野村総合研究所

プライバシー保護に係る最近の動向

ーIoTへの対応と匿名加工情報の活用に向けてー

2015年11月6日

株式会社野村総合研究所
ICT・メディア産業コンサルティング部

小林慎太郎

IoT（Internet of Things）への対応

IoT（Internet of Things）時代は、これまでのインターネットサービスとM2Mが融合し、人、モノ、機械が、相互につながって、新たな製品・サービス・社会システムが生まれる。

利用者・デバイス　　通信　　サービス

これまでの（よく使う）
インターネットサービス：

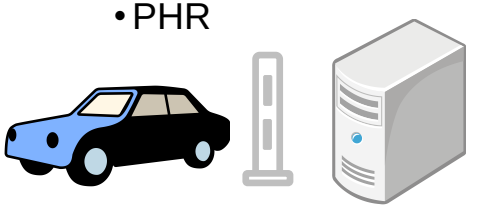
人が、PC等からウェブサーバへアクセスすることで
サービスが提供される。

- 電子メール
- 検索
- ソーシャルメディア
- ゲーム
- ・・・

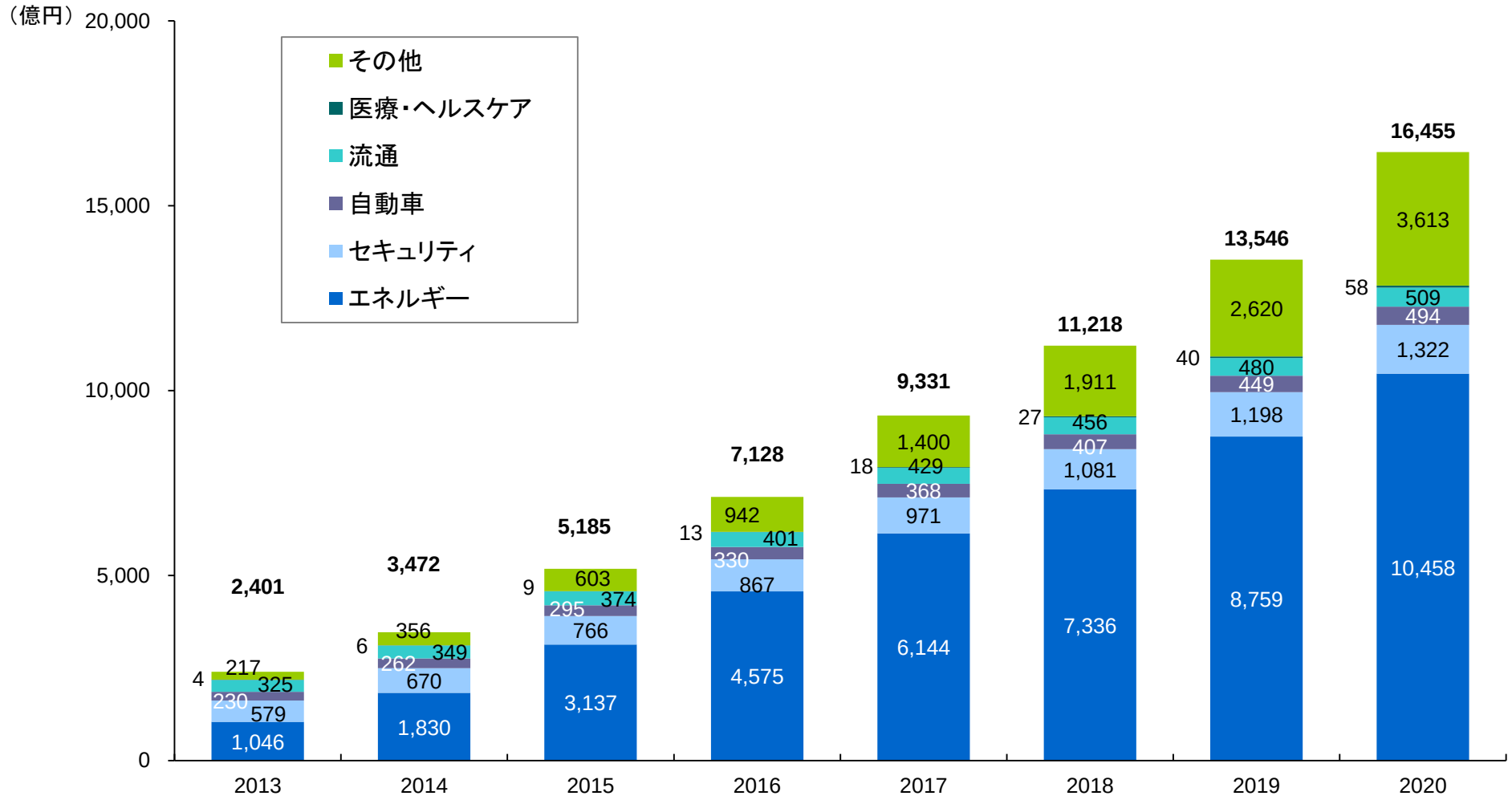
M2M（Machine-to -Machine）：

モノや機械が、お互いに
通信することで、サービス
が提供される。

- エネルギーマネジメント
- 遠隔監視
- ITS
- ｻﾌﾟﾗｲﾁｪｰﾝﾏﾈｼﾞﾒﾝﾄ
- PHR



国内のM2M市場の規模
エネルギー、セキュリティ、自動車、流通、医療・ヘルスケアの5つがメイン



出所）野村総合研究所「ITナビゲーター2015年版」2014年12月

エネルギー分野の事例： HEMS　電力の見える化サービスによって、節電を喚起。

サービスの概要

- 日々の消費電力量をグラフ表示するなど、視覚的に分かるように提示し、節電を喚起する。

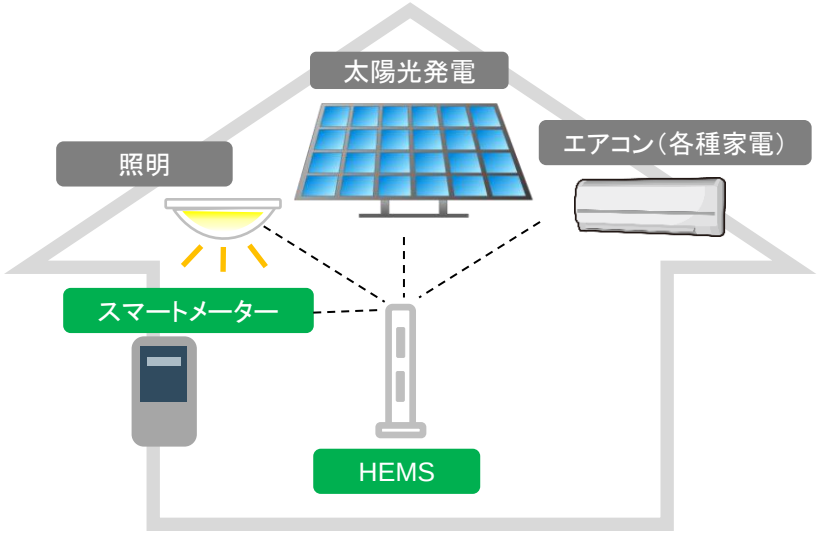
サービスの広がり

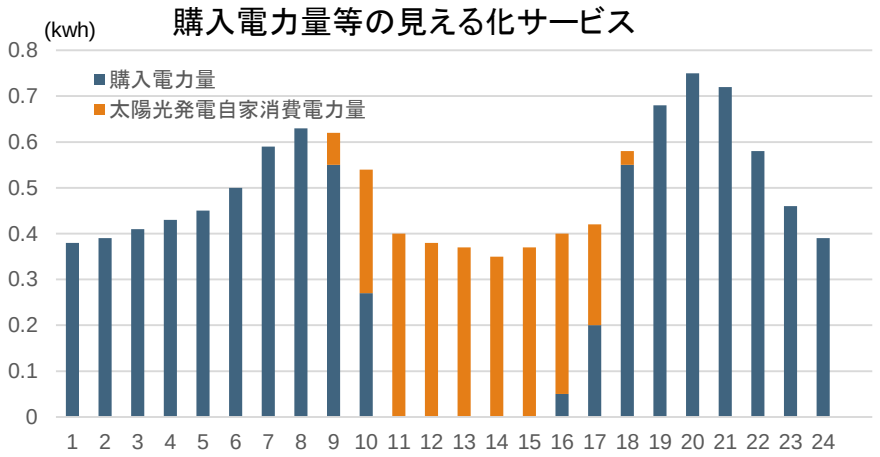
- デマンドレスポンス（電力需給の状況に応じて、家庭側で電力の使用を抑制。）
- 見守りサービス（消費電力量の変動を遠隔モニタリングし、異常を検知すると保護者に通知）
- 宅配の効率化（消費電力量から在／不在を判定して、在宅時間に配送）

プライバシーに関する考察

- 電力の波形グラフから、入浴時間等の生活パターンや在／不在の実態など、プライバシー性の高い情報が読み取れる。

HEMS（ホームエネルギー・マネジメントシステム）





自動車分野の事例：
Snapshot® 走行データによって自動車保険料を最適化（米Progressive社）

サービスの概要

- 走行実態から、事故リスクを判定し、ユーザごとの保険料の最適化を行う。
- 自動車に標準搭載されているメンテナンスポートから走行データを収集し、携帯電話網を通じてセンターに送信し。リスク判定する。

サービスの広がり

- 走行実態と合わせて車両の状態（走行距離、バッテリー充電量等）を取得することで、車両や部品の品質管理ができる。メンテナンスを効果的に行う。
- モニタリングを継続することで、品質保証が可能となり、中古市場の価格設定に反映できる。

プライバシーに関する考察

- 走行データから分かる移動履歴、ドライバーの運転の技能や癖の情報には、プライバシー性が高い。
- 自動車の車体番号は不変のため、中古市場で取引されると、前のオーナーの情報も車体番号にひもづいてトレースされる可能性がある。

デバイス

装着は簡単

参照データ（一部）

Date	Trips	Driving time (hr:min:sec)	Mileage	Hard brakes	Speed chart
[+] Friday, 08/19/2011	3	00:38:05	22.87	1	
[+] Wednesday, 08/17/2011	1	00:04:01	0	0	
[+] Monday, 08/15/2011	2	00:38:06	22.73	0	
[+] Sunday, 08/14/2011	3	00:42:53	18.3	0	
[+] Saturday, 08/13/2011	3	00:37:33	22.88	0	
[+] Tuesday, 08/09/2011	5	01:12:37	42.37	0	
[+] Monday, 08/08/2011	6	01:53:23	78.2	0	
[+] Saturday, 08/06/2011	10	02:16:04	76.51	2	
[+] Friday, 08/05/2011	2	00:34:03	22.77	0	

出所）Progressive

セキュリティ分野の事例： 映像センサー（監視カメラ）による行動追跡

サービスの概要

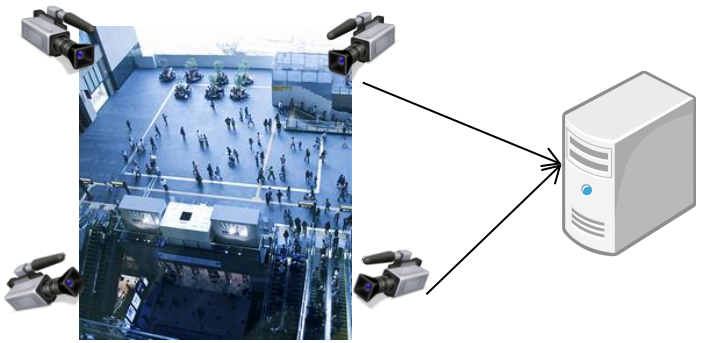
- 映像センサーによって、個体を識別し、施設内での行動を追跡することで、人流・滞留の実態を把握し、設備や商品の再配置、動線計画に利用する。
- 個体識別は、機械的に顔や動作の特徴を解析して行う。

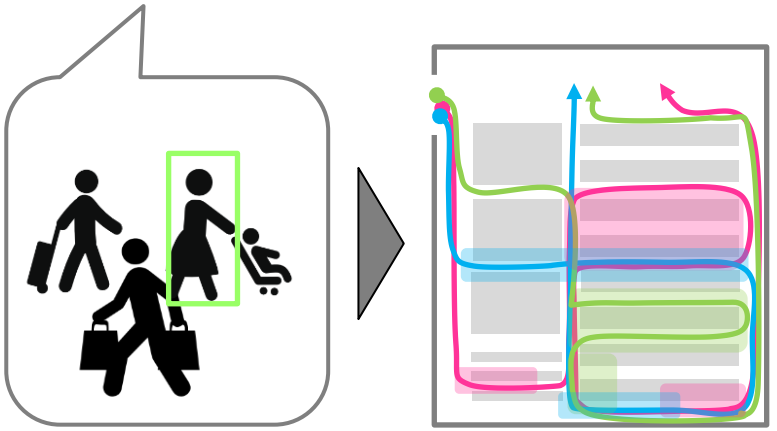
サービスの広がり

- 災害時の避難計画の立案・見直し。
- 不審な行動をする人物を検出して、管理者に警告を発する。

プライバシーに関する考察

- 映像センサーによる撮影に際し、本人が撮影を回避する手段が無い一方で、明示的な同意を取得することが難しい。
- 取得されたデータに対して、本人が閲覧したり、修正したりすることが難しい。





映像センサーによる
個体識別、追跡

人流、滞留の実態を
見える化

欧米におけるIoT×プライバシーの議論

欧州連合（EU）

- 2014年9月に、EUデータ保護専門部会は、IoTの動向に関する意見を公表し、IoTにおけるプライバシー/データ保護の課題に対する意見を表明。
  - ウェアラブル端末、状態・活動測定計（Quantified Self）、ホームオートメーション（スマート家電等）の3つの製品・サービスを対象に評価。
  - 「コントロールの喪失と情報の非対称性」「ユーザ同意の品質低下」「属性推定データと処理の目的変更」等の課題を指摘。
  - その上で、EUデータ保護指令、EU電子プライバシー指令への対応のあり方を提示。

出所）ARTICLE 29 DATA PROTECTION WORKING PARTY ” Opinion 8/2014 on the on Recent Developments on the Internet of Things”（2014年9月16日）

米国

- 2015年1月に、連邦取引委員会は、IoTへのプライバシーとセキュリティ対応のあり方に関するスタッフレポートを公表。
  - IoTの便益として、ヘルスケア、ホームオートメーション、自動車を例に挙げて評価。
  - プライバシーリスクへのベストプラクティスとして以下を推奨。
    - データ最小化： 保管するデータの最小化、速やかな消去、匿名化
    - 通知と選択： 同意取得の方法を選択肢を上げて解説。なお消費者の合理的期待の範囲内であれば同意取得が不要。また、データ取得後に速やかに匿名化を行えば同意取得は不要。
  - IoTは発展途上にあるとして、現状では、IoTに特化した新たな立法は不要と判断。

出所）FTC Staff Report “Internet of Things Privacy & Security in a Connected World”（2015年1月）

今後の議論に向けた整理

1. 通知と同意の取得
   - 監視カメラ等、実質的に事前の同意取得が困難な場合がある。
   - 今後、身の回りのセンサーの数が飛躍的に増大し、個別の意思確認が困難になる可能性がある。

2. 本人のデータへの関与
   - スマート家電等、機器・デバイスがデータを収集する一方で、その事実を本人は十分に認識していない、できない場合がある。また、取得されたデータに対して、本人がアクセスしたり、訂正したりすることが難しい場合がある。

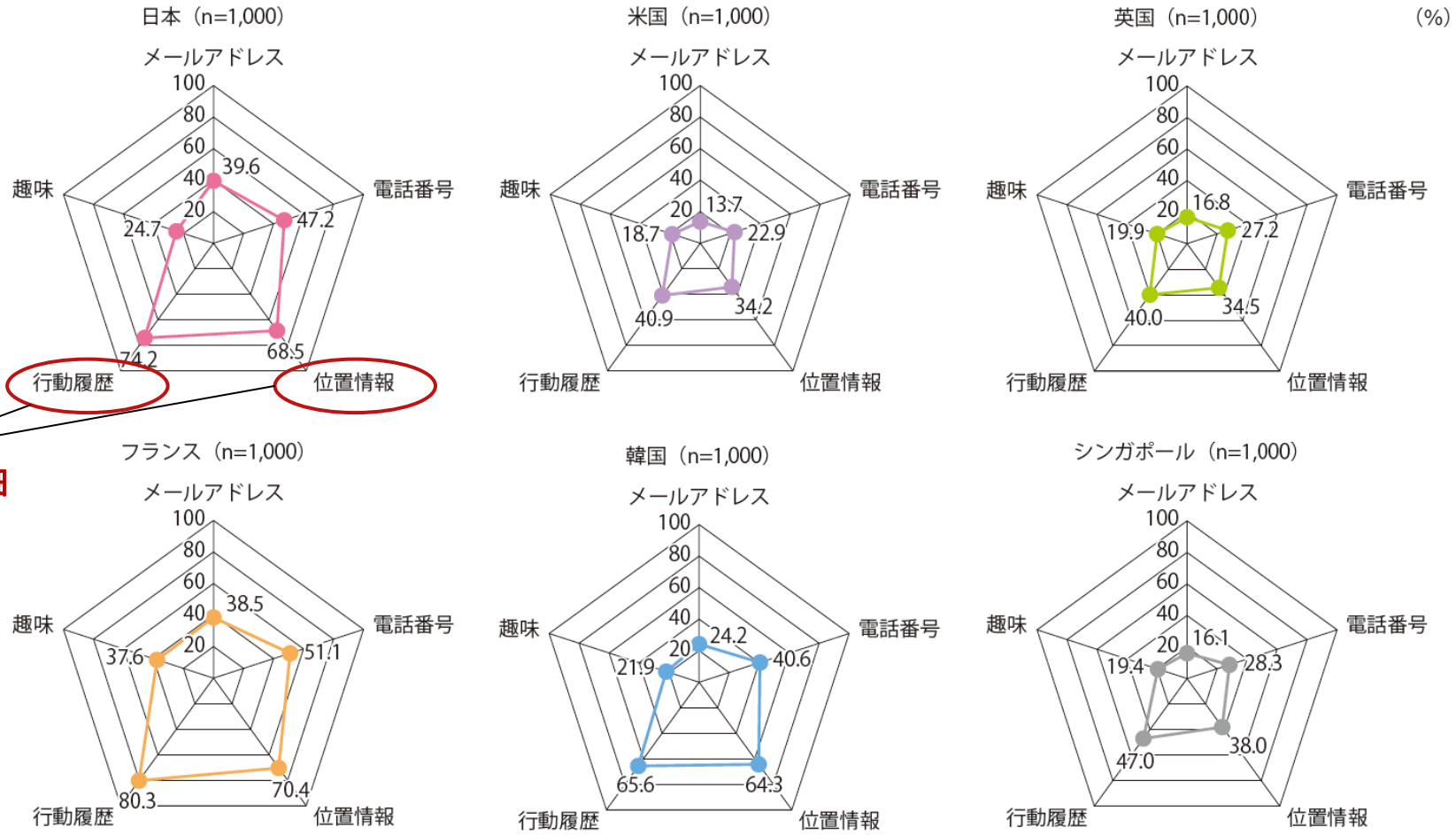
3. 個人の行動履歴の蓄積・プロファイリング
   - PCや携帯電話に加え、家電、自動車、健康機器などから個人の行動履歴データが集約できるようになり、生活パターンや本人の趣味嗜好、行動範囲など、プライバシー性の高い情報が蓄積され、精度高くプロファイリングされる。

4. モノに紐付いて管理されるデータの取扱い
   - 転売等により、モノが本人の手を離れた後も、モノのIDに紐付いて管理されるデータが残る場合がある。
     Ex.賃貸住宅のスマートメータのID、中古車市場にある自動車のID等に紐付いて管理されるデータ。

5. モノから取得したデータに対する個人情報、通信の秘密への該当性（そもそも）
   - プローブ情報等、特定の個人を識別しないで利用されるケースは、往々にしてある。

（参考） 行動履歴や位置情報は、電話番号よりも他人に知られたくない情報

どのような場合でも提供・公開したくないデータの種別

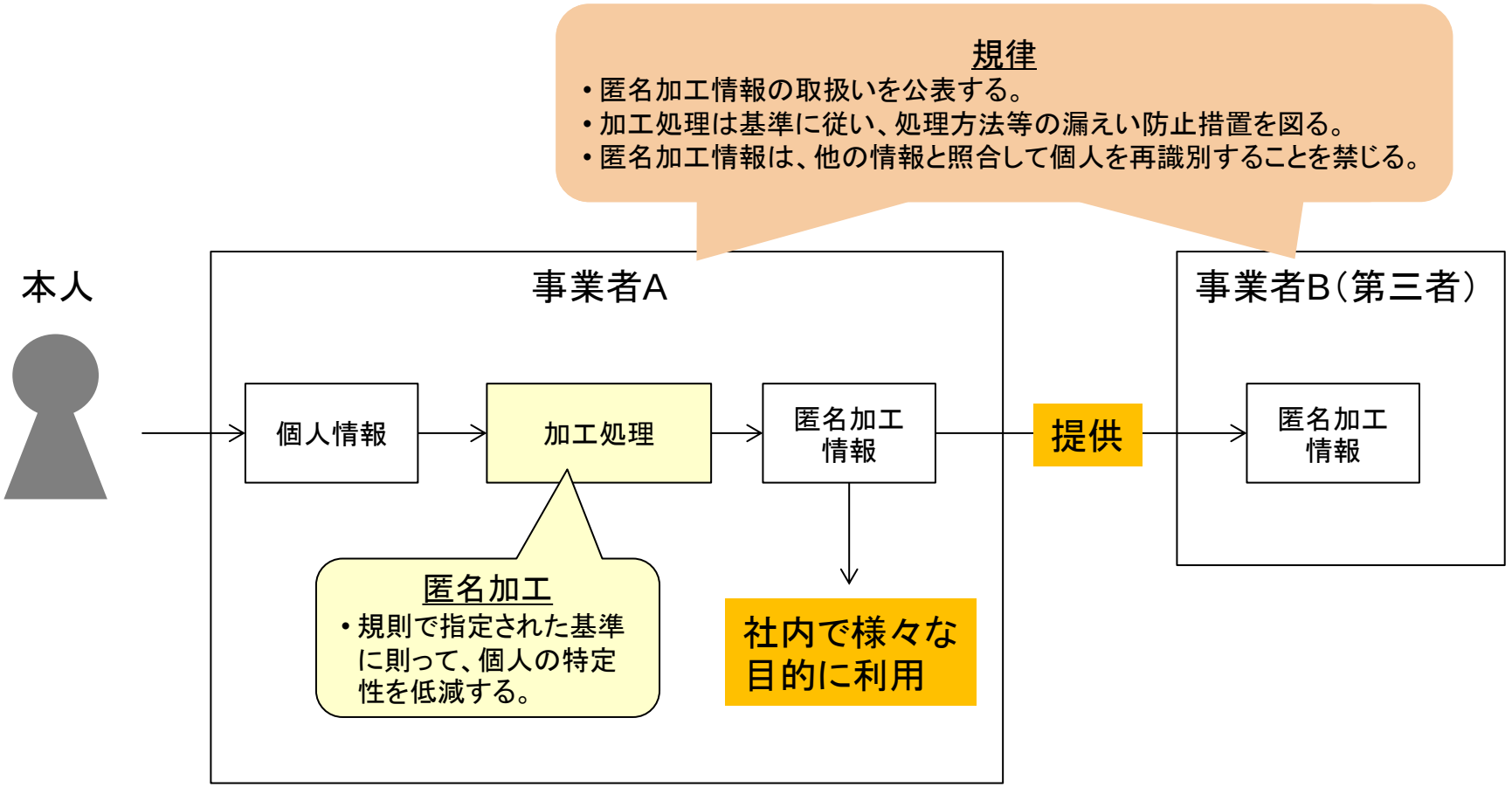


IoTは、より詳細な把握が可能

出所）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（2013年）

匿名加工情報の活用

個人情報保護法の改正によって、本人の同意がなくてもデータの利活用を可能とする枠組み「匿名加工情報」が整備された。



匿名加工情報として活用が見込まれる情報

- IoT領域のデータ全般
  - スマートメーター／HEMS
  - スマート家電（照明、エアコン、冷蔵庫、テレビ）
  - 自動車
  - 映像センサー（監視カメラ）
  - 流通
  - 医療・ヘルスケア
- 電子商取引（EC）データ
  - ウェブ閲覧履歴
  - 購買履歴
  - クレジットカード
- 移動データ
  - 携帯電話の位置情報
  - 鉄道の乗降履歴情報

異分野データを組み合わせて活用することで、新たな付加価値を生み出すことが期待される。

（参考）クレジットカードデータの匿名加工のイメージ（経済産業省実証事業より）

ローデータ

ID	氏名	性別	年齢	住所	職業	店舗	利用履歴	年間利用額
10001	野村太郎	男	28	埼玉県さいたま市〇〇町1-6-5	会社員	三越新宿店	18,000円（2014年 1月 3日） 9,000円（2014年 1月 9日）	241,056円
10002	佐藤一郎	男	58	東京都練馬区〇〇町5-8-13	公務員	高島屋新宿店	160,000円（2014年 1月 2日） 120,000円（2014年 1月25日）	669,600円
10003	山田花子	女	42	神奈川県横浜市港北区〇〇町9-3-1	自営業	高島屋二子玉川店	300,000円（2013年12月23日） 260,000円（2013年12月25日）	4320,000円
10004	曽我和子	女	37	栃木県さくら市1210	会社員	ユニクロ池袋店	9,200円（2013年12月20日） 9,200円（2014年 1月20日）	107,784円
10005	大田二郎	男	66	山梨県甲府市3-5	無職	ユニクロ新宿西口店	50,000円（2014年 1月 2日） 30,000円（2014年 1月 3日）	108,000円
…	…	…	…	…	…		…	…

匿名加工データ

ID	氏名	性別	年齢	住所	職業	店舗	利用履歴	年間利用額
XY03		男	20代	埼玉県さいたま市	会社員	百貨店	18,000円（2014年 1月 3日） 9,000円（2014年 1月 9日）	～50万円
PQ72		男	50代	東京都練馬区	公務員	百貨店	160,000円（2014年 1月 2日） 120,000円（2014年 1月25日）	50～100万円
AB97		女	40代	神奈川県横浜市	自営業	百貨店	300,000円（2013年12月23日） 260,000円（2013年12月25日）	400～450万円
MN36		女	30代	栃木県さくら市	会社員	衣料店	9,200円（2013年12月20日） 9,200円（2014年 1月20日）	～50万円
EF14		男	60代	山梨県甲府市	無職	衣料店	50,000円（2014年 1月 2日） 30,000円（2014年 1月 3日）	～50万円
…		…		…			…	

仮名化

加工 (k-匿名)

加工（曖昧）

非加工 (制限)

加工（外れ値）

出所）経済産業省事業「平成26年度我が国経済社会の情報化・サービス化に係る基盤整備（パーソナルデータ利活用に関するマルチステークホルダープロセスの実施方法等の調査事業）報告書」野村総合研究所（2015年3月）

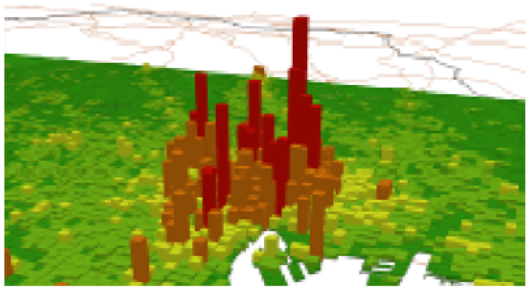
（参考）携帯電話の位置情報は、現状では統計データとして提供されている。匿名加工情報の枠組みの利用によって、より詳細なデータの提供が期待される。

＜事業者によるサービスの実証事例＞

○NTTドコモ「モバイル空間統計」

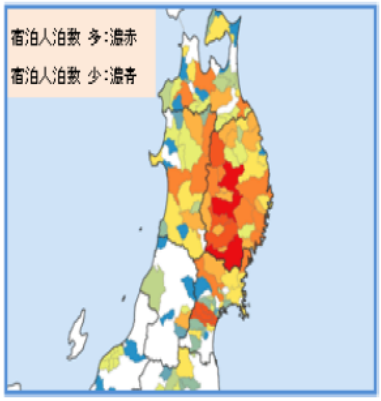
基地局に係る位置情報を利用し、基地局エリア毎の携帯電話台数を利用者の属性別に集計することによって、人口の地理的分布を推計したもの。地域毎の人口分布や、性別・年齢層別・居住エリア別の人口構成などの統計情報知ることが可能。

通信の秘密に該当する位置情報は利用されていない。また、複数地点間の移動に係る情報（誰が、どこからどこへ、何時ころ）など、詳細な位置情報は利用されていない。



○KDDI・コロプラ「観光動態調査レポート」

個別の通信に含まれる位置情報（「通信の場所」の情報）を統計処理し、調査結果を地方自治体等に提供。移動経路・行動範囲を分析したエリアマーケティングなどを行うことが可能。利用者から個別に明確な同意を得ている。



出所）総務省　個人情報・利用者情報等の取扱いに関するWG（第4回）資料「位置情報に関するプライバシーの適切な保護と社会的活用の両立に向けた実証実験」（2015年4月）から抜粋