資料１

海外における位置情報の取扱いについて

平成２６年３月１８日

海外における位置情報に係る規律（米国）

✓ 米国においては、**個人情報・プライバシーに関する分野横断的な法律は存在せず、分野毎の個別法と自主規制が基本**となっている。

✓ **電気通信分野**においては、通信法（Communications Act）第222条において顧客情報のプライバシーを規定。電気通信事業者は、**顧客に関する専属的な網情報（CPNI）に関して、集計顧客情報**（集計データで、個人顧客の身元及び特徴が除去されているもの）**については、通信目的外での利用や公開を許容**されている。

✓ 自主規制として、携帯電話業界団体CTIAが、**GPS位置情報等を利用した位置情報サービス**に関するベスト・プラクティス・ガイドラインを2010年3月に採択している。その二大原則は以下の通りであり、**位置情報サービス提供者は、ユーザーに通告し、同意を求めること**とされている。

- ユーザーに位置情報がどう利用されるか、開示されるか、保護されるかについて、通知し、ユーザーが位置情報を利用する決断を下す際の情報を提供することで、位置情報に関するコントロールを与える。
- ユーザーに位置情報の利用、開示について同意を求め、いつでも同意を撤回する権利を与える。

なお、**集計データ及び匿名データはガイドラインの対象外**となっている。

✓ FTCは**モバイル端末上の利用者情報の取扱い**について、スタッフレポートとして「モバイル・プライバシーディスクロージャーズ：透明性の確保による信頼の構築」を2013年2月に公表しており、**OS事業者、アプリ開発者双方に対し、位置情報についてはセンシティブ情報として、取得前に消費者に通知し、明白な同意をとること**が提言されている。

✓ また、近時**Wi－Fi等を使った位置情報サービスのプライバシーについて議論**がなされており、本年2月19日には、FTCにおいて「Spring Privacy Series: Mobile Device Tracking」と題するセミナーを開催。（詳細次頁）。

Wi－Fi位置情報に関する米国での議論の状況

✓ FTCセミナーにおける議論

FTCは、モバイル端末の位置情報の活用や消費者プライバシーへの影響等について把握するため、セミナーを開催し、位置情報サービス提供会社、データ分析会社、市民系団体等によるパネル討議を実施。参加者の主なコメントは以下のとおり。

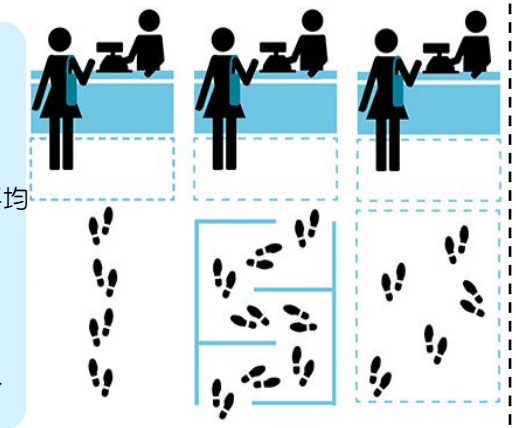
・消費者の行動分析を通じて、会計時の待ち時間減少や商品選別・商品棚配置の最適化等消費者の利便性を高めることが可能となる。

・消費者の信頼は重要であるが、一定の場合には消費者への事前通知が不要な場合も存在する。（例：不特定のデータを追跡することで作成されたヒートマップ）

・GPSやWi-Fi、Bluetooth等の位置追跡技術により、店舗付近にいる利用者端末へのクーポン配信等が可能になる一方、利用者に気づかれない情報収集の是非、オプトインまたはオプトアウトの選択肢、匿名による情報管理、情報の保存期間といった懸念が存在。

・行動追跡について通知した上で、客がこれを許可するか否か選択できるようにすべき。

位置情報を活用したサービスイメージの一例



上記の項目を分析し、会計時の待ち時間減少につなげる

✓ フューチャー・オブ・プライバシー・フォーラム（FPF）の取組

米国のシンクタンクであるFPFは、位置分析を行う企業が提供するサービスに対する強制力を持った自主規制の枠組みとして、「移動端末の位置情報分析に関する行動規範」を作成。同行動規範に賛同する位置分析企業とともに、MACアドレスにより企業に行動を追跡されたくない消費者に一括でオプトアウトさせるウェブサイト（www.smartstoreprivacy.org）を立ち上げている。

・あるエリアでの位置情報の収集および利用について、エリア内の目立つ場所に掲載し、ウェブサイト上に取得する情報や提供するサービス等について記載した詳細なプライバシーの通知を提供すること。（取得される情報が、①個別の端末・利用者に紐付かない、または②直ちに集計され個別の情報が保持されない場合は不要）

・消費者の同意がない場合、取得したMACアドレスは即座に非特定化または非識別化すること。

≪非特定情報の定義≫①個人への紐付けを不可能とする手段を講じること。（例）MACアドレスのハッシュ化や個人識別情報の削除
②非特定化された状態での情報の維持を公的に約束すること。
③提供先がデータを個人識別に利用することを契約上禁止すること。
≪非識別情報の定義≫①非識別化を確保する合理的な手段を講じること。（例）集合情報、データへのノイズ付加、統計的サンプリング
②データの再識別化を試みないことを公的に約束すること。
③提供先がデータを再識別化することを契約上禁止すること。

・モバイル端末の位置情報の分析についてオプトアウトの機会を提供すること。（取得される情報が、①個別の端末・利用者に紐付かない、または②直ちに集計され個別の情報が保持されない場合は不要）

・個別の端末情報は保存期間を定めて保持すること。

海外における位置情報に係る規律（英国）

欧州レベル

- ✓ EUの第29条作業部会は、2011年5月に、スマートフォンやタブレットなどのスマートモバイルデバイス上での位置情報サービスの使用についての意見を公表している。この意見の中では**欧州データ保護指令（Directive 95/46/EC）が、携帯電話の三角測量や、Wi－FiアクセスポイントとGPSを利用するなどによって生成された位置情報に対して、適用される**ことを明確にしている。
- ✓ なお、同指令前文第26条において、**データ主体がもはや識別できない**(the data subject is no longer identifiable)**ような方法で匿名化されたデータについてはデータ保護の原則は適用すべきでない**とされている。
- ✓ **電気通信分野**については、電子通信プライバシー指令（2002/58/EC）において、**トラフィックデータ**について、通信に不必要になった場合に、消去又は**利用者を識別できないような状態**にしなければならないと規定されており（第6条）、それを超えるマーケティング目的の利用や付加価値サービスの提供については、利用者の同意が必要とされている。**位置情報（トラフィックデータを除く。）**については、付加価値サービスの提供について**利用者の同意**を得た場合のほか、当該データが**匿名化**された場合においても処理が可能とされている。**利用者の同意を取得する前には、処理される位置情報の種類、処理の目的及び期間、第三者に提供されるか否かについて通知しなければならない。また、利用者は同意をいつでも取り消すことができること**とされている（第9条）。

英国内

- ✓ データ保護法（Data Protection Act 1998）の下、**識別できる生存する個人に関する位置情報は、「個人データ」に該当**する。
- ✓ 電気通信分野については、プライバシーと電子通信に関する規制（Privacy and Electronic Communications Regulations 2003）において、電子通信プライバシー指令と同旨が定められている。
- ✓ なお、英国においては、GPS情報、携帯電話端末が取得した基地局情報、携帯電話端末が取得したWi－Fi情報のいずれも、位置情報として扱われ、個人データに該当しうると考えられている。
- ✓ 英国情報コミッショナーは、**ヨーロッパのデータ保護当局として初めて匿名化に関するガイドライン**を示している。（詳細次頁）

英国ICOの匿名化ガイドライン（2012年11月）

匿名化に対する本ガイドラインの基本的な認識及び目的

- ✓ 匿名化は個人のプライバシーを保護するとともに、データ保護法が推進する「プライバシーバイデザイン」の実践例。
- ✓ 個人データの効果的な匿名化は可能であり、望ましく、社会が個人のプライバシーを保護しながら豊富なデータ源を入手できるように手助けとなることを提示。

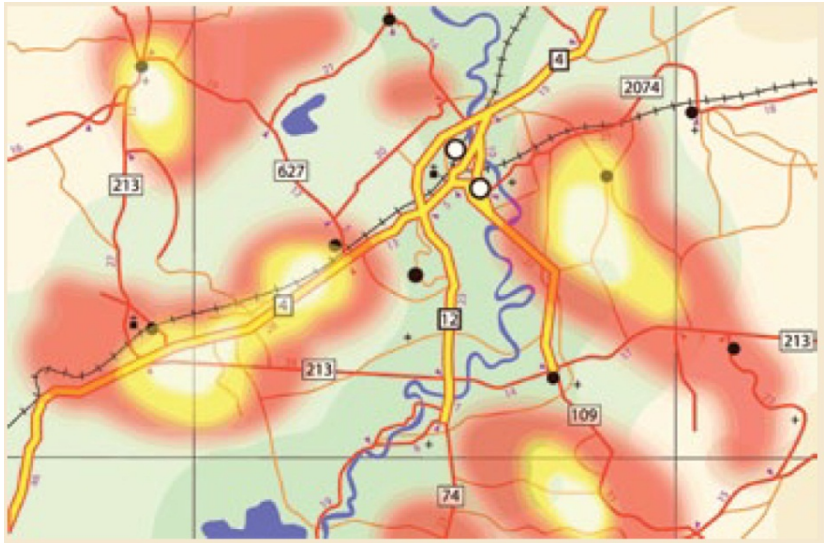
再識別化のリスクについて

- ✓ データ連結を通じた再識別化のリスクは基本的に予知できない（何のデータが将来公開されるか等を評価することは不可能）。
- ✓ 再識別化の結果が、個人が損害、苦悩、経済的損失を被った状態にさらされるため重大となりうるケースでは、組織は以下を行うべき。
  - ・データの開示について、データ主体（本人）に生じ得る結果を説明し、同意を求める。
  - ・より厳密な形態のリスク分析及び匿名化を採用する。

個人データと空間的情報

- ✓ データ保護法には、空間的情報（GPSデータ等）の取扱いに関するルールは定められていないが、一部の状況によっては、これらの情報は個人データに相当する。
- ✓ 空間的情報が合法的な目的のために公表されている場合、個人のプライバシーの保護とのバランスをとることができる最大限の詳細度を達成することを目指すべきであり、プライバシー影響評価（PIA）は当該目標の達成のために実践すべき。
- ✓ 空間的情報のために採用すべき（匿名化）方法は、保有するデータセットの規模によっても異なる。一部のケースでは、識別化のリスクを軽減するために、空間的情報を処理して、一定の情報を除去または「曖昧に」する必要がある。
- ✓ 空間的情報を公表する際にプライバシーリスクを軽減する原則として以下が挙げられている。
  - ・地図のエリアを拡大して、より多くの土地建物と居住者をカバーする。
  - ・公表の頻度または対象期間を縮小して、より多くの出来事を取り上げることによって、最近のケースの特定がより困難になり、その出来事の発生日時等の追加のデータが明らかにならない。
  - ・特定の場所または人についての詳細な情報の推測を可能にすることなく、ヒートマップなど概況を示すフォーマットを使用する。
  - ・住居レベルに関する空間的情報の公表を避ける（当該情報の公表には個人データの処理を伴うことがあるため）。

犯罪地図作製のためのヒートマッピング（色分け地図作成）手法



匿名データの開示形態について

- ✓ 匿名データの使用者が直面する問題は、一方では、彼らは自身の使用目的のために豊富で十分に利用できるデータを欲しているが、もう一方では、再識別化が発生しないことを望んでいる。
- ✓ 匿名データを広く社会全体に公表することとアクセス制限を区別することが重要（集計的かつ連結不可能なデータは公表しやすい一方、アクセス制限を用いると、データの更なる開示または使用に対する制限がなく、かつ、安全性が維持される。）。