフログが収集通信の秘密、**個人情報やプライバシーの保護**といった側面で、**法的脆弱性**の問題が指摘されている。

- ①ユビキタス情報社会の到来によるパーソナル化が進み、購買情報や決済情報、サイト閲覧情報など個人の行動が収集され、消費者の不安がつのりだしてきたこと、
- ②ストリートビューに代表される街角映像や写真が、無警戒に撮影され開示されていることで、**情報開示**がされているのではないという不安がつのり始めてきたこと、
- ③クラウドコンピューティング化によりあらゆる情報が、データベース化され、どこでどのように情報が収集管理されているのか、**自己がコントロールできない情報社会**になってきたこと、
- ④ICTの活用は情報戦略が優先し、**法的脆弱性**から発生する法的リスクについて、十分に検討されないまま、活用されること、などが挙げられる。

ライフログの法的問題

個人情報保護とプライバシー侵害

ライフログの法的問題

ライフログサービスに関連して、今後検討すべき法的に問題は、おもに「**個人情報保護**」と「**プライバシー保護**」がある。

しかし、ICTの高度化とライフログサービスのニーズの多様化で、今後どのようなサービスが展開されるかは予測することは難しい。サービスを提供する事業者にとって、個人情報保護とプライバシー保護の問題以外に、集められた情報の利用面で「**著作権法**」上の問題が発生することも考えられる。また、サービスを提供する側にとっても、同意のない「個人情報の収集」や本人の承諾のない第三者提供という問題も発生する。

POSや携帯電話、電子マネー、ポイントカードやクレジットカード等から集められた購買履歴が行動履歴の情報、いついつに、どのような商品をどこから買ったとか、どこどの店に立ち寄ったとかいう情報、GPS機能をもつ携帯電話により取得された位置情報、ユーザの年齢・性別等の属性情報、街角で撮影された人物写真、住宅の中が詳細に写った表札や車のナンバープレート等、**個人情報として問題のほか、プライバシーや肖像権でも大きな問題となることが予想される。**

個人情報とは

■個人情報は、「**特定の個人を識別できる情報**」(個人情報保護法第2条)

個人情報保護法では、**生存する個人に関するもので**、①氏名や写真のように見れば識別できる情報、②他の情報と照合することで識別できる情報がある。但し、社員番号や電話番号、住所などは個人が**識別できなければ個人情報とされない**。

■個人情報には、氏名、住所、性別、年齢、生年月日などの「**基本情報**」と電話番号、趣味、職業、職例、学歴、病歴、写真、映像、音声などの個人にとって知られたくない、プライバシー度が高い、取扱いの注意義務がある「**センシティブ情報**」がある。電話番号のように公開されている情報もある。

■名誉となるような情報(表彰、栄誉など)は、個人情報であるが一般に公開を望むことになり、プライバシー情報とされない。

プライバシーの保護と法

プライバシーや肖像権を定めた法律はない。しかし、判例の中で実質的にみとめられている[注1]。

- ①個人の私生活上の情報,
- ②まだ、一般の人が知らない情報,
- ③一般人ならば公開が望まない情報, とされている。

しかし、近年の判例では、「自己が欲しない他者にみだりに知られたくない情報か否か」で判断されるが[注2], 名誉となるような情報(表彰, 栄誉など)は、個人情報であるが一般に公開を望むことになり、プライバシー情報とならない。

また、街角で撮影された人物写真等は、明らかに誰か分かる状況であれば、プライバシー問題のみならず、肖像権の侵害になりえる。肖像権はプライバシー権の一部を構成することになる。したがって、写された場所や状況によっては、プライバシーの侵害となる。ただし、大勢のなかで写されたもので個人が特定できないような場合や撮影が前提になっている場合には、侵害とならない場合もある。

1. POS情報とCRM

■ POS情報におけるライフログ

スーパーや、CVS(コンビニエンス・ストア)、ドラッグストア等の流通業では、古くからPOSを導入し、欠かせない情報機器となっている。近年のPOSは、受発注管理や店舗管理のみではなく、顧客カードと連動して、顧客の詳細な購入データが収集される。また、顧客カードをクレジットカード化して、クレジット決済情報も収集される。さらに、銀行との連携で、デビット決済やローン契約による決済も可能である。この情報をもとにCRM(Customer Relationship Management)が構築される。ある大手スーパーでは、顧客特性を分析して優良顧客を定義、LTV(生涯価値情報)とポケットシェア(収入からどの程度購入しているかの消費シェア)等の管理をしている[3]。

■ POS情報は、日常生活のなかでの食品や衣料の購買履歴がライフログとして蓄積されているが、これまでは、情報システムの投資及び大容量データの分析のための要員等で、CRM進んでいなかったが、ICTの高度化やクラウドコンピューティング化によるCRMは大きく進化することになる。

統計情報とCRM情報の法的問題

■ 統計情報として販売

大手のスーパーや量販店のPOSデータは、流通POSデータサービス企業に対して、マーケティング情報を求める企業への分析情報として販売されている。

例えば、商品メーカーでは、新製品の立ち上がり動向分析や地域別販売動向分析、競合他社商品とのシェア分析など、卸売企業などは、市場動向を加味した品揃え提案、地域別・業態別売れ筋情報の把握、販売予測等のマーケティングへの情報活用がある。統計データとして集約されたPOS情報は、個人情報ではなく、販売されても問題ない。ただし、**考え難いが詳細データがそのまま販売されれば、個人情報保護法に抵触する。**

■ 個人顧客へのターゲット広告

CRM情報は顧客の購入履歴から「顧客のライフステージ」合わせて、商品提案がなされていく。例えば、人は、学生生活→就職→結婚→出産→育児→子供の独立→退職→老後生活といったライフステージが、購買履歴から推定できるのである。この家族属性の変化を推定し、最適な商品のDMを送ることで、顧客一人ひとりに対してOne to Oneマーケティングがなされるのである。

POSにおけるCRMの情報活用は、顧客自身にも情報収集の意識は少ないが、まさしく、個人情報である。ターゲット広告として活用するのであれば、**情報蓄積について、情報の収集内容、活用の目的など、顧客の同意が必要である。**

2. 閲覧履歴のライフログと法的問題

- Webをベースしたサービスは非常に高度化、消費者の多様化のニーズに応えるものである。Webでの行動記録は、どのようなWebページをアクセスしたのか、また、閲覧したコンテンツの内容はどのようなものか、サーチエンジンで検索した語句はどのような語句か、サイバーショッピングに訪れたWebサイトで購入した商品はどのようなものか、閲覧履歴(ウェブのアクセス記録、検索語句、訪問先URLや滞在時間、視聴者履歴等)が収集される。そして、きめ細かいユーザの情報が収集されることで、そのユーザにさまざまなサービス展開される。
- Webページのアクセス情報や閲覧記録、検索語句等は単独の情報としては個人の識別性がなく、個人情報とは言い難い。また、プライバシー侵害としても成立し難い。ただ、行動記録と位置情報が長期間蓄積され、個人が容易に推定されることになりかねない。事業者は、情報取扱いについての透明性を高め、情報取得の停止や利用停止が可能な配慮が必要である。

3. 行動ターゲティング広告の法的問題

- 行動ターゲティング広告が行われる場合に必要な情報には、
①インターネットでのWeb閲覧記録や、サーバーホッピング等のWebサイトからの購買記録等とユーザの趣味・嗜好を分析情報、②クッキー技術を用いて生成された識別情報、契約者固有ID、③GPS機能から得られる位置情報、携帯電話での基地局からの位置情報などがある。これらの情報からは、個人の識別情報はなく、個人情報とはならない[2]。
- DPI技術を用いた行動ターゲティング広告の場合には、通信プロバイダー(ISP)を通過するパケットの内容から分析されることになり、内容が個人情報及びプライバシー情報となりえることも考えられる。加えて、「通信の秘密保護」との関係で、電気通信事業法、憲法(第21条:通信の秘密)に抵触することも考慮しておくことが必要である。また、事前に通信当事者のとの明確な同意が必要である。約款やホームページ上の周知のみでは、有効な同意と認め難く、個別の契約が必要と思われる。
- 一方的で迷惑なメール広告は「特定電子メール送信適正化法」に、また、通信販売での同意のない広告や拒否のできないメール広告等は、「特定商取引法」に抵触することも考えられる。

4. 行動支援サービスの法的問題

■ 例えば、朝6時に起きて、自宅を7時に出発、9時には会社のつき、昼食は近くのコンビニエンスストアで弁当を購入、午後6時には会社と出て、本屋に立ち寄り、フィットネスクラブに行く、軽く居酒屋で飲み、電車で午後11時帰宅といった生活状況の情報が収集できる。この情報をもとに、「行動支援サービス」が実現される。自宅を7時に出発しなければ、ワーニングが発せられるし、通勤経路の電車で遅延や運休があれば、ただちに情報を提供してくれる。最短の迂回情報も提供されよう。

現在、位置情報をもとにした「行動支援型サービス」の代表的な事例として「iコンシェル」(NTTdocomo)がある。

■ 情報の収集方法は、行動記録や属性情報をもとに、ユーザの行動とともに、位置情報と組み合わせられてユーザをアシストしていく。仮にユーザの一日の行動記録を長期間蓄積し分析されれば、ユーザの生活態様が手に取るように分かることになる。ユーザ本人との契約にもとづき、情報が収集されているが、その内容はプライバシー情報そのものである。

■ 行動支援サービスが、ライフログ情報提供者が、サービスの受領者本人であり、契約者でもあることで、本人の同意を得ていることといえるが、①サービスの内容を提供する範囲での情報収集であること、②サービス契約が破棄されれば、すぐに情報を削除すること、③蓄積された情報を他の目的に活用したり、第三者提供しないことが遵守されなければならない。

4. 道路周辺情報映像提供の法的問題

■近年、公道から道路周辺画像を編集して提供する「インターネット道路周辺映像提供サービス」がある。代表的なサービスとして**グーグル社の「ストリートビュー」**がある。平成20年(2008)年8月か日本においても、サービス提供が開始され、2009年現在全国の主要都市12都市のほぼ全域がグーグルマップ上で公開されている。国内では、他に**「ロケーションビュー」(ロケーションビュー社)**、**「ウォークスルービデオシステム」(NTTレゾナント社)**などがある。

■道路周辺映像サービスは、一般公開され、①バリアフリーの整備状況確認、②個人による外出先の情報確認、③施設や店舗の案内、金融機関の担保調査、不動産会社の不動産取引情報等のビジネス活用、④インフラ施設管理(マンホール、電線、電柱管理等)、⑤観光振興、教育、消防・防災・救急等活動、⑥水道、道路管理、下水管理の行政サービス等多方面に活用されており、社会的意義は大きい[1]。

■ グーグル社の「ストリートビュー」サービスが開始して以後、プライバシーや肖像権侵害や防犯上の問題が大きいと指摘された。事実、**通行者の判別ができる写真**、**住宅街では表札(名札)が写っていたり**、**高い個所(地上約220cm)からの撮影であり**、**家の中ばかりでなく**、**干し物が写って場合もある**。また、**車庫の自動車や停車している車のナンバープレートも写っており**、**プライバシーの問題が大きい**。

■ 国会では、平成20年(2008)年11月に、衆議院総務委員会で、ストリートビューに関して質疑が行われた。地方自治体においても、各地の議会において、意見書が多数採択されている。また、福岡弁護士会から「ストリートビューサービスの中止を求める声明が発出されている。

■ 住居の外観、周辺道路状況のみであれば、原則として個人の識別情報がなく、個人情報には該当しないと考えられる。また、ナンバープレートの番号が写っていても、その番号から所有者個人を識別することが難しく、個人情報とも言い難い。この見地から、**現状では、個人情報やプライバシーの侵害にならないとされている**。

しかし、**判読可能な表札や車庫に入っている車のナンバープレートの撮影は、プライバシーの問題が発生する**。また、**私道内の撮影や学校内に入っの撮影は、プライバシーも問題のほか、不法侵入にもなりかねない**。

■ グーグル社は、人の顔や表札、車のナンバープレートのぼかしを入れるとともに、ユーザからの申告があれば、原則24時間内に削除等の対応をとっている状況にある。

5. デジタルサイネージでの法的問題

■ 街角の情報収集は、デジタルサイネージ(Digital Signage: 電子看板)の高度化により、**看板の周りにいる人を瞬時の読み取り、骨格、髪の毛から、性別・年齢層等の画像分析**することで、広告効果を測定し、看板をみている人の属性に応じて広告を配信できることになる。

例えば、街角情報を見ながら、若者女性が集まっているならば、通信ネットワークを使ってリアルタイムな操作をして、表示される広告内容を若者志向の化粧品に随時配信・変更し、集まる地域に即したリアルタイムのキャンペーンが配信可能となる。この時、必要となる情報は集まる一人ひとりの属性を集めた「**群集特性**」である。

■ **広告を見ていると撮影されているとは、ほとんどが気づいていない状況での隠れた場所からの撮影は、防犯上の撮影でない限り、プライバシーや倫理の問題が発生する。**

実際に、2010年の6月から運用されているJR東日本での「デジタルサイネージ」では、プライバシー保護のためにデータ保存をしておらず、「**広告調査中**」「**性別、年代を調査するため撮影をしています**」の表示がなされている。

ライフログの法的問題への対応



1. 法的問題への対応と社会的責任

サービス提供者としてのライフログの法的問題への対応に、最も重要なことは三つある。

一つは、個人の「**識別性の排除**」である。即ち「**匿名化**」である。ライフログを活用したサービスのほとんどは、個人情報が必要としないのである。ユーザの閲覧記録や購買記録、位置情報などを個人情報となるために「**契約者情報(住所、氏名、生年月日等の記載情報)**」とが、結合されないようなシステム作りが前提である。サービス提供に不必要な情報をもたない、個人の抽象化技術も重要である。

二つは、「**透明性の確保**」である。ユーザに対して、情報サービスの内容とその情報の収集の手段を明確化すること、ユーザにはその情報の利活用について通知し、必要なときには、いつでも確認と訂正・削除ができる状態にしておくことである。また、サービス契約が破棄されれば、速やかに契約者の情報を廃棄することも重要である。

三つは、事業者自らが、安心して安全なサービスシステムであることを「**宣言**」し、ユーザから信頼されるシステムであるための、継続的努力が必要である。例えば、「**プライバシーポリシーの策定**」、とともに「**プライバシー保護のガイドライン策定**」、「**業界ガイドラインの策定**」など、その遵守とともに、このような「**社会情報システム**」の提供者として、**企業の社会的責任(CSR)**を果たすとともに、**業界責任を果たす**ことである。

ライフログの法的問題への対策

サービス事業者は、実施すべき対策として以下がある。

- ①ライフログと契約者情報の完全な**システム分離**,
- ②ライフログサービスに必要な内容の**最低限のデータベース化**,
- ③ライフログデータの取扱者の限定,
- ④サービス実施のための**抽象化情報技術への対応**(非個人情報化技術や集合匿名化技術等),
- ⑤業界ガイドラインの策定・運用のガイドラインの策定,
- ⑥収集情報**透明化と選択権**の確保,
- ⑦**オプトアウトの限界**によるオプトインの実施,
- ⑧新規サービス開発計画の段階で**法的脆弱性分析**の実施,
- ⑨定期的な外部監査(システム監査や情報セキュリティ監査等)の受診,
- ⑩新たな**法改正**など,
法的問題への対応が重要となる。

おわりに

ライフログサービス事業はまだまだ、未成熟の段階である。ライフログ技術の高度化やニーズの多様化が不透明であるがゆえに、どうしても、ニーズの多様化を予測して、この情報があるのではないかと、この情報とこの情報を連結させることで、もっと面白い(有意義な)サービスが提供できるのではないかという思惑で、現在は不要である情報を、無意味にデータベース化していこうとする。結果的には、個人情報やプライバシーを侵害する環境ができあがってくる。

ライフログ活用には、社会的意義の大きいものもある。法的問題が大きい故に情報活用を萎縮させてはならない。事業者は、情報の取扱を透明化するとともに、法的脆弱性をサービス開発の時点から十分に調査・分析し、情報システムの中に組み入れるとともに、もし、問題が発生すれば、情報取得の停止や利用の停止、情報の削除等の対応を迅速に実施できる体制も確立させておくことが重要である。

参考資料

諸外国の対応 ～米国, 欧州, 英国～



【米国】

■2007年にFTC(米国連邦取引委員会)が、事業者の自主的なガイドライン作成にあたっての原則となる「オンライン行動ターティング広告に関するプライバシー保護指針」を公表

①透明性と消費者によるコントロールの確保:

Webサイト利用者に対して、行動ターゲティングの行うために情報収集がされていることを明確に知らせ、その目的のための情報収集を認めるかどうかの選択の自由を付与

②合理的なセキュリティの確保と限定的データ保存:

情報保存期間は正当な業務又は司法機関のために必要な期間に限定

③プライバシー方針の実質的な変更前における明示的な同意の表明の取得

④機密データを行動広告に向けて利用する前における明示的な同意の表明の取得:

医療・健康情報、子供、財政といった機密情報を行動ターゲティング広告のために利用する場合には、消費者から明示的な同意の表明のもとで取得すること。

■2008年4月にCTIA(携帯電話事業団体)「位置情報サービスガイドライン」

①利用者通知、②利用者のからの同意、③セーブガード

■2008年12月にNAI(オンライン広告事業者団体)「オンライン行動広告に関する自主規制行為規範」

【欧州:EC】

■ 2009年11月に、クッキー及び個人情報の利用について事前に分かりやすい説明でおこなうことを義務付けを行うこと

■個人の識別可能な情報については、指令95/46/EC(個人データ処理及びデータの自由な移動に関する個人の保護に関する指令)及び指令2002/58/EC(電子通信分野における個人データ処理及びプライバシー保護に関する指令)が適用

■2007年6月から、第29条データ保護作業部会において、指令95/6/ECに基づき、検索サービス提供事業者の検索ログ保存期間に関して審議、2009年2月、個人特定可能なIPアドレスがるログファイルの保存期間を6ヶ月とすることで米国主要検索事業者と合意

【OECD】

■2008年6月18日採択のソウル閣僚会議において、「センサーベースネットワークを含む、新たなインターネット技術、アプリケーション及びサービスの経済的、社会的及び文化的影響をOECDにおいて分析すること」を要請

【英国】

■2009年の業界団体がInternet Advertising Bureau (IBA)がオンライン上の行動 ターゲティング広告に関する行動原則「Good Practice Principles for Online Behavioural Advertising」を公表。原則は、情報提供の原則、選択の原則、教育の原則、機微な情報区分の内容となっている。

注

[注1] 東京地裁昭和39年9月28日判決「宴のあと」事件

[注2] 最高裁平成15年9月12日第2小法廷判決では、学籍番号、氏名、住所及び電話番号については、「秘匿されるべき必要性が必ず高いものではない」としつつ、自己の欲しない他者に開示されたくない情報であり、「プライバシーに係る情報として法的保護の対象となる」としている。

[注3] DPI(Deep Packet Inspection)

Packet検査技術の一つである。これまで、ネットワークからの外部侵入を防ぐためにACL (Access Control List) というパケットフィルタリング技術で、プロトコルの種別で「通過」「拒否」を判断していた。インターネットの高度普及で、HTTP上で実行されるようになり、「プロトコルの内容」でパケットを検査するDPI技術が開発された。DPIにより、URLやメッセージに含まれる内容、パケットの振る舞いまで検査が可能になった。これにより、HTTPを利用して侵入するウイルス検出は、情報漏洩を検査できるような高度なセキュリティが可能になった。

参考文献

参考文献

- [1] 総務省 「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会 ー第一次提言(案)」 平成21年8月 2009
- [2] 総務省 「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会 ー第二次提言(案)」 平成22年5月 2010
- [3] 「蓄積データは万能にらずポイントカード依存症から脱せよ」 日経ストラテジー 2008年4月
- [4] 堀部政男編著 「プライバシー・個人情報保護の新課題」 商事法務 2010
- [5] NTTドコモ 「情報大航海プロジェクト マイ・ライフ・アシストサービス概要」平成平成20年1月30日 2009
http://www.meti.go.jp/policy/it_policy/GIS/080130/3-1nttdocomo0130.pdf
- [6] NTTドコモ 「iコンシェルでできること」
<http://www.nttdocomo.co.jp/service/customize/iconcier/function/#p01>
- [7] 堀部正男, 宇賀克也編集 「地理空間情報の活用とプライバシー保護」 地理科学研究会 2009