

改正個人情報保護法等を踏まえたプライバシー保護検討タスクフォース

IoT時代のパーソナルデータの取扱い
事業者の課題と対応について

2016,04,06

株式会社オプト 寺田眞治

一般社団法人モバイル・コンテンツ・フォーラム 常務理事
一般社団法人OpenID ファウンデーション・ジャパン 理事

IoTの構造とパーソナルデータの関係

1. パーソナルデータは誰がどのように扱っているのか？

事業形態も多様に

1. 垂直統合型
2. 水平統合型
3. 独立モジュール型
4. 協業型 等

従来の定義では対応できない

電気通信役務

電気通信設備を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供すること

電気通信事業

電気通信役務を他人の需要に応ずるために提供する事業

誰がControllerで
誰がProcessor？

クラウド化の進展により、設備、ネットワーク、プラットフォーム層が複雑にモジュール型で繋がる（仮想化により境界線も曖昧化）

SaaS

PaaS

IaaS

Controller to Controller
Controller to Processor
複数社がデータ提供

端末は3タイプに

1. センサータイプ（単一機能型）
2. 特定領域タイプ（中間型）
3. バーサタイルタイプ（万能型）

今後増えるIoT機器は、個人所有ではなく、外部よりセンシングするものが増える。

Application

ミドルウェア

OS

非所有物系

認識困難（不可知）
利用者の関与が困難

Application

ミドルウェア

OS

所有物系

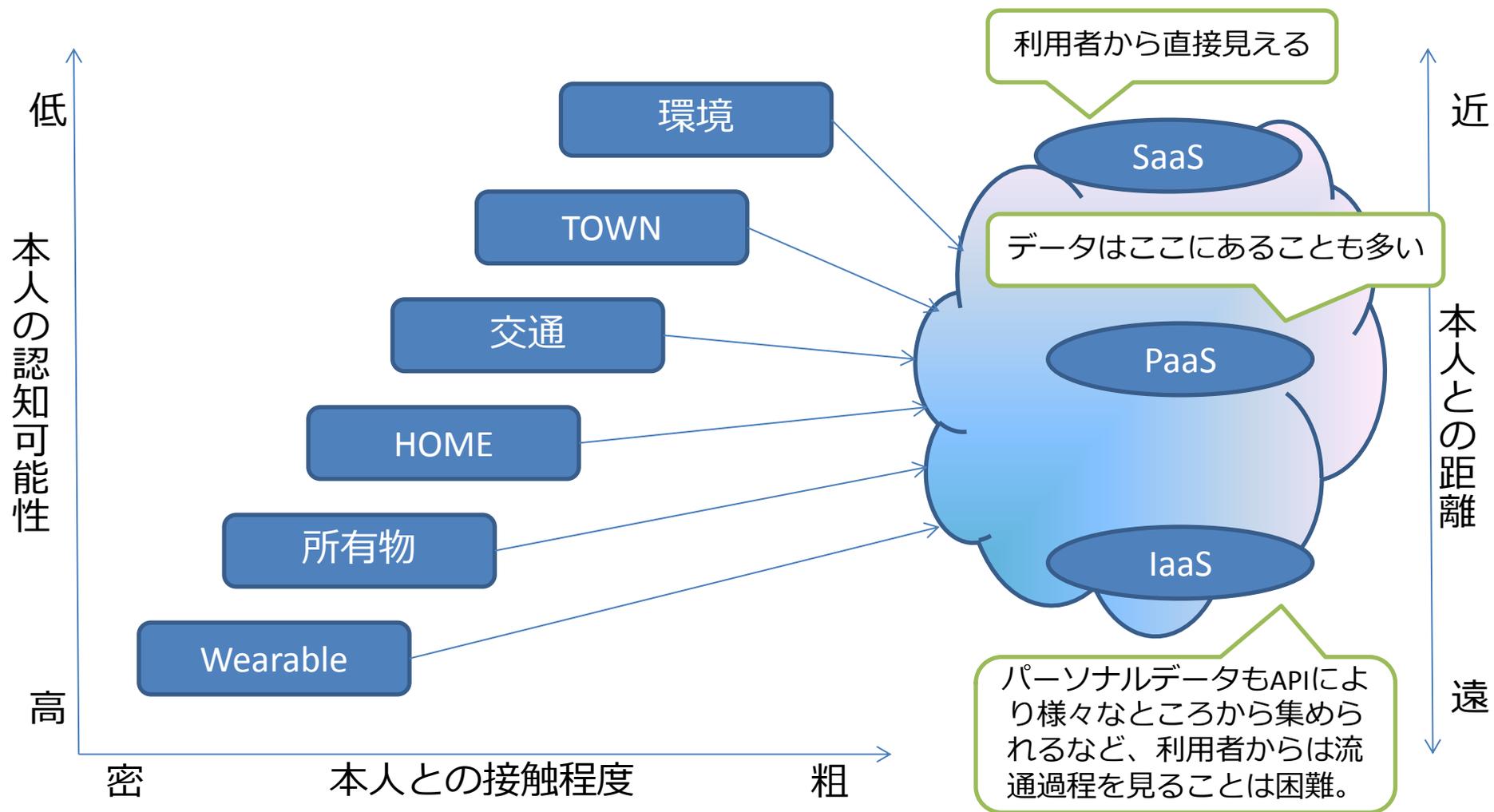
認識（可知）
利用者の関与が可能

その他に

- ・人が関与しないもの（自動化、AI等）が増える
- ・データ互換（データポータビリティ）の進展

2. パーソナルデータはいつ、どこで取得され、どこにあるのか？

センサーは、本人の身体から離れるほど、認知されにくく、接触頻度も少なくなる。
クラウドの低いレイヤーになるほど、本人との距離が遠くなる。



3. IoTに求められるプライバシー保護の新しい視点

消費者の知らない間にセンシングされる
↓
個別に取得されないようにするのは不可能
(**取得規制**はIoTの発展を阻害)

行為規制へ（行動規範の明文化）

消費者の望まない利用、プライバシー侵害を引き起こす利用を規制

データポータビリティの確立（消費者の権利と義務を明確化）

消費者の意思の尊重 → データコントロールの権利と義務を実現させる

トラスト・フレームワークの構築

信頼できる事業者の認定
信頼できる事業者同士による連携促進

データ・トレーサビリティの確保

データ流通の透明化
消費者によるデータコントロール実現

事業者の課題と対応

1. パーソナルデータの取扱いにおける課題

1. 透明性の確保が困難に

- ①複雑化、多重化する利用者への説明がもたらす透明性の低下
 - 事業者としてのプライバシーポリシーとサービス毎のプライバシーポリシーの多層化
 - 個人情報保護とプライバシー保護（cookieポリシー等）の二重化
 - 利用規約、約款等のその他の重要な規約との棲み分け
 - 複雑化する法律（個人情報保護法、消費者保護法、景表法等）による説明量の増大
- ②消費者とのタッチポイントが増大、多様化することによる透明性の低下
 - サービス加入方法の他種類化（対面、郵送、オンライン（PC、モバイル）、KIOSK端末）

2. 同意取得や本人の関与の確保が困難に

- ①増えすぎて覚えていられない & どこに問い合わせれば良いのか迷う（わからない）
- ②パーソナルデータの取得ポイントが増大、連続的（常態的）な取得の拡大
- ③IoT進展に伴う本人非接触の取得（不可知なセンサー）
- ④共同利用、情報収集モジュール等によるサービス提供者以外の取得
- ⑤第三者提供等による情報の流通先の増加

3. 個人情報以外のプライバシー保護の基準が無い

- ①統一的な指針やガイドラインが無い
 - ②海外との整合性が取れていない
- 根拠となる思想の欠如

4. レピュテーション・リスクによる萎縮

- ①消費者の意識や感覚とのずれ
 - ②一部の原理主義者への対応
- 消費者と事業者の対話不足
→マルチステークホルダープロセスによる信頼の構築

本日はこちらを
中心に

2. 透明性の確保

①説明事項の整理 ②説明事項の構造化 ③説明タイミングの標準化



基本構造のモデル化と業界別ガイドライン等の整備

形式的にある程度標準化されることにより、利用者にとって理解しやすくなる。
しかし、膨大な「お決まりの約束事」となり、「理解しようとする意識」はむしろ後退する可能性が高い。

また、事業者も「コピペ型の安易な説明」となり、本来の「理解してもらおうとする意識」は醸成されない。

さらに、利用者・事業者双方から産業発展に伴う多様な状況への対応を求められることとなり、ガイドラインは膨大で難解な経典になっていく。



単なる形式化の拡充は相互不信を招き、「消費者 vs 事業者」の構造を解消できない

事業者：お作法に則って全て説明している

利用者：膨大すぎて読めないし、分からない

事業者：読まない、理解しようとしないう者についての責任は無い

利用者：分かるようにしてくれない者は信用できない



実効性のある透明化は困難になると考えて、他の方法も考えるべき

※基本的な「透明性の確保」についての指針は必要で、そのうえで考えることが前提※

3. 同意取得や本人の関与の確保が困難に

あらかじめの完全な同意取得（いつ、何について、どこまで、どのようにetc）は、「十分な透明性」が前提で、事業者、利用者ともに負担が重く、形式的になる

事業者

利用者の信頼獲得より法的リスクヘッジのため想定される可能性全ての詳細説明となる一方、産業振興に繋がる利用者にとって有益となる新たな利用には消極的とならざるをえない

利用者

あらゆる登録時に自明の理のことから具体的に何が起こるのかよくわからないものまで説明が膨大で、結局、サービスを手っ取り早く享受するために理解を放棄し、その後は放置している

「事前の完全性」から「常時の制御可能性」へ

米国：ホワイトハウスのビッグデータレポート、FTCのデータブローカーレポート
※通知と同意を中心とした規制から行為規制、情報へのアクセスの拡充
EU：データ保護規則
※データ対象者によるアクセスの権利、データポータビリティの権利

取得から利用、流通、廃棄に至る「データのライフサイクル」に対して、いつでも簡単に安全に閲覧し操作できる仕組みが必要

4. 常時の制御を可能とする仕組み

各事業者のパーソナルデータを 一か所で直接操作するポータル

メリット

- ①高い信頼性
- ②ワンストップの利便性

デメリット

- ①膨大な事業者への対応
フォーマットの統一、事業の秘密の保護
事業者認定が厳しくなる
- ②ポータルのセキュリティ・リスクが高い
- ③事業の多様性、発展性への対応が困難
- ④コスト負担が重い
- ⑤当該機関の監視が困難

民間では当該機関の恣意的操作の抑制や事業者間の相反する利害の調整が難しく、コスト負担による事業継続性にも不安があるため、公的機関もしくは予算処置のある第三者機関でなければ難しい。



**プライバシーへの影響が大きい
特定の領域へ適応**

パーソナルデータを操作する 各事業者のインフォメーションへ 誘導するポータル

メリット

- ①事業の多様性、発展性、独立性の保護
- ②低いコスト

デメリット

- ①信頼性の確保
参加事業者の適正性の認証
- ②利便性の確保
リンク先の操作、説明等の統一性
- ③当該機関の妥当性の保証が困難

プライバシー保護の責任はリンク先の各事業者にあるため、事業者への干渉やコストは抑えられ、民間でも可能。ただし、妥当性や強制力を担保するために、公的機関や消費者等の関与が必要。

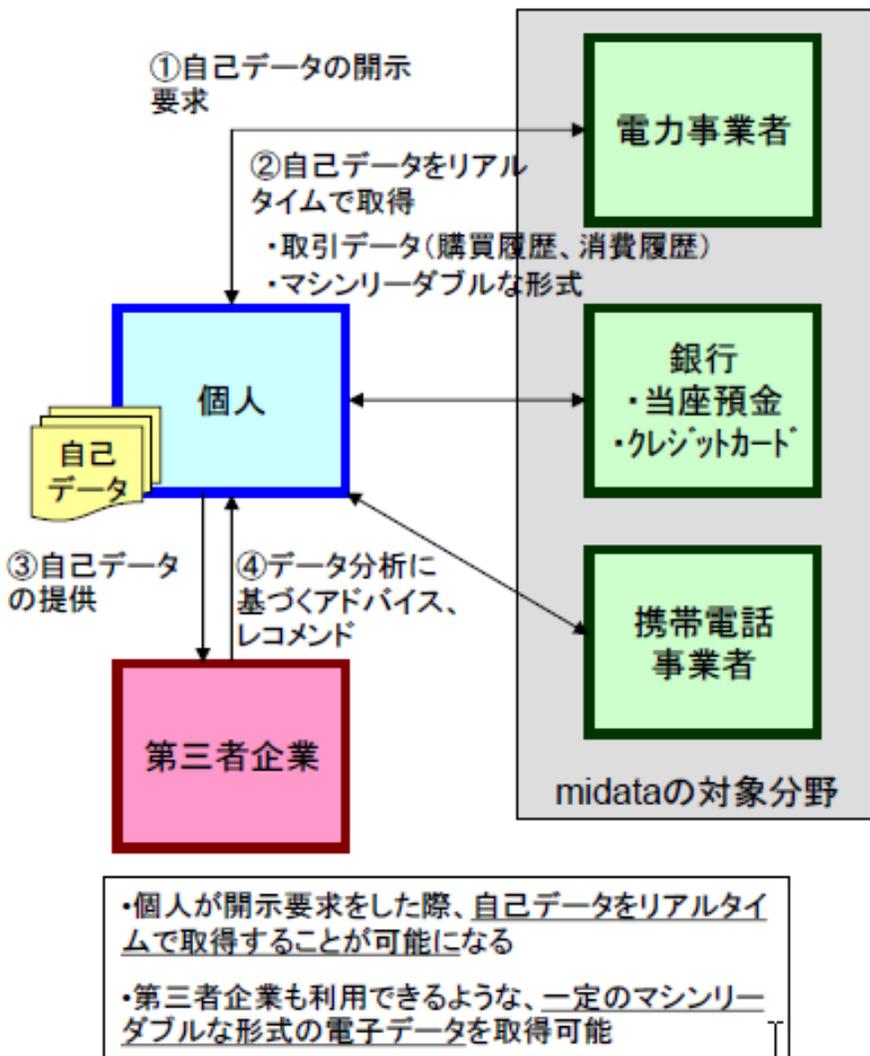


**対象事業者の多い
広範囲な領域へ適応**

5. 各事業者のパーソナルデータを一か所で直接操作するポータル

【英国：midata】

【米国：Smart Disclosure】



データの開示元	開示するデータの種類	
	製品やサービスに関するデータ	個人データ
公的分野	<p>II</p> <ul style="list-style-type: none"> ・Education.Data.gov(教育) ・Saferproducts.gov(製品情報) ・HealthData.gov(医療) ・Broadband Map(電気通信) ・DOT Data Inventory(交通) ・Energy.data.gov(電力) ・Finance Data Directory(金融) ・Food Environment Atlas(食品) <ul style="list-style-type: none"> ・College Navigator(教育) ・What's in the Food You Eat(食品) ・Healthcare.gov(医療) 	<p>I</p> <ul style="list-style-type: none"> ・Blue Button(医療) ・MyData(教育) ・my Social Security(社会保険)
非政府分野	<p>III</p> <ul style="list-style-type: none"> ・Billshrink.com(携帯電話) ・Hello Wallet(金融) 	<p>IV</p> <ul style="list-style-type: none"> ・Green Button(電力) ・Mint.com(金融)

データ開示
にシニアティブ

データ活用
ツール

多くの事業者が重複するため、各Disclosureのポータルが同様の仕様でなければ、事業者の負担は非常に大きくなる。

(本ページの出典：国際社会経済研究所)

6. パーソナルデータを操作する各事業者のインフォメーションへ誘導するポータル

個人情報保護法 / 個人情報保護委員会
各種ガイドライン / 監督官庁

必要条件

十分条件

インフォメーション
ポータル

事業者

事業者

事業者

自主規制として望ましい形だが、客観的な妥当性の根拠や消費者の信頼性を確保するのが難しい。

個人情報を含まないパーソナルデータの場合は統一されていないため、現状では監督官庁毎の業界単位にならざるを得ない？

【課題】

- ①業界毎にあるべきか、業界横断であるべきか？
- ②消費者の視点をどうやって反映させるのか？
- ③誰が誰を認定し、評価するのか？
 - ・ポータル運営者を認定するのか
 - ・ポータルに参加することを許可するために事業者を認定するのか？
- ④事業者の参加を促進するインセンティブとエンフォースメントは何か？

7. 消費者・事業者の双方がHappyな方法とは？

消費者の視点

簡単・便利に

- ・いつでもすぐに
- ・ワンストップで

法律・公的機関の裏付け（信頼性担保）

- ・便利＝安心・安全とは限らない
- ・ポータルの中で個別に信用確認は面倒
- ・大企業であっても信用できない

事業者の視点

負担の軽減

- ・システムの開発や改修を避けたい
- ・進化や変化に柔軟に素早く対応できる
- ・中小の事業者でも対応が可能

法律・公的機関のお墨付き（信頼性付与）

- ・冗長で複雑な対応を低減したい
- ・中小の事業者でも信頼を得ることが出来る

法律・公的機関が認める「信頼」のある仕組み

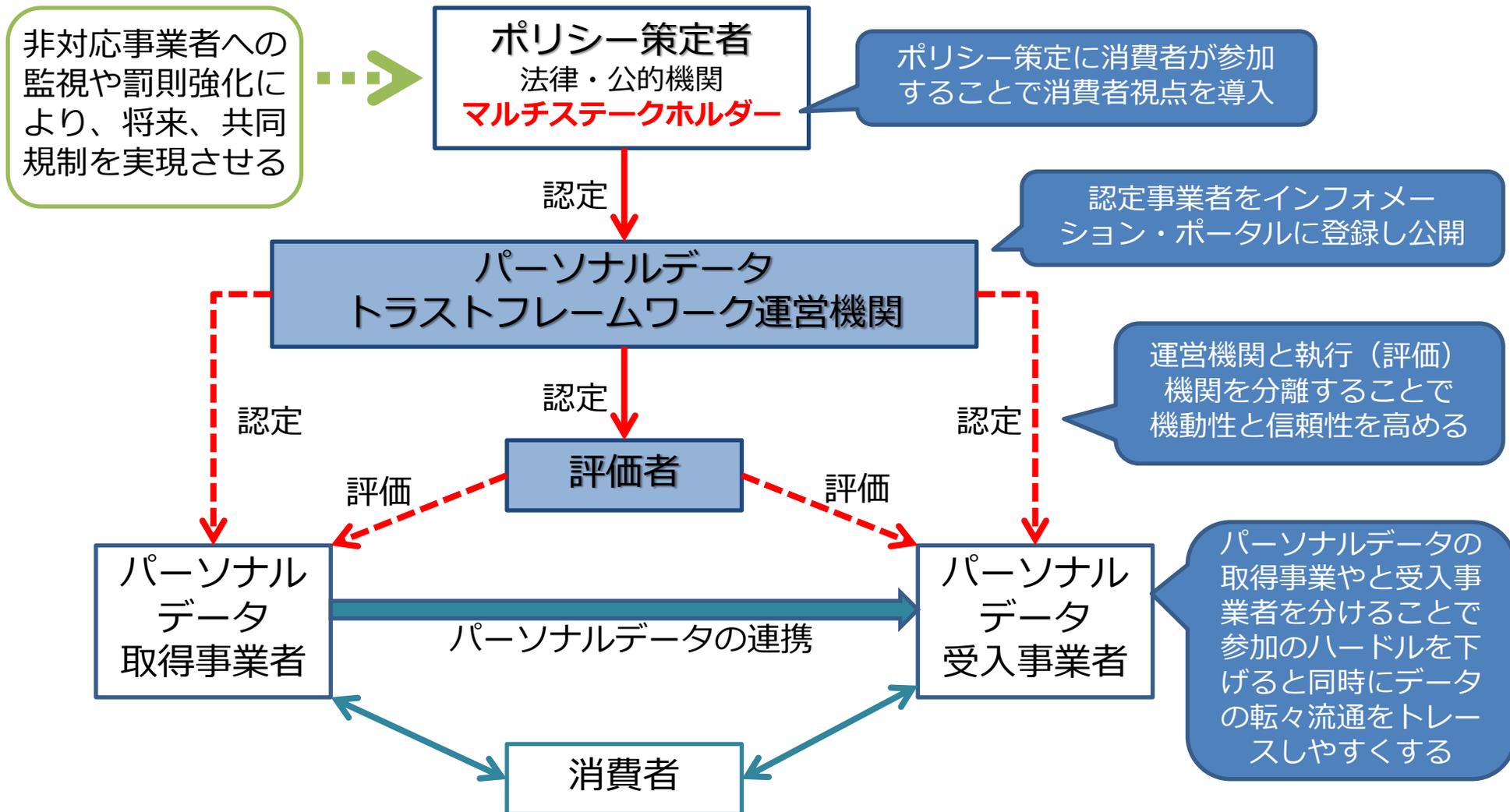
+

各事業者が柔軟に素早く、かつ過大な負担をかけずに対応できる仕組み

消費者は、まずはこのポータルを頼りにすれば良い
ポータルに登録されることが、信頼できる事業者であることの証
消費者による高度なコントロールはポータルから各事業者のインフォメーションへ

8. 信頼性のあるインフォメーション・ポータルの例（トラストフレームワーク）

ポータルを「信頼できるプログラム」で構築することにより、パーソナルデータの流通における消費者の不安、事業者間の不安を解消できるのではないか？



9. その他の課題

① 現実に即したプライバシー保護のための基準

必要条件：法律やガイドライン

十分条件：技術的・学術的な論理的完全性ではなく、様々な対策を行うことによる一般論的な十分性で考える

※企業がパーソナルデータを悪用して実質的な被害が発生した例は極めて稀。
ほとんどが、犯罪的行為のためのセキュリティ侵害。

② プライバシー侵害の救済措置

侵害されないようにすること、責任を事業者だけに負わせることに注力すると、安全サイドへ偏り、利活用が阻害される。突発的、偶発的な事故等のことも考えて、救済措置も必要。

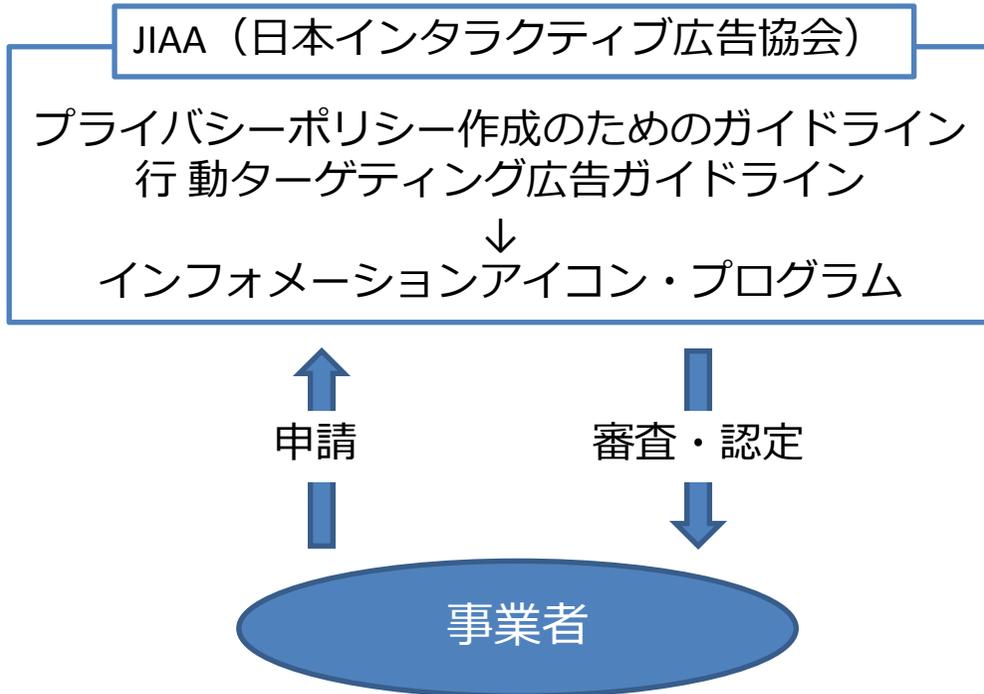
③ データ・トレーサビリティに関する技術開発の推進

データアクセス権、データポータビリティ権を実現するためには必須。

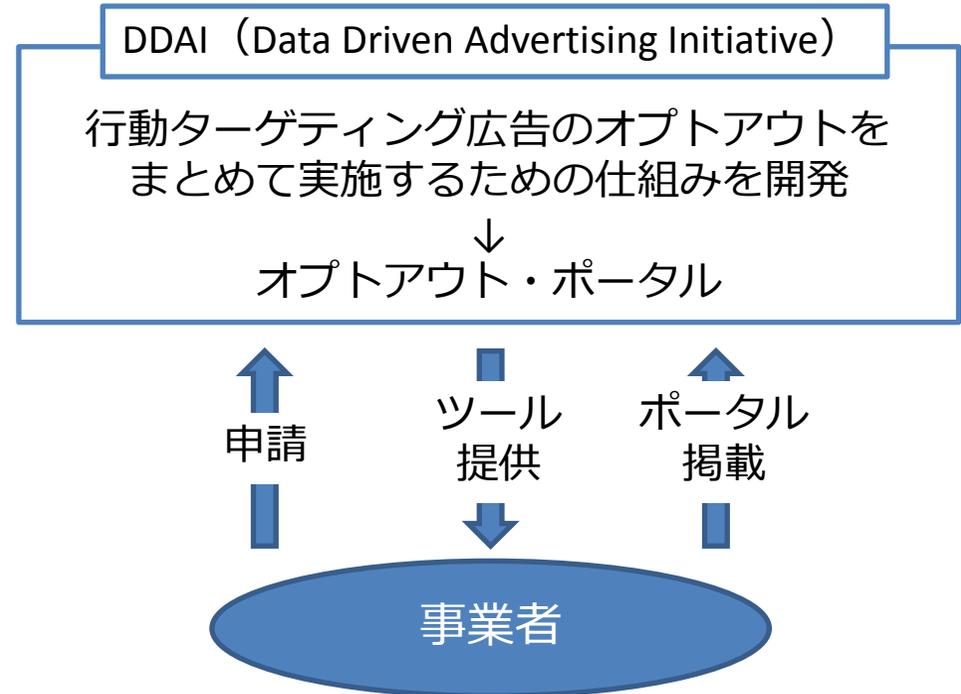
④ 消費者の権利と義務

パーソナルデータの利活用は、少子高齢化対策、地方活性化等、広く国民に資するものであり、よりよい社会システムを国民全体で考え、構築するための義務についても検討する必要。

(参考) 広告事業者の自主規制プログラム



広告へのインフォメーションアイコンの実装を認定する自主規制プログラム。アイコンをクリックすることにより各事業者のインフォメーションページへ誘導し、説明やオプトアウトが可能。ポータル等は存在せず、説明やオプトアウトの方法等は各事業者に任されているが、ガイドラインに則ったものであるかどうかの審査がある。



DDAIのサイトにて、登録事業者を選択して一括してオプトアウトを可能とする自主規制プログラム。DDAIの基準に合致すれば、DDAIのツールを実装することで、ポータルに掲載することが可能となる。

- P9 ホワイトハウスのビッグデータレポート（2014年5月）
 BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES
 https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf
- FTCのデータブローカーレポート（2014年5月）
 Data Brokers – A Call for Transparency and Accountability
 <http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>
- P16 JIAAガイドライン
 http://www.jiaa.org/archive/s_guideline.html
- DDAIオプトアウト
 <http://www.ddai.info/optout>