

IoTに係るプライバシー上の課題等に関する諸外国の状況について

2016年5月12日

I . IoTに係るプライバシー上の課題に関する諸外国の状況

1. 諸外国の動向

- 諸外国では、IoTとプライバシーを対象とした文書を発行している。
- 各文書では、IoTによって取得されるデータはパーソナルデータとして取り扱うべきであるとして整理した上で、消費者からの同意を得ることなくデータ取得がなされてしまうことが起き得ることを指摘し、そのような行為への対応方法を検討することを求めている。

発行年	発行主体	タイトル	概要
2013年11月	アメリカ FTC	<ul style="list-style-type: none"> • Internet of Things – Privacy and Security in a Connected World (シンポジウム) 	<ul style="list-style-type: none"> • IoTに関するプライバシーやセキュリティに関する課題について、ステークホルダーがどのように対応していくべきかについての議論を行ったシンポジウム。 • シンポジウムを受けてのレポートが2015年1月に発行。
2014年9月	EU 29条作業部会	<ul style="list-style-type: none"> • Opinion 8/2014 on the on Recent Developments on the Internet of Things 	<ul style="list-style-type: none"> • IoTに関わるステークホルダーはEUの個人データ保護指令及び、e-プライバシー指令に従う必要がある。 • IoTで利用されるセンサーについては、消費者の明示的な同意がない限り、データ取得をしてはならないと整理している。
2014年10月	第36回データ 保護&プライバ シー・コミッショ ナー国際会議	<ul style="list-style-type: none"> • Internet of Thingsに関するモーリシャス宣言 	<ul style="list-style-type: none"> • IoT機器によって取得されたデータはパーソナルデータとして取り扱うべきであるとして整理。 • その上で、機器を提供するものはどのようなデータを、どのような目的で取得し、利用するのか、またどの程度の期間保持するのかを明確にすることを求めている。 • また、IoTに関わる全ての関係者は、IoTの可能性について建設的な議論をしていくことを求めている。
2015年1月	アメリカ FTC	<ul style="list-style-type: none"> • Internet of Things – Privacy and Security in a Connected World (FTC Staff Report) 	<ul style="list-style-type: none"> • IoTをインターネットに接続し、情報を保存し、互いに通信するような機器やセンサーと定義した上で、その便益とリスク(プライバシーリスクとセキュリティリスク)を整理 • 現状ではIoTに特化した立法は不要として整理。

2. アメリカ IoTに関する課題と法制度の整理 (1) 概要

- アメリカではIoTに関するデータの権利について、消費者の情報は消費者自身に権利があることを規定している。
- 利活用に際しては基本的に消費者の同意が必要となるが、IoTによって同意取得が難しくなることは認識されており、なんらかの対応が行われる可能性がある。産業分野別には、一部消費者の同意無く利用できるものがある。

課題・検討事項	内容	法制度・レポート
データの権利に関する事項	<ul style="list-style-type: none"> ● データの権利について、消費者は事業者がどのような個人情報を収集し、それらをどのように利用するかについてコントロールする権利を有するとされている。 ● そのため、データの権利については消費者が有することとなる。 	<ul style="list-style-type: none"> ● 消費者プライバシー権利章典
データ提供者の同意	<ul style="list-style-type: none"> ● データの収集・利用に際しては同意を取得することが基本的に必須。 ● HEMSについて、委託モデルまたは規定された目的の範囲内であれば消費者の同意無く提供可能。 ● IoTではインターフェース上の問題から全てのデータ収集において同意を得ることが困難であり、元々の取引や消費者との関係性において矛盾しない実務について収集・利用される場合には、事前の同意を強制しないと整理。 	<ul style="list-style-type: none"> ● DOE “Privacy Voluntary Code of Conduct” 等 ● FTC “Internet of Things - Privacy & Security in a Connected World”
データの管理に関する事項	<ul style="list-style-type: none"> ● データの安全管理措置については、Security by Designを考慮すること。 	<ul style="list-style-type: none"> ● DOE “Privacy Voluntary Code of Conduct” ● FTC “Internet of Things - Privacy & Security in a Connected World” 等
データの加工に関する事項	<ul style="list-style-type: none"> ● データを匿名加工することによって提供することが可能になる。しかし匿名加工の手法や基準については具体的な定めがない。 ● HEMSについては、集約データ (Aggregated Data) について、15/15ルールという手法が一部の州で利用されている。 	<ul style="list-style-type: none"> ● 4 Code of Colorado Regulations (CCR) 723-3-PART 3 RULES REGULATING ELECTRIC UTILITIES

2. アメリカ IoTに関する課題と法制度の整理 (2) 事例－HEMS

- HEMSについては連邦のガイドラインを参考に、各州が州法によってプライバシールールを規定。
 - 提供先がContracted Agentである場合には、消費者の同意無しでデータを提供可能とされている。
 - またデータの利用目的が一次目的にあてはまる場合も、消費者の同意無しでデータを提供可能とされている。
-
- HEMSについては、連邦エネルギー省によって、Privacy Voluntary Code of Conduct (VCC) というガイドラインが定められており、これを基準にして各州でプライバシールールが定められている。
 - 連邦政府には各州の公益事業を規制する権利がないため、ベストプラクティスを示した強制力の無いガイドライン
 - データの取扱いについては、以下の2つの基準が挙げられている。
 - ① サービスがアグリゲータのContracted Agentであるかどうか
 - ② サービスのデータ利用目的が、Primary Purpose (一次目的) か Secondary Purpose (二次目的) か
 - Contracted Agentは、VCCにおいて、電力会社等のアグリゲータと契約関係にあり、かつ、一次目的または二次目的でサービス提供を支援する事業者と定義しており、この場合は消費者の同意無しで提供可能 (日本の委託モデル類似)。
 - Contracted Agentでない場合も、一次目的であれば、第三者に対して消費者の同意無しでデータを提供可能。

目的	内容
Primary Purpose (一次目的)	顧客情報や、電力利用データについて、以下の利用を目的としている場合 <ul style="list-style-type: none"> ・ 顧客の選択したサービスの提供、サービスの維持・継続 ・ 顧客の期待に反しない範囲での第三者とのデータ共有
Secondary Purpose (二次目的)	一次目的とは大きく異なった目的で、アグリゲータもしくはContracted Agentによって提供されているサービスで掲げられている目的としている場合

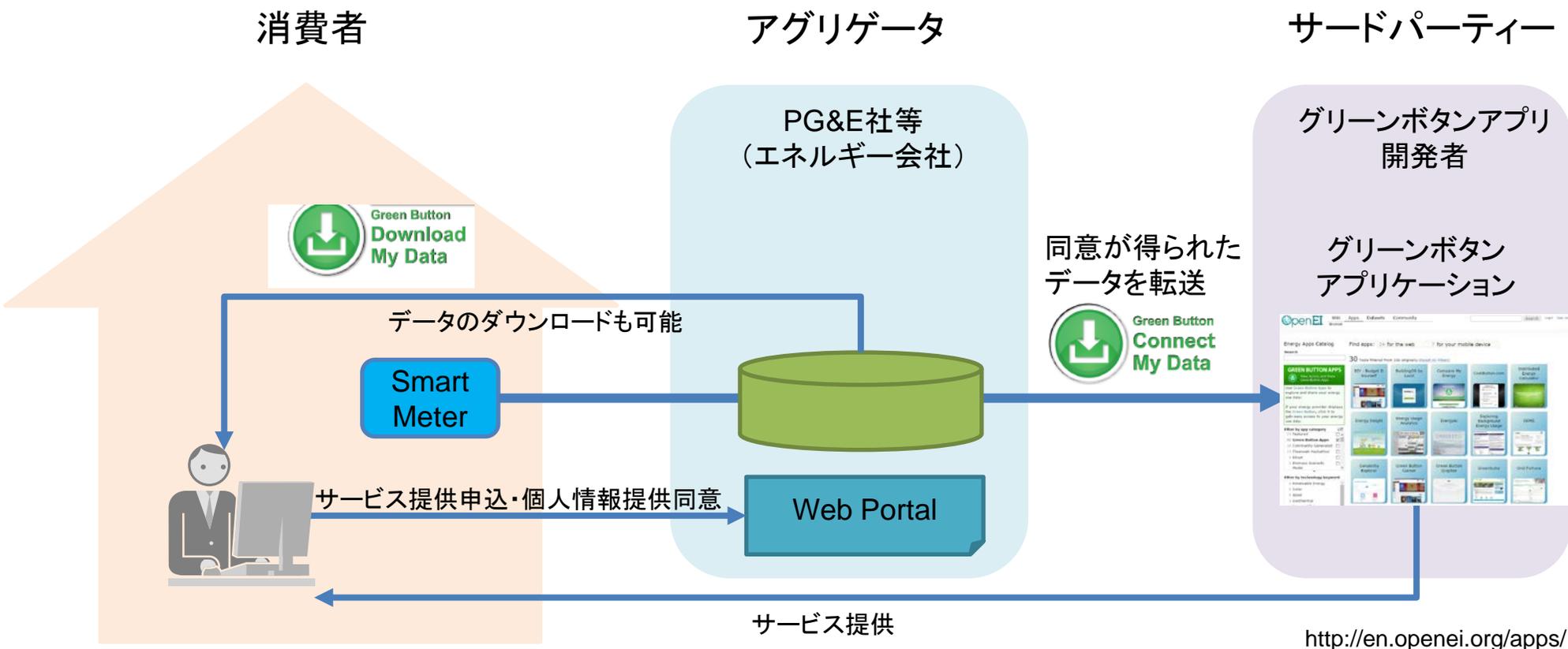
目的	Contracted Agent	第三者
Primary Purpose (一次目的)	消費者の同意無しで提供可能	消費者の同意無しで提供可能
Secondary Purpose (二次目的)	消費者の同意無しで提供可能	消費者からの同意が必要

2. アメリカ IoTに関する課題と法制度の整理 (2) 事例－HEMS

- HEMSについて、第三者に対してエネルギーデータを提供する仕組みとして、Green Buttonの仕組みを整備。
 - 消費者の同意を得ることで、第三者が電力会社から電力利用データを受け取り、当該データを利用したサービスを提供できる仕組み。
 - データ形式が統一されているため、サービス提供者は各州にサービスの横展開が可能。
-
- オバマ大統領が2009年1月21日に発表したオープンガバメントに関する三大基本原則である”Transparency and Open Government”に基づいて始まった”Open Government Initiative”によって、取り組み開始。
 - 取組には起業家によるデータ活用を促進することが含まれており、その中で”MyData”ダウンロードサービスと呼ばれる個人情報安全、適時、電子的にやりとりするための技術的な枠組みが提唱されている。
 - 医療分野 …Blue Button
 - エネルギー分野 …Green Button
 - 2012年にPG&E社とSDG&E社が対応。2014年夏時点で全米で35社が導入を約束。
 - 2015年時点でも全米で利用されているわけではない。
 - あくまで同意による利用のため、カリフォルニア州のPG&E社の場合、2015年12月時点で加入者の0.1%とされる。
 - 消費者がアグリゲータの用意するWebポータルにアクセスして、同意することで、電力利用データを第三者に提供する。方法としては下記の2通り。
 - ① サービスに同意した時点以降の電力利用データを自動的に送る「Connect My Data」。
 - ② 同意の時点までの電力利用データをダウンロードして渡す「Download My Data」。

参考：Green Buttonの仕組み

- エネルギーデータについて、消費者の同意のもとに収集して、第三者に提供。
- 第三者はエネルギーデータを活用して、エンドユーザーに対してサービスの提供を実施。
- 2016年2月末時点でアプリの数としては30個。電力データの比較等のアプリケーションを利用可能。



3. フランス IoTに関する課題と法制度の整理 (1)概要

- フランスではIoTに関するデータの権利について、消費者の情報は消費者自身に権利があることを規定している。
- 利活用に際しては基本的に消費者の同意が必要である。
- 匿名化は他のデータセットとの照合によっても個人の再識別化を不可能な不可逆的な技術を使用すべきとされている。

課題・検討事項	内容	法制度・レポート
データの権利に関する事項	<ul style="list-style-type: none"> • あらゆる個人は、本法に定められた条件の下で、自らに関するデータの用途を決定かつチェックする権利を持つとされている。 • そのため、データの権利については消費者が有することとなる。 	<ul style="list-style-type: none"> • デジタル経済法第26条
データ提供者の同意	<ul style="list-style-type: none"> • データの収集・利用に関する同意取得について、情報処理と自由に関する法律において、同意は必須とされている。ユーザーに十分に情報が提供されていることが条件とされている。 • データの委託の場合、同意取得は必要ないが、データ処理の主体は、データが代理者により処理される場合は、技術的セキュリティ措置及び組織上の措置に従って、十分な保障を与え得る代理者を選択せねばならない。第三者提供に関しては、同意取得が必要とされている。 	<ul style="list-style-type: none"> • 情報処理と自由に関する法律
データの管理に関する事項	<ul style="list-style-type: none"> • 医療データなどの機密データとそれ以外のデータでは取扱に大きな違いがある。 • 「データ処理の主体は個人データ保護のための適切な技術・組織上の措置を実装」せねばならず、「データ処理の主体は、データが代理者により処理される場合は、技術的セキュリティ措置及び組織上の措置に従って、十分な保障を与え得る代理者を選択せねばならない」と定めている。 	<ul style="list-style-type: none"> • 情報処理と自由に関する法律
データの加工に関する事項	<ul style="list-style-type: none"> • - 	<ul style="list-style-type: none"> • -

3. フランス IoTに関する課題と法制度の整理 (2) 事例－自動車

- フランスでは、高級車のリースをしている事業者で、CNILから摘発された事例がある。
 - フランスではコネクティッド・カーに関する規制、ガイドラインは公表されていないが、EUレベルでは欧州自動車工業会が、自主的なガイドラインを公表している。
-
- フランスでは、高級車のリースをしている「LOC CAR DREAM」社がCNILから制裁(5,000ユーロの罰金)を受けた事例
 - CNILへの届出無しにリースしている車に位置情報特定システムを設置。顧客はオフにすることが出来ない仕様。
 - システムは常時位置データ(主に日時・場所データ)を記録。
 - ユーザに対してシステムの存在は口頭では知らされていた模様だが確かではない。
 - 同社のDBへのアクセスには、ハンドルネームと12桁のパスワードが必要だったが、導入以来、2年間一度も変更されていなかった。
 - なお参考として、EUレベルではあるが、コネクティッドカーに関して、欧州自動車工業会(ACEA)が、2015年9月に「Principles of data protection in relation to connected vehicles and services(コネクティッド・ビークルとサービスに関するデータ保護原則)」が公表されている。

5つの原則	内容
①透明性確保	<ul style="list-style-type: none"> ● 処理の対象となる個人データあるいは個人データの категория、データ処理の目的、及び、データを共有するかもしれないサードパーティやサードパーティの категория、データ処理の主体の身元のそれぞれについての情報を提供
②顧客の選択の尊重	<ul style="list-style-type: none"> ● ユーザーが個人データを共有するかどうか選択できるよう配慮 ● ユーザーには、位置特定システムをオフにする可能性を与える。ただし、契約上の義務や(緊急時の通報など)法的義務の場合は例外とする
③データ保護への配慮	<ul style="list-style-type: none"> ● 新たな製品、サービス、プロセスを設計・開発・考案する際に、データ保護義務を考慮に入れる。 ● データ保護確保のために、新製品の市場への投入の前に、データ保護に関するインパクト調査を行う
④データ・セキュリティ確保	<ul style="list-style-type: none"> ● データの事故、あるいは違法行為による破壊、喪失、改竄、漏洩に対して、ユーザーのデータを保護するため、技術、セキュリティ及び組織上の適切な措置を実装する
⑤適切なやり方による個人データ処理	<ul style="list-style-type: none"> ● データ処理の目的に応じた適切で過剰でない個人データだけを処理 ● データの匿名化、偽名化、非識別化を個人データ保護のための重要な手段だと認識

4. ドイツ IoTに関する課題と法制度の整理 (1)概要

- ドイツではIoTに関するデータの権利について、消費者の情報は消費者自身に権利があることを規定している。利活用には基本的に消費者の同意が必要である。
- スマートメーターについて、法律で明記された目的であれば、同意無しに収集・利用しても良いという判断がある。

課題・検討事項	内容	法制度・レポート
データの権利に関する事項	<ul style="list-style-type: none"> ● 個人情報の提出および加工に関する決定は、すべての個人が独立に決めなければならない。そのため、データの権利については個人にあると考えられる。 ● 自動車についても別途規定があるが、これも自動車の所有者、運転者に情報の自己決定権があると整理されている。 	<ul style="list-style-type: none"> ● 連邦データ保護法 ● 連邦および各州のデータ保護監督官と自動車産業連盟の共同宣言
データ提供者の同意	<ul style="list-style-type: none"> ● データの収集・利用に際しては、本人の同意が必須である。 ● スマートメーターに関して法律に明記されたエネルギー経済の目的に必要な内容に限り、消費者の明確な同意無しにデータ収集と利用を行っても良いとされる。 	<ul style="list-style-type: none"> ● 連邦データ保護法 ● 連邦および各州のデータ保護監督官による要求
データの管理に関する事項	<ul style="list-style-type: none"> ● データの管理についてはドイツの連邦データ保護法が適用される。 	<ul style="list-style-type: none"> ● 連邦データ保護法
データの加工に関する事項	<ul style="list-style-type: none"> ● データの加工に際しては、予め本人の同意を得ることが必須である。 ● IoTデータの匿名化については現時点では規定が行われていない。 	<ul style="list-style-type: none"> ● 連邦データ保護法

4. ドイツ IoTに関する課題と法制度の整理 (2) 事例－自動車①

- IoTに関して、ドイツ各州のデータ保護専門官と自動車産業連盟が共同声明を発表。
 - 自動車で生成されるデータは、当該自動車を保有する個人のものであると位置づけ、当該データの取扱いについて原則を規定。
- コネクティッドカーに関して連邦および各州のデータ保護専門官と自動車産業連盟(Verband der Automobilindustrie, VDA)は2016年1月26日に共同声明を出し、以下のデータ保護法に関連する諸点について特別に留意することを合意。

主な項目	内容
①データの個人性	<ul style="list-style-type: none">● 車両を利用することによって生成されるデータは、車台番号やナンバープレートと併用することによって、連邦データ保護法の規定する意味において個人情報と判断され得る。
②データ取得及びデータ加工の妥当性	<ul style="list-style-type: none">● 基本的に同意を必要とする。● 原則として、データ加工に関するもっとも重要な情報に関しては、一般に理解できる形で、メーカーが用意する車内資料の形で後々まで読めるように保管する必要がある。
③データの開示	<ul style="list-style-type: none">● 本人が関与するデータに関しては、メーカー側は無料で情報開示に応じる義務がある。● 所有者側は、データ保存システムの構造に関する総合的な責任に基づくだけではメーカー側に対してデータ保護法に基づく情報開示義務は発生しない。● データの読み出しに有料の専門家の手を借りることが必要な場合、所有者本人に対しては無料でなくてはならない。
④データの権限	<ul style="list-style-type: none">● データ権限に関して、車両ユーザーは、個人に関連する情報の加工や利用に関して、さまざまなオプションの中から自分で決定できるようになっていなければならない。● データ消去可能性の制限は法的な義務または当該データが保証サービスや製造責任に重要な場合、またはそのデータを利用することが安全な車両運行に必要な時に限られるべき。● 座席設定などの快適さのデータ、ラジオのチャンネル、ナビデータ、メールやSMSのアクセス・データなど、ユーザー独自の情報は、本人がいつでも変更でき、または解除することができなければならない。

4. ドイツ IoTに関する課題と法制度の整理 (2) 事例－自動車②

- ドイツでは、自動車会社(BMW社)が販売した自動車の情報を必要以上に取得していたことについて非難されている。
 - データ転送に関する同意が自動車購入契約書に含まれており、抱き合わせの形になっていたことも批判の一因。
-
- ドイツでは、自動車会社が利用者からの同意無くデータを取得していた例について問題となっている。
 - 2015年11月24日に、国際自動車クラブ連盟(FIA)とドイツ自動車クラブ(ADAC)が実施したデータ取得に関する調査結果で、BMWの3シリーズおよびi3において、必要以上と判断されるべきデータがメーカーに送信されていたことが判明。
 - BMW社は、データは「純粋に技術データ」であり、「改修場所の認知と車両最適化」のためにのみ利用されるとし、「第三者への転送は実施されておらず、必要な情報を整理した後には削除される」とした。
 - しかし別の箇所では「契約の実施上必要なサービスプロバイダ」にはドライブデータを転送していることに言及。
 - BMW社は「集積されたデータによって車両の移動プロフィールを作成することは不可能」と強調しているが、実際には直近100ヶ所の駐車場所が分かるため、十分に移動圏内を特定することは可能と指摘されている。
 - 車両購入に際して、購入契約書に、データ転送に関する項目を設けており、購入することによって、抱き合わせ的にデータ転送を承諾しなければならない。
 - 2016年3月時点では問題が解決したわけではない。
 - 取得されていた具体的なデータ項目は以下の通り。

主な項目	ガソリン車(3シリーズ)	電気自動車(i3)
運転情報	<ul style="list-style-type: none"> ● 各ドライブモードの利用時間、急ブレーキによるシートベルトロックの回数および時間、走行回数および走行距離 	<ul style="list-style-type: none"> ● ドライブモード、充電関連情報(場所・方法)
車両立地	<ul style="list-style-type: none"> ● ナビの目的地 	<ul style="list-style-type: none"> ● 直近100ヶ所の駐車場所、電車・バスへの乗り換え場所
メンテ情報	<ul style="list-style-type: none"> ● エンジンの最大回転数、総走行距離、照明状況 	<ul style="list-style-type: none"> ● バッテリー充電の品質、充電プラグの利用
コンタクト情報	<ul style="list-style-type: none"> ● 同期された携帯電話の個人情報 	

参考：EUの動向

- 参考として、EUにおいてもこれらの事項について検討が行われており、特徴的な情報を整理した。(網羅的な整理ではない)
- 下記は2015年3月時点の情報のため、4月のEUデータ保護規則可決に伴い、今後変わってくるものと考えられる。

課題・検討事項	内容	法制度・レポート
データ提供者の同意	<ul style="list-style-type: none"> • IoTに関しては、データの同意を取ることが難しくなることは認識されているが、同意を容易にするのではなく、IoT機器に対してデータの取得をしないようにする機能を持たせることを想定した検討が行われている(「分離される権利 <i>right to be disconnected</i>」)。 	<ul style="list-style-type: none"> • EU 29条作業部会
データの管理に関する事項	<ul style="list-style-type: none"> • データ管理者がEU域外に居ても、媒体がEU加盟国内部に置かれている場合には、EUのデータ保護指令が適用される。 	<ul style="list-style-type: none"> • EUデータ保護指令
データの加工に関する事項	<ul style="list-style-type: none"> • 匿名化にあたっては、他のデータセットとの照合によっても、個人の再識別化を不可能な不可逆的な技術を使用すべきとされている。 • 匿名加工データの第三者への提供は自由とされている。 	<ul style="list-style-type: none"> • EU29条作業部会、匿名化技術に関する意見(意見05/2014)

※斜体はレポート等で示されたもので法律等で定められてはいないもの

Ⅱ．携帯電話事業者が保有する位置情報の取扱いに関する諸外国の状況

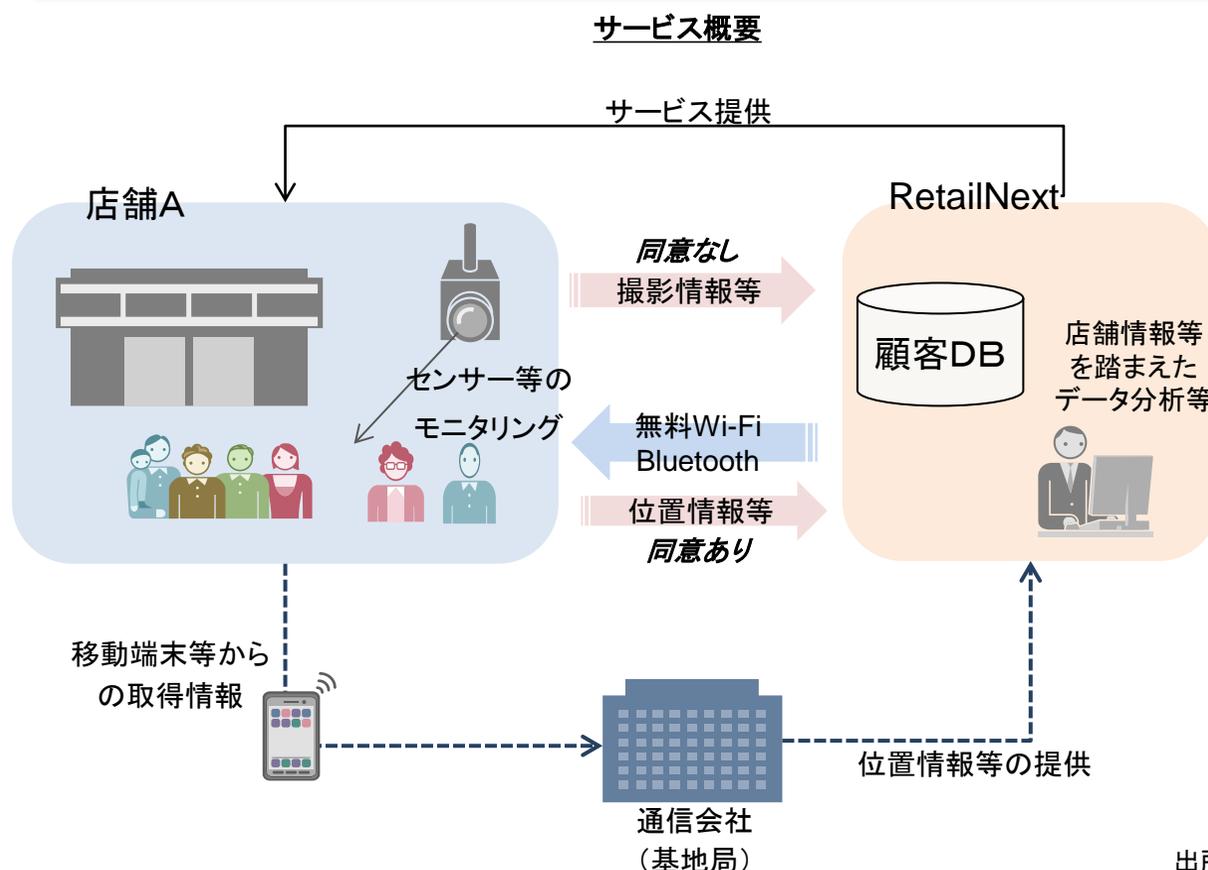
1. アメリカ (1)位置情報活用状況の整理

- アメリカでは位置情報の活用について、携帯電話事業者から外部への提供を行っている事例が少ない。
- Verizon社が一度実施していたが、2015年に外部への提供を終了し、自社内での活用にシフトしている。位置情報によって得られる利益を自社で独占した方が良いと考えているという指摘がある。

項目	対応状況
位置情報の提供に関する法制度	<ul style="list-style-type: none"> ● 通信法と電気通信プライバシー法で規定。 ● 通信法第222条によって、集計顧客情報については、通信目的外で利用可能。
他事業者との連携による位置情報活用状況	<ul style="list-style-type: none"> ● Verizon社が実施していたが、現在は自社で閉じる形に変更。 ● AT&T社は実施を発表したものの、具体的なサービスが公表されていない。
他事業者との連携による位置情報活用の手法	<ul style="list-style-type: none"> ● 事例としては匿名化して提供しているものが大半である。具体的な技術については公表されていない。
他事業者への提供を前提とした顧客との契約	<ul style="list-style-type: none"> ● 匿名化して提供する場合、顧客から同意を取得する必要はない。 ● 匿名化しての利用ではあるが、Verizon社ではプライバシーポリシーを変更の上で顧客に通知している。

1. アメリカ (2) サービス事例 ①RetailNext

- 店舗内の監視カメラによる映像情報とWi-FiやBluetoothで取得された位置情報等を基に、店舗内の買い物客の行動を分析し、経営やマーケティング活動の最適化を図るコンサルティングサービス等を提供。無料Wi-Fiを提供する見返りとして、リアルタイムの買い物行動に関する情報(位置情報など)を収集。
- 無料Wi-Fi等の利用の際に、位置情報に対する同意を取得。
- 同社へのヒアリングによれば、アメリカでは公共空間の監視カメラの撮影について同意を取得する必要がないと業界的に一般的に捉えられているため、撮影及び当該情報の利用に関する同意は取得していないとされる。



- ① 取得情報
 - 店舗内の監視カメラの映像情報
 - Wi-FiやBluetoothによる位置情報
- ② 同意形態
 - Wi-Fi等の利用時に同意を取得
 - 映像情報については言及なし
- ③ その他
 - 位置情報等の様々な情報を利活用することで、価値を創出
(利活用方法は未定)

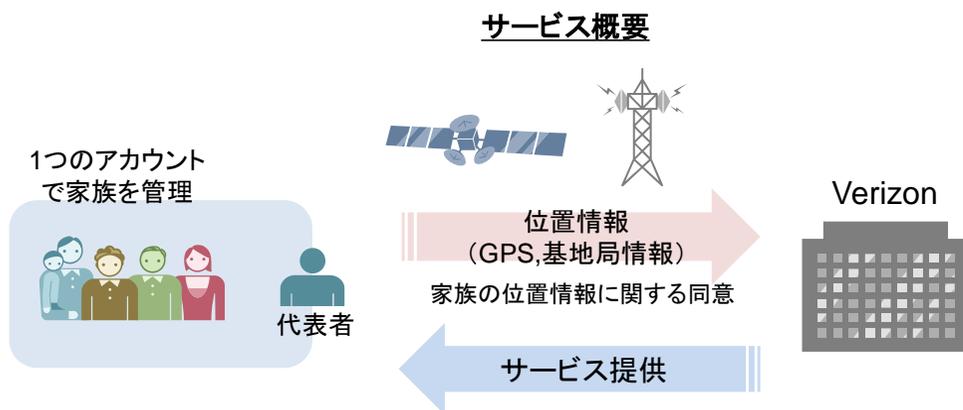
ビデオカメラによるデータ収集



出所) RetrailNextホームページ、Techcrunch2013年12月3日号

1. アメリカ (2) サービス事例 ② Verizon Family Locator

- 本人及び家族の位置情報を登録することで、家族の位置をいつでも知ることができるサービス。事前に指定された場所に行った場合、通知が来る機能も付与されている。
- 家族の位置が分かるため、合法的な目的に利用することしか許されていないこと、非合法的な利用をした場合には、民事・経時的な処罰を受けることが利用規約にて明記。一方、得られた情報はVerizon社、その代理者、契約者がサービスを実現する目的のもとで使用、公開などができると規定。
- 家族の位置情報に対する同意は、サービスアカウントの代表者から取得。代表者の同意によってサービスの利用可能。



- ① 取得情報
 - 基地局またはGPSから取得される位置情報
- ② 同意形態
 - サービス登録時に個人情報(位置情報を含む)の取得等に係る同意を取得
 - 代表者一人が同意することで、家族の位置情報等の利用が可能
 - 一つのアカウントで、家族全員の情報が管理・利用
- ③ 管理形態
 - 家族の位置情報を取得するため、目的外利用については、厳しい処罰等が課されることを利用規約にて明記
 - 取得した情報やサービス提供に係るステークホルダーのみで利用

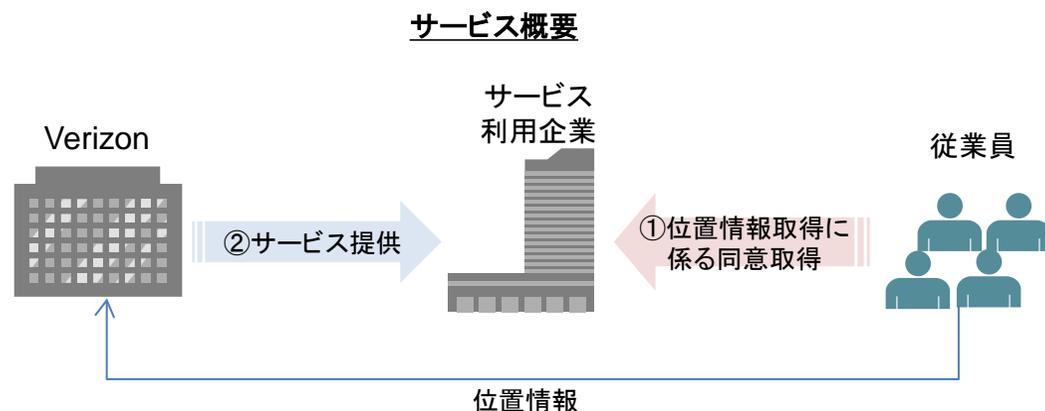
サービスイメージ



出所) Verizon Family Locatorホームページ、

1. アメリカ (2) サービス事例 ③ Field Force Manager

- 従業員が広い地域に分散して働くことが多い事業者(物流、建設など)を対象として、従業員の位置等をモニターし、ビジネスを支援するB to Bのサービス。モニタリングに限定せず、利用料金に応じて、多様な機能を提供。
- アプリによって従業員等の位置情報をモニタリングするが、アプリは登録された法人しか利用できない仕組みとなっている。また、アプリ利用者はサービス利用企業側において登録する必要がある。
- サービス利用企業側において、位置情報取得に係る同意を従業員から取得する必要がある。同意を得た従業員の位置情報のみがVerizonに提供され、サービスが企業に提供される。



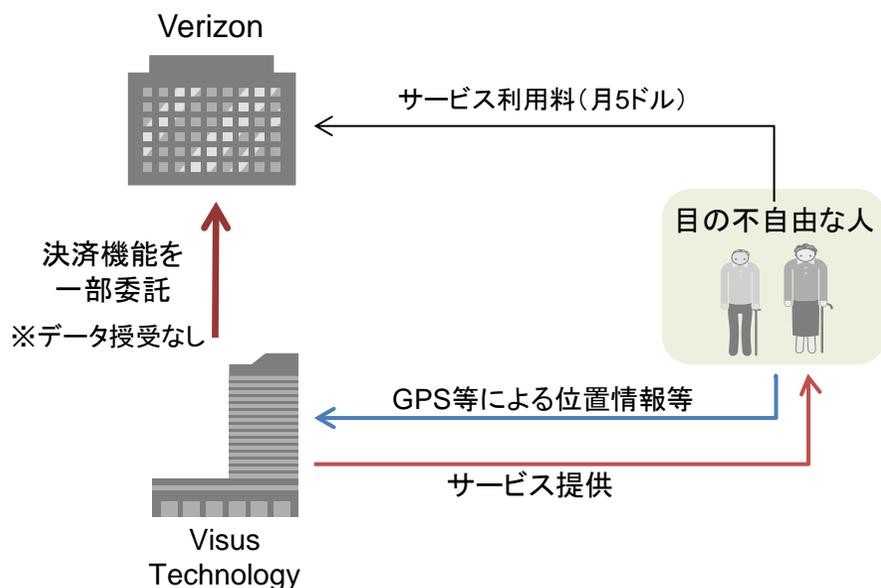
- ① 取得情報
 - アプリを利用することで位置情報を取得
 - GPSから位置情報を取得
- ② 同意形態
 - 位置情報の取得等についての同意は、サービス利用企業が事前に従業員等から取得(就業時に説明)
- ③ 管理形態
 - 第三者への提供は行わない
 - Verizonは、本サービスによって取得された情報をサービス以外の目的で加工・利用することはできない
 - このアプリによって得られた情報はVerizonがそのサービス継続のために利用可能



1. アメリカ (2) サービス事例 ④ Velasense

- スマホにより視覚障害者の日常生活の移動を支援するサービス。Visus Technology社のアプリケーションをダウンロードすることで利用することが可能。
- 位置情報を取得することによるナビサービスがサービスの1つとして存在。GPSから取得される位置情報をもとに現在地や目的地までのルートを音声等で通知を行う。GPS等で取得される位置情報に係る同意は、アプリケーションダウンロード時に取得。
- 位置情報等は、アプリケーションを提供するVisus Technologyが取得・管理。サービス利用料金の決済機能の一部をVerizonが担う。

サービス概要



- ① 取得情報
 - GPSから取得される位置情報等
 - サービス利用に係るその他の個人情報 (電話番号、登録した音声データなど)
- ② 同意形態
 - サービスの利用前に同意を取得 (アプリダウンロード時)
- ③ 管理形態
 - Visus Technology社とVerizon社との間にデータの授受等は存在しない
 - 音声データは、サービス提供以外の目的で利用しないことを利用規約にて明記
 - アプリ利用料等の決済機能の一部をVerizonが担う

出所) Velasenseホームページ

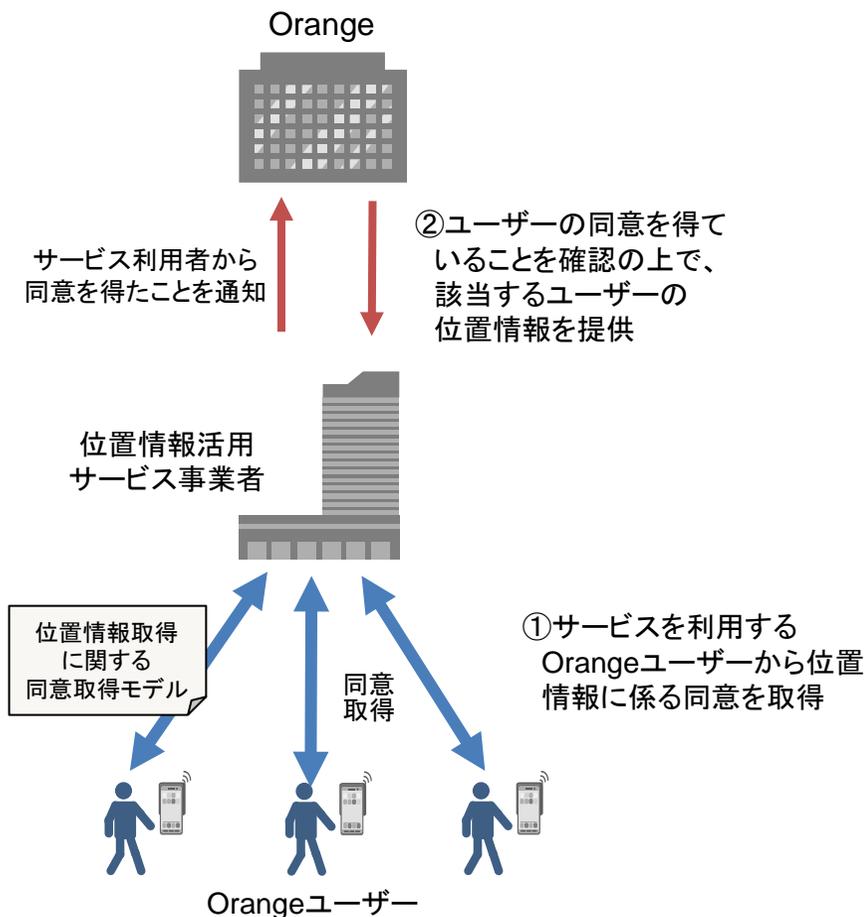
2. フランス (1)位置情報活用状況の整理

- フランスでは位置情報の活用について、携帯電話事業者が積極的に実施している。
- 匿名加工化した情報の分析サービスの提供と、顧客からの同意を得て位置情報を提供するサービスの双方が行われている。

項目	対応状況
位置情報の提供に関する法制度	<ul style="list-style-type: none"> ● 情報処理と自由に関する法で規定。基本的に同意の取得が必要。匿名加工情報については顧客からの同意を得る必要はない。 ● フリート(車両)管理についてはCNILから別途ガイドラインを発行
他事業者との連携による位置情報活用状況	<ul style="list-style-type: none"> ● 積極的な活用が行われている。 ● フリート管理のようなB2Bサービスから、顧客向けのメッセージ送信等のB2B2Cサービスまで複数のサービスが展開されている。
他事業者との連携による位置情報活用の手法	<ul style="list-style-type: none"> ● 顧客からの同意を取得して位置情報を提供している場合と、匿名化した上で特に同意を取得せずに提供している場合の双方が存在する。 ● 顧客からの同意を、情報を取得する通信事業者ではなく、サービスを提供する事業者が取得するケースが見られる。
他事業者への提供を前提とした顧客との契約	<ul style="list-style-type: none"> ● 匿名加工をする場合、特に顧客からの同意は取得していない。 ● 顧客からの同意を得る場合、Orange社は事業者向けに同意取得すべき内容についてのフォーマットを提供している。

2. フランス(参考)個人データ取得の際の個人の同意取得モデル(Orange)

- 位置情報を利用してサービスを提供しようとする事業者は、サービス利用者から個人データ取得に係る同意を取得することで、Orangeから当該個人の位置情報データを取得できる。
- Orangeは、事業者に個人データ取得における同意取得のひな形を提示。①個人データ収集に関する同意取得モデル、②データの欧州外への移転に関する同意取得モデル、③位置情報取得に関する同意取得モデルの3種類が存在。



<①個人データ収集に関する同意取得モデル>

[個人データ]

このフォーマットにより収集された情報は、以下の者のための情報処理の対象となります。

[情報処理の責任者名]

その目的は以下のとおりです。

[処理の目的]

データの受取人は次のとおりです。

[データの受取人]

1978年1月6日の「情報処理と自由」法(修正後)に則り、あなたには、あなたに関する情報にアクセスし、その訂正を求める権利があります。あなたに関する情報にアクセスするには、以下に申請をしてください。

[アクセス権の担当部署の名前]

あなたはまた、正当な理由であれば、あなたに関するデータの処理に反対することもできます。

詳細については、CNILのサイト上で権利について参照してください。

2. フランス(参考)個人データ取得の際の個人の同意取得モデル(Orange)

<②データの欧州外への移転に関する同意取得モデル>

[個人データ]

[処理の担当者名]は、[処理の目的]のための情報処理の手段を保有しています。

記録された情報の利用は、一又は複数の担当部署によるものに限定され、以下の者以外に通知されることはありません。

[データの受取人]

これらのデータの受取人の一部は、欧州連合(EU)域外に本拠を置いており、特に以下の諸国です。

[受取人の国]

これらの受取人には、以下のデータが通知されます。

[伝達されるデータ]

EU域外の受取人へのデータの伝達は、以下を目的とするものです。

[伝達の目的]

個人データの十分な保護水準を確保する目的で、以下の保障措置が講じられます。

[保障の種類][リファレンス]

1978年1月6日の「情報処理と自由」法(修正後)に則り、あなたには、あなたに関係する情報にアクセスし、その訂正を求める権利があります。あなたに関係する情報にアクセスするには、以下に申請をしてください。

[アクセス権の担当部署の名前]

<③位置情報取得に関する同意取得モデル>

[個人データ]

このフォーマットにより収集された情報は、以下の者のための情報処理の対象となります。

[情報処理の責任者名]

(車両内に、車両の位置情報の常時取得を可能にするシステムを設置したので、お知らせいたします。)この新サービスは、以下を目的とするものです。その目的は以下のとおりです。

[処理の目的]

当方は、あなたの移動経路と停止場所を把握することになります。

あなたの移動に関するデータは、最大で[保存の期間]の間、保存されます。それ以降は、すべてのデータは匿名化され、統計作成の目的のためにのみ使用されます。

これらの情報を受け取るのは以下の部署のみです。

[データの受取人]

1978年1月6日の「情報処理と自由」法(修正後)に則り、あなたには、あなたに関係する情報にアクセスし、その訂正を求める権利があります。あなたに関係する情報にアクセスするには、以下に申請をしてください。

[アクセス権の担当部署の名前]

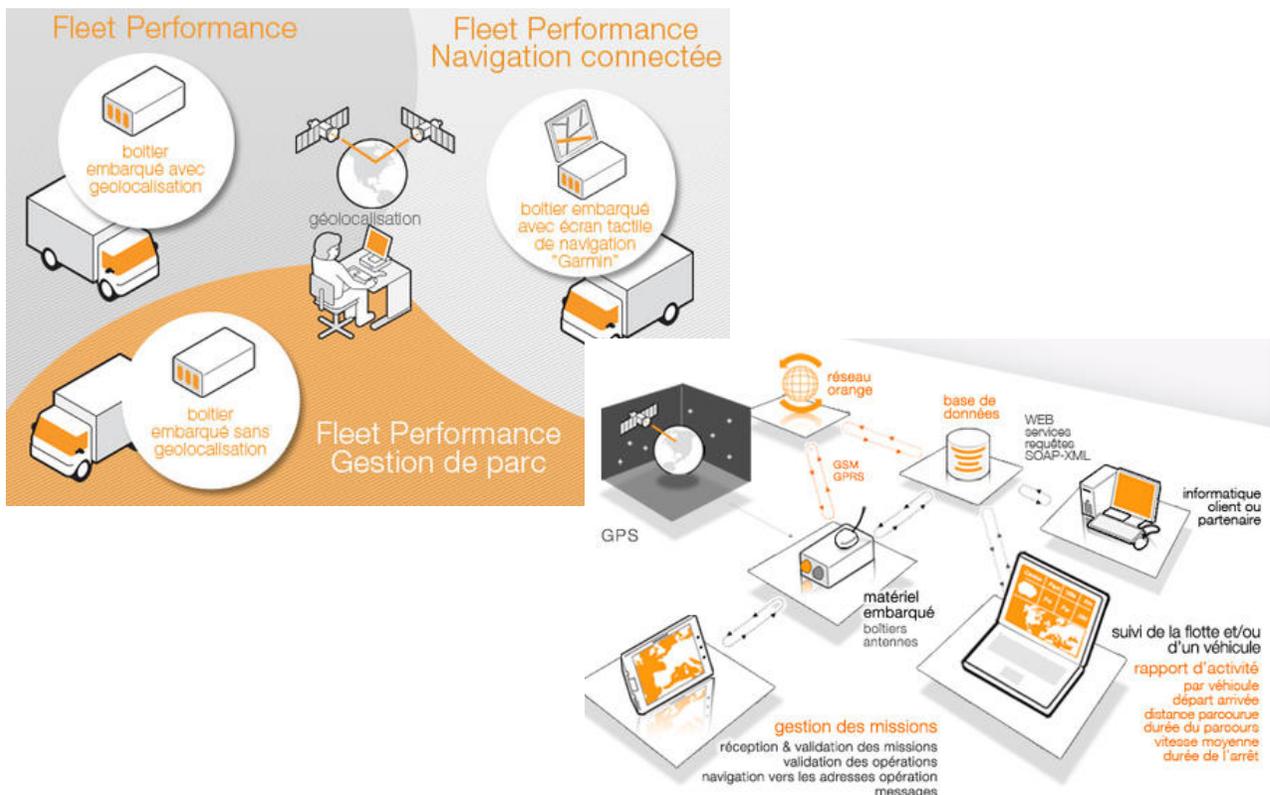
あなたはまた、正当な理由であれば、あなたに関係するデータの処理に反対することもできます。

詳細については、CNILのサイト上で権利について参照してください。

2. フランス (2) サービス事例 ① Fleet Performance

- フランスの通信会社であるOrangeが企業向けに提供しているフリート(車両)管理サービス。携帯電話の基地局情報やGPS情報等を利用して車両の位置情報を管理し、効率的な配送網の構築等に利用することを目的としている。
- サービスはオプトイン形式であり、ユーザー(従業員)の同意を前提とする。
- Orangeは、個人情報保護の第三者機関であるCNILの「雇用者によるフリート管理のためのGPS/GSMを利用した位置特定に関する勧告」に基づいて、サービスを利用する企業が、従業員から個人情報の取得と利用について同意を得ることを求めている。

サービス概要



① 取得情報

- M2M向けSIMカードとGPS/GPRS/GSMアンテナを備えた端末により、車両の位置、速度、方向、使用時間などの情報をリアルタイムで収集

② 同意形態

- サービス利用企業が事前に、従業員等から個人情報の取得と利用に対して同意を取得
- サービス利用企業は、Orangeから情報を取得

③ 管理形態

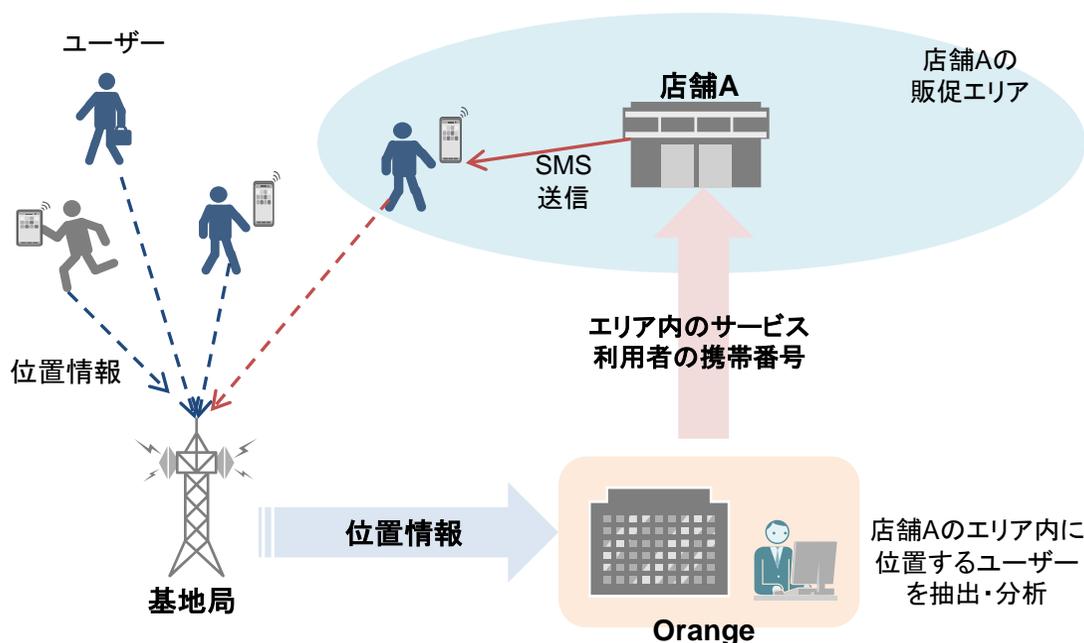
- フリート管理へのアクセスは、Orangeのサーバにホスティングされたカスタムメイドのウェブ・インターフェイスにより可能

出所) <http://www.orange-business.com/fr/produits/fleet-performance>

2. フランス (2) サービス事例 ②Géo Présence

- 位置情報を利用した販促用SMS送付のためのプラットフォームを提供するB to Bサービス。
- Orangelは、マーケティング事業者から予め伝えられた携帯番号のユーザーがある一定の範囲内に入った場合、マーケティング事業者に通知する。マーケティング事業者は、その情報を受けてユーザーにSMSを送信。
- 携帯基地局情報を利用するため、他の位置特定システムとは異なり、ユーザーがGPSあるいはBluetoothをオンしておく必要はなく、また、アプリを事前にインストールしておく必要もないことに特徴がある。
- 携帯基地局に付随したCell IDをベースとしているため、都市部では、その誤差は100-700m程度だが、農村部では、10kmに達する。

サービス概要



出所) Géo Présence ウェブサイト

① 取得・提供情報

- 端末から取得される位置情報(基地局)
- ユーザーの電話番号

② 同意形態

- SMSを送信する店舗事業者が、事前に「Géo Présence」利用のために、ユーザの明確な同意を取得する必要がある(オプトイン形式)
- サービス利用者がサービスを受け取りたい店舗事業者を選択する際に同意を取得
- 同意の際は、サービス提供のため、Orangeから位置情報及び電話番号を取得することを明示

事業者は郵便・電子通信法第L34-1の履行義務が存在

<法第L34-1 >

第三段「通信事業者は、加入者の明確な同意があれば、限定された期間の間、自らの通信サービス、又は付加価値サービスを提供するために、通信に関するデータを処理することができる。 (以下、略)」

第四段「第三段に定められた条件の下で保存・処理されるデータは、サービスのユーザーの身元の特定、通信の技術的仕様、及び、端末の位置特定に関するものだけとする。」

2. フランス（参考）Géo Presence 利用規約

Geo Presenceの利用規約において、位置情報の取扱いについて言及している箇所を以下に抜粋。

5 ユーザーの同意と位置情報のデータの管理

郵便・電子通信法典の第L34-1条に則り、調査の対象となりうるのは、役務の目的で位置情報のデータを利用することを、判断を下せるだけの知識を得た上で、明確に、あいまいさが一切ない形で事前に同意したところのユーザーのみに限定される。

オレンジは、契約者が位置情報取得の目的で提示する利用規約について、それが、郵便・電子通信法典の第L34-1条に定める位置情報に関する要件に適合していることを、またより一般的に、契約者がオレンジに対して、個人情報の処理とプライバシーの保護に関する法令の規定、主に、ユーザーが自らの個人情報の取り扱いについての情報請求を行う権利と自らの個人情報の利用に反対する権利について、「情報処理と自由」法（修正後）に由来する諸義務を遵守する旨を保障することを求める。オレンジは、契約者に対して随時、ユーザーの同意に関する証拠を提出するよう要求する権利を留保する。契約者は、単に請求を受けただけで、その情報をオレンジに通知することを約束する。この約束の尊重は、この契約における基本的な義務をなしている。

特に、契約者がユーザーの位置情報取得のオファーを使用する場合、契約者はこのユーザーから以下を取得することを約束する。

- ユーザーが、判断を下せるだけの知識を得た上で、明確に、あいまいさが一切ない形で与えた同意書。
- ユーザーが、自らの位置情報をオレンジが契約者に対して伝達することに与えた許可。

契約者はオレンジに対して、役務の提供に必要な時間を越えて、オレンジから伝達された位置データを保存しない旨を保障する。

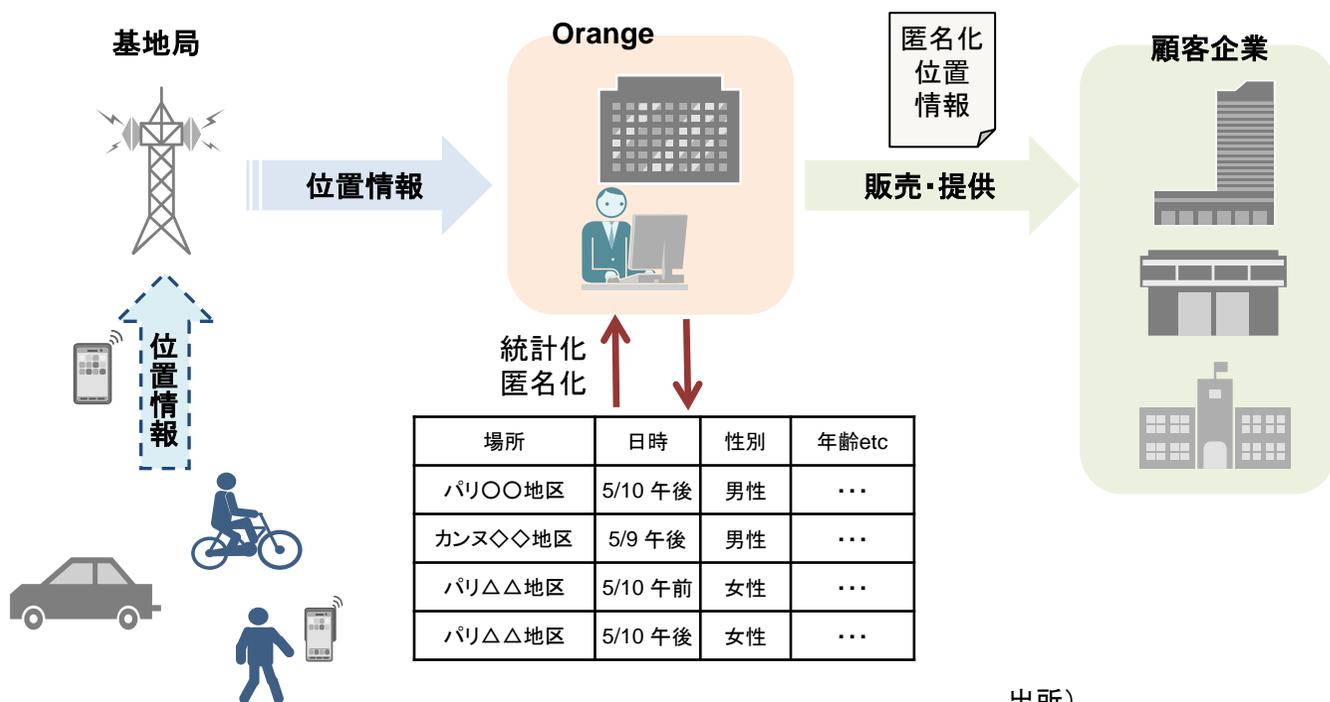
11.2 位置情報のデータの保護

契約者は、この販売一般規約に定める枠内においてのみ、位置情報のデータを使用する旨を約束する。ユーザーを対象にしたトラッキング等の目的にデータを流用、悪用又は再利用する行為と、許可されていない第3者にデータを伝送する行為は、位置情報提供の役務の即時の打ち切りをもたらし、また、訴追の対象となり得る。

2. フランス (2) サービス事例 ③ Flux Vision

- 携帯ネットワークに由来する数百万件の技術データをリアルタイムで統計指標に変換して匿名化された位置データとして販売するサービスを提供(モバイル空間統計に類似したサービス)。輸送インフラや観光インフラの最適化等へ利用することが可能。
- Orangeが取得したデータを不可逆的な匿名化手法によって、加工。利用している匿名化手法は、OrangeによるとCNILによって承認されたものとされているが、具体的な手法は公開されていない。
- 本サービスは、匿名化されたデータの提供のため、位置情報を取得される利用者からの同意を取得していない。

サービス概要



- ① 取得情報
 - 端末によって収集された基地局データ(位置情報含む)
- ② 同意形態
 - 同意取得なし
- ③ 匿名化手法
 - ランダム化、曖昧化を主要な手法として定義
 - ①個人の選抜が可能か、②個人に関するデータとリンク可能か、③個人に関する情報が推定可能かの3点を踏まえ、匿名化手法を検討
 - 具体的な手法は非公開
(作業部会では、ケースバイケースで検討されるべきだと結論づけている)

出所)
<http://fr.slideshare.net/Metronum2015/fluxvisiontourismern2dmetronum2015>

2. フランス (参考) モバイル・ストリート・マーケティング

- 小売店やイベント会場から200メートル内にいる携帯ユーザーへのSMSによるプロモーションやイベントの案内を送付するサービス。
- 様々な条件に従って、ターゲットを絞ることも可能であり、ユーザーは、SFRのウェブサイトにて無料で登録をすることで利用することが可能。本サービスに関連して「SFR Shopping」というモバイルアプリを提供しているが、アプリでは、ユーザーがアプリによる位置情報利用を許可すると、ある商品の販売ポイントが地図上に表示される機能を提供。
- Orangeの「Géo Présence」では、サービスの主体であるSMSによるマーケティング事業者が自らの顧客に同意を得るというシステムであるのに対し、SFRのモバイル・ストリート・マーケティングでは、SFRの加入者がSFRのモバイル・サイト上で申し込む形式をとっており、SFR社自らが事業主体となり利用者から同意を得て、サービスを提供。

サービス概要

- ▶ Renvoyer les consommateurs vers les points de vente qui référencent Fanta avec une offre On Pack

1
J'arrive à 200 M d'un point de vente



2
Je reçois un SMS Promo



3
Je me rends dans le magasin



① 取得情報

- 端末から取得される位置情報(基地局)

② 同意形態

- サービス提供するSFRが顧客から直接同意を取得

③ データフロー

- SFRがデータを収集し、サービスとなるSMSを発信するため、提携事業者に位置情報の提供は行わない
- 提携事業者は、SMSとして発信する広告等情報をSFRに通達するのみ

出所)SFRウェブサイト

3. 韓国 (1)位置情報活用状況の整理

- 韓国では位置情報の活用について、携帯電話事業者が積極的に実施している。
- 匿名加工化した情報の分析サービスの提供と、顧客からの同意を得て位置情報を提供するサービスの双方が行われている。

項目	対応状況
位置情報の提供に関する法制度	<ul style="list-style-type: none"> ● 位置情報の保護及び利用等に関する法律で規定。基本的に同意の取得が必要。位置情報を活用する事業者は登録が必要。 ● ビッグデータについては、政府が別途ガイドラインを発行。 ● しかし、ガイドラインを利用している事業者は限定的。
他事業者との連携による位置情報活用状況	<ul style="list-style-type: none"> ● 積極的な活用が行われている。 ● 基地局情報を利活用している例は少なく、GPSを利用するものが多い。また携帯電話事業者からではなく、自ら集めている場合もある。 ● ただし位置情報を利用していれば全て位置情報サービスとして整理されており、単に投稿時に現在地を取得するだけのサービスも含まれている。
他事業者との連携による位置情報活用の手法	<ul style="list-style-type: none"> ● 顧客からの同意を取得して位置情報を提供している場合と、匿名化した上で特に同意を取得せずに提供している場合がある。
他事業者への提供を前提とした顧客との契約	<ul style="list-style-type: none"> ● 匿名加工をする場合、特に顧客からの同意は取得していない。 ● 顧客からの同意を得る場合、KT社、SKT社共に利用規約を公表している。

3. 韓国 (2)位置情報の保護及び利用等に関する法律①

- 韓国では位置情報の活用に関して、2005年に「位置情報の保護及び利用等に関する法律」を制定。
- 位置情報事業者と、位置基盤サービス事業者を定義。GPS、ETC、自家通信網による情報収集についても位置情報事業者として許可制としている。位置情報を活用するサービス事業者も届出が必要。
- 同意取得時に伝えるべき項目についても規定。

- 位置情報法では、以下の2つの事業者を規定

	位置情報事業者	位置基盤サービス事業者
定義	携帯キャリア等のように携帯電話端末がどの基地局と信号を送受信しているかを把握して利用者の位置情報を直接収集する事業者	位置情報を位置情報事業者から提供してもらい利用者にサービスを提供する事業者
事業者例	携帯電話キャリア、物流業界の事業者やタクシー組合等 (GPS、ETCや自家通信網についても対象)	スマートフォンアプリを開発する会社
許可等	放送通信委員会の許可	放送通信委員会への申告

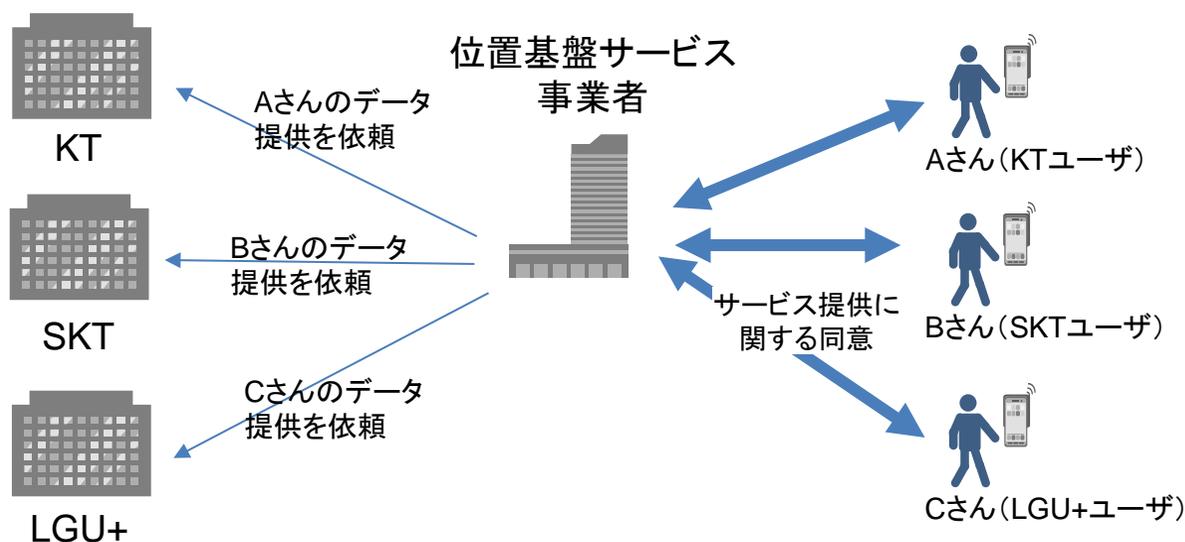
- それぞれ、同意取得時に以下の項目を利用約款に明示して同意を得る必要がある(第18条、19条)

	位置情報事業者	位置基盤サービス事業者
位置情報事業者の情報	商号、住所、電話番号、その他連絡先	商号、住所、電話番号、その他の連絡先
権利	個人位置情報主体と法定代理人の権利、その行使方法	個人位置情報主体と法定代理人の権利、その行使方法
サービス内容	位置基盤サービス事業者に提供しようとするサービスの内容	位置基盤サービス事業者が提供する位置基盤サービスの内容
保有期間	位置情報収集事実確認資料(※)の保有の事実と保有期間	位置情報の利用・提供の事実に対する確認資料の保有の事実と保有期間

3. 韓国 (2)位置情報の保護及び利用等に関する法律②

- 位置情報法では、位置情報を活用しようとする位置基盤サービス事業者がサービス利用者からの同意を得れば、該当する個人の情報について位置情報事業者から提供を受けることができる。
 - 位置情報事業者は、位置基盤サービス事業者からの依頼に対して、正当な理由無く提供を拒絶できない点に特徴がある。
-
- 位置情報法では、位置情報事業者が位置情報を収集する部分について得る同意と位置基盤サービス事業者が位置情報を利用して利用者にサービスを提供する際の同意は別のものとして整理。
 - 位置基盤サービス事業者は、利用者にサービスを提供するに当たって別途の同意を得る必要(第19条)
 - 位置基盤サービス事業者は、消費者から第19条の同意を得ていれば、位置情報事業者から該当する個人の位置情報の提供を受けることができる。この際、位置情報事業者は正当な理由なく提供を拒絶することはできない。(第20条)

位置情報事業者



- 位置基盤サービス事業者は、サービス利用者から同意を得れば、当該個人が利用している位置情報事業者から、データ提供を受けることが可能
- サービス利用者から同意を得る際には、前頁の事項を利用約款に明記して、同意を得る必要がある
- 位置情報事業者は、位置基盤サービス事業者から情報の提供依頼を受けた際に、正当な理由無く提供を拒絶できない

3. 韓国（参考）ビッグデータの個人情報保護ガイドライン

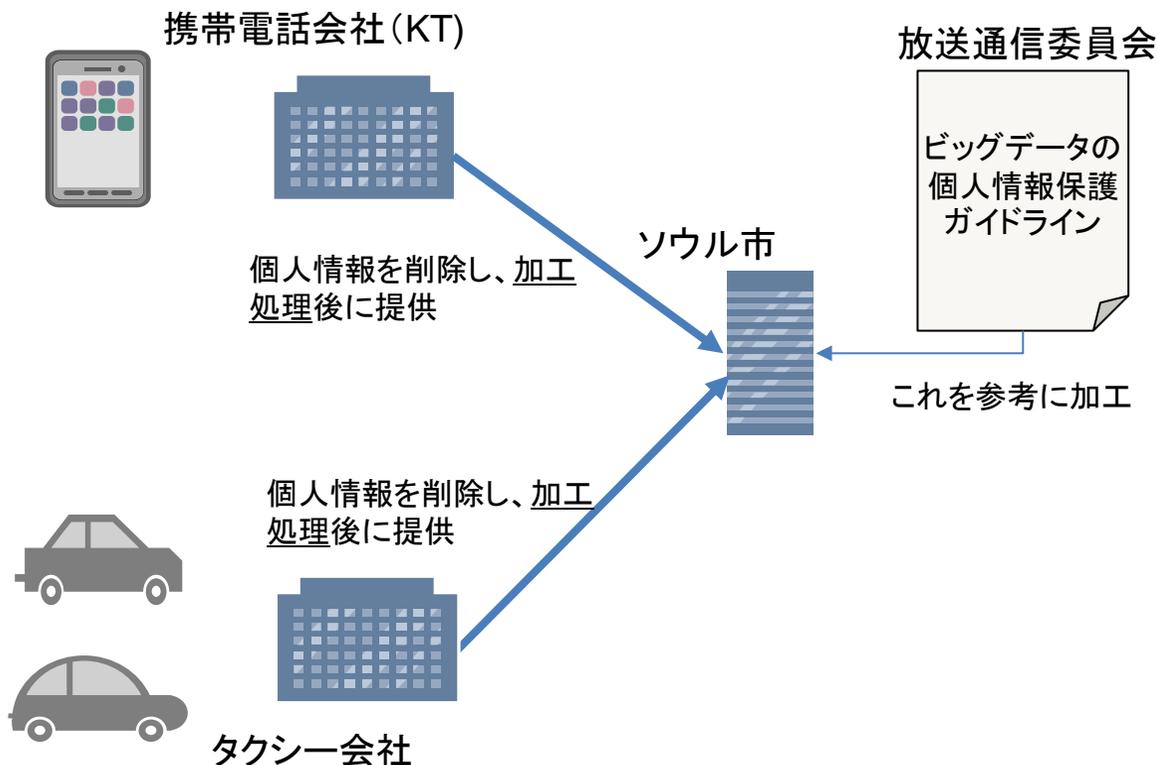
- 2014年12月23日、放送通信委員会は、ビッグデータ処理・活用の際、個人情報の保護と活用のための具体的な基準を定めた「ビッグデータの個人情報保護ガイドライン」を発表。
- ビッグデータ処理の過程で収集されたデータに個人情報が含まれている場合、これを他の情報に置き換えるか、他の情報と組み合わせても、特定の個人を識別することができないようにする「非識別化」の措置が行われると、収集・活用ができるようにした。事業者の規制の不確実性を最小限に抑えるため、現行の法令で公開された情報などを合法的に収集・活用できる具体的な基準を提示。

項目	内容
第4条(公開された情報の収集・利用)	<ul style="list-style-type: none"> ① 情報通信サービス提供者が、個人情報が含まれている公開された情報を非識別化措置した場合には、利用者の同意なしに収集・利用することができる。ただし、利用者の同意を受け、法令上許容される場合には、非識別化措置を取らずに収集・利用することができる。 ② 情報通信サービス提供者は、第1項の規定により、個人情報が含まれている公開された情報を収集・利用する場合、公開された情報の収集源、収集・保存・組合・分析等を処理するという事実およびその目的を利用者などがいつでも簡単に確認できるように、個人情報の取り扱い方針を介して公開しなければならない。 ③ 情報通信サービス提供者は、利用者等の要求があれば、即時次の各号のすべての内容を利用者等に通知しなければならない。 <ul style="list-style-type: none"> 1. 個人情報の収集源 2. 個人情報の収集・保存・組合・分析などの処理の目的 3. 個人情報の処理の停止を要求する権利があるという事実
第5条(利用履歴情報の収集・利用)	<ul style="list-style-type: none"> ① 情報通信サービス提供者は、次の各号の場合を除いては、利用者の同意を受け、非識別化措置をとった後、利用履歴情報を収集・利用することができる。 <ul style="list-style-type: none"> 1. 情報通信サービスの提供に関する契約を履行するために必要な利用履歴情報として、経済的・技術的な理由で通常の同意を受けることが明らかに困難な場合 2. 情報通信サービスの提供による料金精算のために必要な場合 3. 他の法律に特別の規定がある場合 ② 情報通信サービス提供者は、第1項の規定により利用履歴情報を収集する場合は、その情報が収集・保存・組合・分析などの処理されている事実と目的を利用者がいつでも簡単に確認できるように、個人情報の取り扱い方針を介して公開しなければならない。 ③ 情報通信サービス提供者は、利用履歴情報の収集・保存・組合・分析などの処理を拒否することができる方法と手順を用意しなければならない。 ④ 情報通信サービス提供者は、利用者の検索プログラムなどで利用者や検索プログラムなどの提供者が設定した利用履歴情報の収集拒否の選択を利用者の同意なしに変更してはならない。

3. 韓国 (2) サービス事例 ① 深夜バス路線作成計画

- ソウル市の深夜バスの路線を作成するために、ソウル市がKTからデータを無償で位置情報提供してもらう契約を締結。
- ソウル市は、2014年3月の1カ月間の0時から5時まで利用されたKTのCDR(Call Detail Record) データ30億件と韓国スマートカード社の提供したタクシーの乗降車情報500万件を分析することで、深夜バスの路線を策定。
- 顧客の個人情報とも言えるデータはKT内部で除去した後、それ以外のデータを分析に利用。具体的には、名前等の個人情報を削除し、個人情報に近い年齢のような場合は特定地域(1km、六角形の形態)単位で加工および統計処理を実施。利用の際に、十分な非識別化を行っているため、位置情報等の個人情報は、同意を取得することなく提供。

分析フロー



深夜バス路線の紹介ウェブサイト

심야 N 버스, '올빼미 버스'만 알면 귀가 걱정 없어요!

라이프 2015.06.22 15:04

하루 100만 명이 드나드는 대한민국의 중심 서울. 이른 새벽부터 늦은 밤까지 서울은 한 시도 잠들지 않는 도시입니다. 서울을 생활터전으로 살을 이어가고 있는 시민들을 위해 서울시에서 심야버스를 운영하고 있습니다. '올빼미 버스'라는 이름으로도 불리고, N버스라고도 불리는 심야버스에 대해서 알아보까요?

심야 버스란?



심야 버스는 대중교통 운행이 끊기는 시간대에 시민들의 교통 불편을 줄이기 위해 그래서 올빼미 버스는 이름을 붙이게 되었죠. 심야버스는 서울 시내에 지하철 사이에 운행됩니다. 배차 간격은 40~50분으로 요금은 카드 결제 기준 1,850원(이 2150원)으로 현재 총 8개 노선을 운영하고 있습니다.

KT의 데이터를 활용한 것을 소개

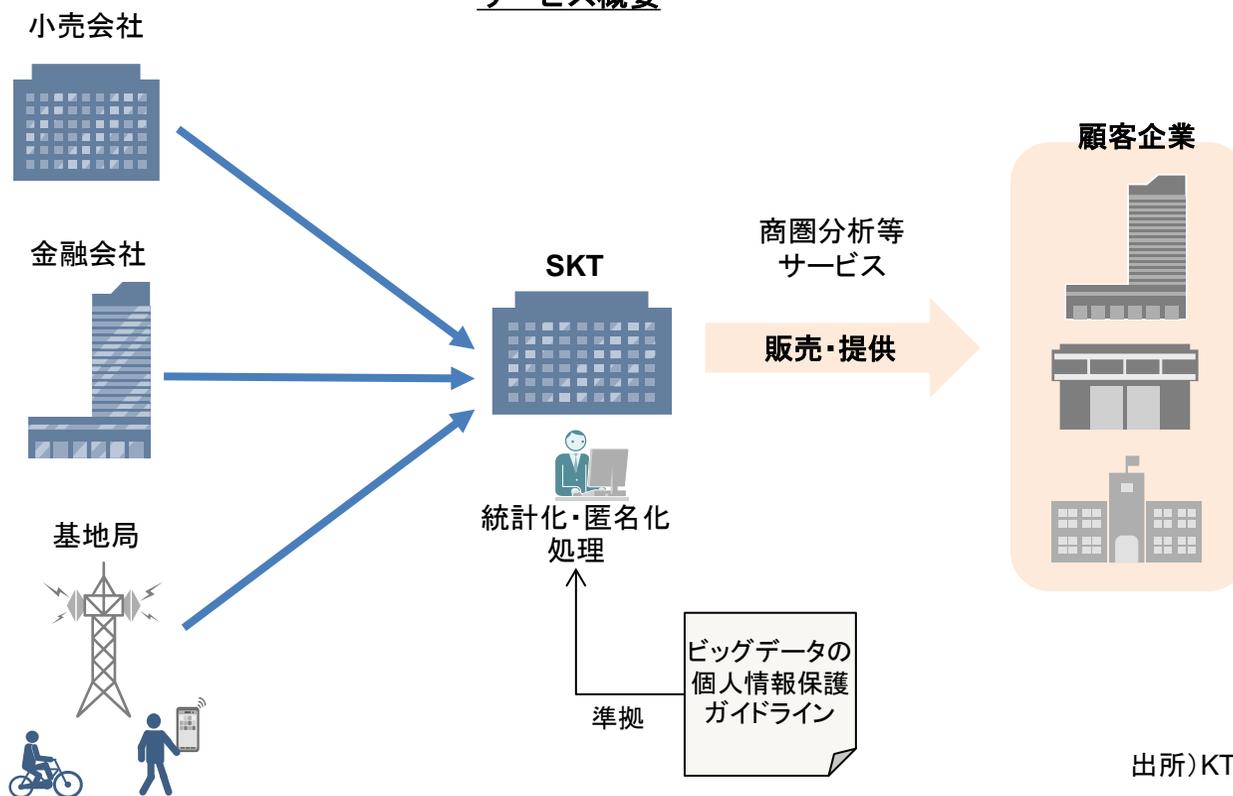
kt 통화량 빅데이터로 만든 심야 버스 노선

심야 버스 8개 노선은 하나 같이 이용자 수가 많은 알짜 노선입니다. 이렇게 인기 구간 노선을 구성할 수 있었던 이유는 바로 빅데이터를 활용했기 때문입니다. 빅데이터를 활용해 심야버스 실수요를 예측하여 도시를 중심으로 시내를 가로지르는 방사형 네트워크를 구축한 것입니다. 빅데이터는 2014년 3월 한 달 동안 차장부터 새벽 5시까지 이용된 kt의 통화량 데이터 30억 건이 활용되었습니다.

3. 韓国 (2) サービス事例 ② ジオビジョン

- 通信会社であるSKTの持っている位置情報(基地局分析)に加え、カード会社の決済情報や売上情報を地図に結合して商圈分析に活用するサービス。時間帯別・月別・性別・年齢別の流動人口や商圈内の購買パターンを分析し、情報として提供している。
- ジオビジョンは、ヒュンダイカード等から提供された信用評価情報などをビッグデータ技術で分析する。毎月、事業者向けに地域流動人口、競争店の分析、顧客の移動パターン、周辺地域分析、売上高情報などを提供している。
- 位置情報を含めた各情報を匿名化処理した上で利用。しかし、具体的な匿名手法は公開されていない。

サービス概要



- ① 取得情報
 - SKTが保有する位置情報
 - 銀行等から提供されるマーケティング関連のビッグデータ
 - ② 同意形態
 - 統計化・匿名化処理を行うため、同意取得なし
 - 信用評価情報等もビッグデータとして扱うため同意取得なし (ガイドラインに準拠)
- ➔ ビッグデータとして個人情報を利活用

出所)KTウェブサイト、その他公表資料よりMRI作成

3. 韓国（参考） 韓国の位置情報活用振興

- 韓国では位置情報の活用に関して、位置情報事業者と、位置基盤サービス事業者の双方を規制する法律を規定
- 当該法律を下敷きにして、位置情報産業の活性化のための計画、仕組み作りを実施。
- 位置情報産業(LBS産業)の市場規模については、2012年をピークに、横ばいの状況である。

- 韓国では位置情報の活用を推進するための法制度の整備及び、振興のための計画を策定している。

年	法律／施策
2005年1月	位置情報の保護及び利用等に関する法律
2010年6月	LBS産業育成及び社会安全網の高度化のための位置情報利用の活性化計画
2016年1月	位置情報利用の活性化計画（上記計画の改定）
2016年3月	2016年度位置情報事業者の許可計画

- 位置情報利用の活性化計画では、①LBS(Location Based Service)産業の育成、②社会安全網の高度化、③プライバシーの保護という3つの推進目標を掲げて実施
- LBS産業の市場規模の推移を見ると、2012年にはLBS産業関連全体の売上高が103兆ウォンであったが、2014年には86兆ウォン、2015年には90兆ウォンと、横ばいである。
 - なお、LBS産業のみに絞った場合の売上高は、2015年時点で4,236億ウォン(約440億円)。

参考. B2Bにおけるデータ流通の促進及びプライバシーの確保に関する課題

1. IoTデータ流通におけるビジネスユースケース①

■ IoTデータ流通においては、主に4つのビジネスユースケースが想定される。以下は、主にアグリゲータによるデータ販売・サービス提供を想定したユースケース(B to B型ビジネス)。

ユースケース	アグリゲーション型	データプロセッシング型
概要	<p>データを集約するアグリゲータが存在し、集約したデータを各事業者等に提供するモデル</p>	<p>消費データ等のデータを集約するアグリゲータが存在。集約データを分析・加工をし、各事業者等に提供するモデル</p>
概略図		
事例	<ul style="list-style-type: none"> ・カルチュア・コンビニエンス・クラブ「Tポイントサービス」 ・プラットフォーム事業者など 	<ul style="list-style-type: none"> ・NTTドコモ「モバイル空間統計」 ・ゼンリンデータコム、Bluekai ・プラットフォーム事業者など

1. IoTデータ流通におけるビジネスユースケース②

■ 以下は、データを収集するアグリゲータを介さず、サービス提供を実現するビジネスモデル(主に、B to B toC型)。

ユース
ケース

サードパーティーユーティリゼーション型

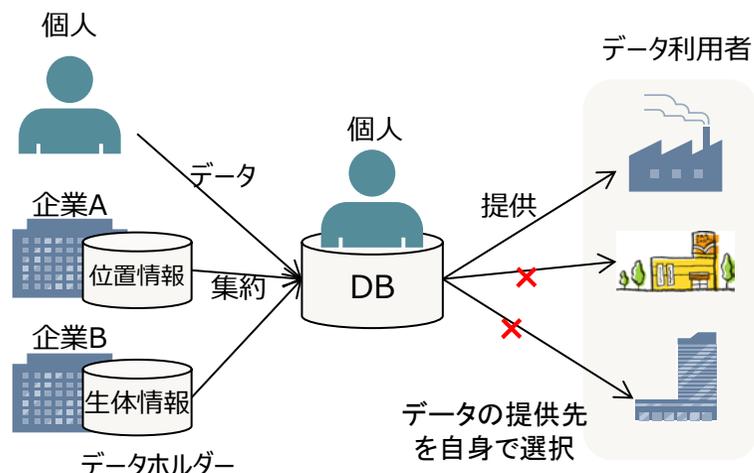
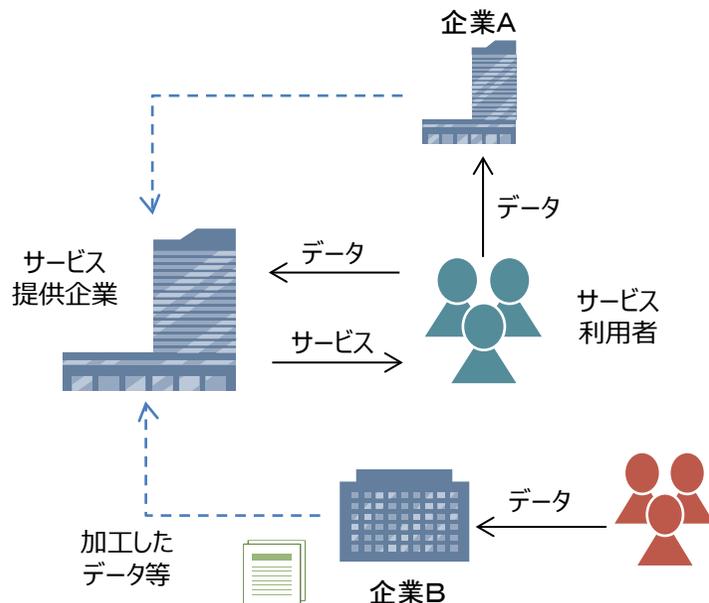
パーソナルデータストア型

概要

新たなサービスを提供するために、他企業が保有しているデータの提供を受け、サービスを利用者に提供するモデル

企業主導で行われていたパーソナルデータの利活用を、消費者が自身のデータを管理し、流通をコントロール可能にするモデル

概略図



事例

・パナソニック「高齢者見守りサービス (位置情報×生体情報)」など
⇒企業が汎用的に利用できるモデル

・情報銀行
・米国 Green Button、Personal.com など
⇒VRMの考えを体現するサービスモデル

2. ビジネスモデルを踏まえたIoTデータ流通における課題・検討事項

- データ流通においては、データの権利帰属や契約・同意の在り方等、様々な課題が想定される。
- IoTデータ流通におけるビジネスモデルによって、データ流通における主な課題と考えられる対応策(案)は以下のとおり。

ユースケース	データ流通における主な課題	考えられる対応策(案)
アグリゲーション型	<ul style="list-style-type: none"> 提供データの信頼性確保(欠損、誤差等への対応、免責規定など) 個人から収集したデータを他企業に提供するための同意・契約の在り方(企業、個人の双方に益がある) データを有償提供する対価条件 	<ul style="list-style-type: none"> データ品質を示すラベル表記、表記内容が真正であることを認証、保証する仕組みの構築 企業、個人にとってより安心・安全なデータの提供可能とする包括的同意プロセスの構築 データ提供先とアグリゲータにおけるデータ権利帰属に関するルールの構築
データプロセッシング型	<ul style="list-style-type: none"> プライバシーに配慮し、企業にとって価値のある匿名化手法の在り方 分析・加工したデータを有償提供する対価条件 	<ul style="list-style-type: none"> 有用性が高く、個人特定性が十分に低減された匿名加工手法の確立(個別データ等による匿名化手法の指針策定等) 有償提供における対価条件の留意点、有償提供形態を整理
サードパーティユーティライゼーション型	<ul style="list-style-type: none"> 他企業からデータ提供(第三者提供)を受けるための契約の在り方 転々流通等を防ぐ個人データのトレーサビリティの確保(転々流通等への対策課題) 	<ul style="list-style-type: none"> データの利用目的を踏まえた、データ提供の契約条件、留意点等の整理 個人が提供したデータの流通ログの見える化、トレーサビリティを確保する同意プロセスの構築
パーソナルデータストア型	<ul style="list-style-type: none"> 企業へのデータ提供を個人の選択に依存することに伴う、個人に対する負荷 プライバシー等に配慮したパーソナルデータを一括に収集する同意の在り方 一括に収集されるパーソナルデータのセキュリティの確保 	<ul style="list-style-type: none"> データを提供する企業の信頼性等を評価するための共通化されたラベル等の提供 収集されるパーソナルデータを一括に管理するための簡易的な同意プロセスの構築 個人の提供条件に合致した企業にデータを提供するための包括的な同意プロセスの構築

参考)IoTデータ流通における一般的な検討事項

検討・整理項目	主な検討内容
データ特性を踏まえた契約条件	<ul style="list-style-type: none"> • 個人情報が含まれているデータの提供における契約条件(利用目的の明示など) • 動的/静的データの提供における留意点(即時性が求められる動的データをリアルタイムに提供するための要件など) • 匿名加工データの流通における条件
データの利用目的に応じた契約条件	<ul style="list-style-type: none"> • データの提供形態(委託、共同利用、第三者提供など)に基づいた利用目的の設定 • 目的外利用が許容される条件(緊急・災害時など) • データの転々流通を防ぐための仕組み
データの権利帰属	<ul style="list-style-type: none"> • データの権利帰属先(個人、データ収集者、ネットワーク管理者など) • データの知的財産権を踏まえた対応(知的財産権が主張できない場合など)
データの利用に起因するインシデント責任関係	<ul style="list-style-type: none"> • インシデント発生元、データの提供形態等を踏まえた企業の責任範囲と対応 • データの提供/流通時におけるインシデント発生元の考え方及び責任範囲
企業間におけるデータ管理形態	<ul style="list-style-type: none"> • データの提供先に求める安全管理措置の要件(組織的、人的、物理的、技術的の4要件)
データの収益性を確保するための条件	<ul style="list-style-type: none"> • 提供データの信頼性確保(欠損、誤差、遅延等への対応、免責規定など) • 取得したデータ、又は加工したデータを有償提供する対価条件の考え方、決め方
プライバシーへの配慮	<ul style="list-style-type: none"> • データの取得や事業者への提供における同意プロセスの在り方、同意・通知方法 • 取得データにおけるプライバシーリスク(モノからデータを取得する際において、取得データにモノの識別IDが付与されている場合など) • 個人識別性の低下や円滑なデータ提供を目的としたデータの加工方法(どこまで加工すべきか等)

参考)IoT進展に伴うデータ流通における共通的な課題

- ビジネスユースケースを踏まえたデータ流通促進に係る課題に限定せず、IoTの進展に伴う企業間のデータ流通における共通的な課題が存在。IoTの実サービスの創出促進のため、現在は技術的検討が中心。(機器間でのデータ交換方法の標準化、センサー等から取得される多量なデータの通信プロトコルなど)
- 今後は、取得したデータをどのように流通して、ビジネスの創出等に繋げるか等の検討が期待される。

課題・検討事項	内容	考えられる対応案
データ・情報の信頼性	<ul style="list-style-type: none"> ● データ情報(取得遅延やエラー率、権利関係等)の表示方法 ● データ情報の信頼性に対する認証制度の構築 	<ul style="list-style-type: none"> ● データの品質を示すラベル表記の標準化(ISO8000など) ● ラベルの記載内容が真正であることを認証あるいは保証する仕組みの構築
異なるデータ間の紐づけ	<ul style="list-style-type: none"> ● 同じ対象物や場所を対象に、異なるセンサーで異なるデータを計測している場合に、それぞれの位置データ等を、その「対象物」のものであると関連づける仕組みの構築 	<ul style="list-style-type: none"> ● 計測対象物の識別IDの標準化(技術規格 ucode、EPCglobalなど) ● 連続的な対象物(大気や空間、あるいは道路等の大規模構造物)においては、グリッド化などの分割方法とIDとの対応関係の標準化(ISO19115-2 など)
多数の異なるデバイス間の円滑なリアルタイムデータ流通	<ul style="list-style-type: none"> ● 多数の異なるデバイス間であっても、リアルタイムに必要なデータを取得・提供できる環境の整備 	<ul style="list-style-type: none"> ● プロトコルやデータの形式の標準化(Wi-SUNなど) ● 流通ハブ・プラットフォームの開発・普及促進等の実施