資料2

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
議論の取りまとめの方向性（案）

平成２８年６月８日
事務局

Ⅰ　位置情報の取扱いについて

Ⅱ　スマートフォンの利用者情報の取扱いについて

Ⅲ　電気通信事業分野ガイドラインのその他の改正事項について

Ⅳ　IoTとプライバシーについて

Ⅰ　位置情報の取扱いについて

Ⅱ　スマートフォンの利用者情報の取扱いについて

Ⅲ　電気通信事業分野ガイドラインのその他の改正事項について

Ⅳ　IoTとプライバシーについて

1　位置情報プライバシーレポートについて

○　電気通信事業者が保有する位置情報は、パーソナルデータとしての適切な利活用が高く期待される。

○　これを受け、総務省は「緊急時等における位置情報の取扱いに関する検討会」において、電気通信事業者が取得する位置情報について、通信の秘密や個人情報、プライバシーを適切に保護しつつ、利活用を促進するための整理を行い、「位置情報プライバシーレポート」（以下「レポート」という。）として公表（平成26年7月）。

○　レポートでは、①位置情報の取得・利用・第三者提供には個別かつ明確な同意取得が必要、②「十分な匿名化」がされた位置情報については利用者の同意なく利用・第三者提供することが可能と考えられる、③「通信の秘密」に該当する位置情報については、「十分な匿名化」を行って利用・第三者提供する場合であっても同意が必要だが、一定の場合には契約約款等に基づく包括同意も許容されると考えられる等の整理がなされた。

○　また、①「十分な匿名化」の水準についての検討（とりわけ、通信の秘密に該当する位置情報について、具体的ケースを用いた実証の必要性を指摘）、②通信の秘密に該当する位置情報について、加工の方法・管理運用体制の適切性の評価・検証の在り方についての検討、③公的分野における位置情報の利用目的・主体・取扱い方法に応じたプライバシー上のリスクや利用者の受容度等とこれに応じた取扱いの在り方についての実証等が必要とされた。

○　そして、これらの実証や、個人情報保護法の改正を踏まえ、位置情報の取扱いを電気通信事業分野ガイドラインに反映させることが適当とされた。

○　さらに、移動体端末から取得される利用者の位置情報については、その高いプライバシー性から強く保護が求められるものであり、電気通信事業者以外の事業者においても、レポートを踏まえた取扱いが期待されるとされた。

2　位置情報の利活用に係る実証の結果概要

○ レポートの提言を受け、総務省は、平成27年度に、電気通信事業者が保有する「通信の秘密」に該当する位置情報について、事前の包括同意に基づき「十分な匿名化」を行い、利活用することについての実証を実施した。

※ 実証に当たって、協議会（座長：森亮二弁護士）を開催。

○ 実証の結果

（1）十分な匿名化の水準

- 防災、交通、観光等の公的分野や、商用分野での利活用が想定されるユースケースを4件設定し、それぞれのユースケースにおいて適切と考えられる匿名化の加工を行った。

※ レポートでは、包括同意に基づき、通信の秘密に該当する位置情報の「十分な匿名化」を行い、利用・第三者提供する場合において、対象となる情報の範囲を「通信の場所、日時及び利用者・端末識別符号」に限定する整理を行っているが、実証では、加工後のデータの有用性の観点から、これらに属性情報（市区町村までの住所、性別、年齢）を加えて実施した。

- これらのユースケースの検証を通じて、「十分な匿名化」に係る要件を整理した。その主な内容は以下のとおり。

① 加工を始める際の入口要件

直接識別子は削除する。仮IDの生成に当たっては、可能な限り短い有効期限を設ける、ハッシュ化等の一方向の置き換えを行うといった措置を講じる。

② 加工を終える際の出口要件

- 原則として、同一時刻のすべての間接識別子について非識別、かつ、すべての時間を通じた履歴において非識別
- 特定の個人が識別されるリスクを定性的に評価するに当たり、評価指標に以下を含める：
  1）データの項目、2）場所の特性、3）利用者の特性、4）取得期間・時期、5）位置データの精度、
  6）追跡可能な移動履歴の長さ・仮IDの有効期間、7）データを取得する際の時間間隔、8）標本数

③ 加工途中の管理運用体制の要件

「アクセス管理」、「持ち出し制限」、「外部からの不正アクセス防止のための措置」、「データの保管方法」、「苦情・問合せ窓口の設置」の各観点からの実施内容を整理。

(2)加工の手法・管理運用体制の適切性の評価・検証の在り方

位置情報に関するリスク対策をデータのライフサイクルを通じて評価すべく、PIAの評価項目、評価手順を策定。

評価項目:

1)全般的事項、2)データの取得(抽出)、3)データの匿名化のための加工、4)データの保管、5)データの提供、6)データの消去

(3)同意取得の方法等

包括同意の上で利活用するに当たり、プライバシー上のリスクについて利用者の理解と信頼を得る等の観点から、包括同意約款、Web等での説明事項、業界としての位置情報取扱いポリシー、一般的な電気通信の仕組みと位置情報の収集に関する説明について検討。

3　本タスクフォースでの主な意見

【実証に対する評価】

- プライバシーの保護は匿名化だけで語るべきではなく、本実証においては、PIA等を含む多角的な検証が行われている点で評価できる。また、匿名加工情報として一般に想定されているものよりも、プライバシー保護に寄せた加工が行われていると考えている。
- 本実証では、データ取得から短期間で分析結果を提供等することを想定していなかったため、「情報の取得時期と利活用時期の時間間隔」をリスク評価指標に含めていないが、一般論としては、指標に含めるべき。
- 本実証では、場所、時間、性別、年代を組み合わせ、場合によってはこれらに移動履歴を組み合わせても、多くの人たちが概ね同じ行動をしていてプライバシーが守られつつ、行動分析も可能なデータが作成できるということが明らかになった。他方、本実証でも、匿名の度合いとデータの有用性のトレードオフの関係は出ており、有用性と安全性のバランスに関しては、引き続き検討していく必要がある。
- k-匿名性のkの値は、学術的には、個人の特定やプライバシー保護の観点で評価することが多いが、本実証では、データの有用性の観点からもkの値を評価している点で、評価できる。データの保護と有用性のトレードオフについては、移動履歴であれば出発点、目的地、移動途中においてプライバシーに対する考え方が異なるなど、状況に応じて変動するものなので、より細かい匿名化の方法はあり得るのではないか。今後の検討に当たっては、統計分野の専門家の知見を役立てると、より精緻な議論ができるのではないか。

【実証を受けての対応】

- 今回の実証は、位置情報プライバシーレポートの宿題に答える形で、通信の秘密について、包括同意により十分な匿名化を行い、安全に利用することについて検証した。今後、レポートの内容、すなわち、十分な匿名化や、包括同意について電気通信事業分野ガイドラインに位置づけるべきではないか。電気通信事業分野ガイドラインの性質上、詳細な規定を行うのは難しいと考えられるので、事業者においてマルチステークホルダープロセスにより、詳細なルールを作っていくべきではないか。

- 位置情報プライバシーレポートの内容を電気通信事業分野ガイドラインに反映させて行くとして、今後、個人情報保護委員会が個人情報や匿名加工情報の取扱いを所管するようになると、事業者としては、総務省と個人情報保護委員会のどちらに問い合わせるべきか分からなくなるのではないか。このため、認定個人情報保護団体が、電気通信事業分野ガイドラインと、個人情報保護委員会が作成する一般ガイドラインの両方を取り込んだ個人情報保護指針を作成し、事業者からの質問に対応していくことが必要ではないか。
- 「十分な匿名化」と「『十分な匿名化』をした情報をどう使うか、誰に渡すか」の関連について、整理する必要。加工水準と、提供目的・提供先が関連することもあり得るのではないか。位置情報と契約者情報を組み合わせること等を想定すれば、「一定の基準で加工すれば、何に使っても良く、誰に渡しても良い」とすべきではない。匿名加工情報は、「公表」を行う等の規律に従えば、何に使っても良く、誰に渡しても良いという緩やかな縛りだが、電気通信分野の位置情報については、「公表」以上の一定の縛りが必要ではないか。

【包括同意について】

- 情報の提供先や利用目的を限定するような、サブカテゴリカルな包括同意も検討し得るのではないか。誰に、何のために情報を渡し、本人にどのようなメリット・デメリットがあるかを示すことが重要。また、「要件が厳しい分、効果は手厚くなる」のであり、同意手続を簡易にして何にでも使うというわけにはいかないのではないか。

【その他】

- 次世代GPSなど、技術の進展により位置情報の精度が大幅に向上する等の事情が想定されるため、これを踏まえた検討も必要
- 位置情報プライバシーレポートにおいて、「十分な匿名化」は、個人情報保護法の議論の過程で提案され、結局は規定されることのなかった「個人特定性低減データ」と対比されるものとして書かれている。改正個人情報保護法に規定された「匿名加工情報」と「個人特定性低減データ」は異なるものであり、位置情報プライバシーレポートの内容は、アップデートが必要ではないか。

4　検討事項（案）

- レポートでは、実証や個人情報保護法の改正を踏まえ、位置情報の取扱いを電気通信事業分野ガイドラインに反映させることが適当とされており、今般、一定の実証が行われたが、位置情報の取扱いを電気通信事業分野ガイドラインに反映させるべきか。
- 反映させる場合、電気通信事業分野ガイドラインには何を規定すべきか。例えば、本実証の結果を踏まえ、「十分な匿名化」の水準に係る要件、加工の手法・管理運用体制の適切性の評価・検証の在り方、同意取得の方法等について規定することが考えられるか。また、電気通信事業分野ガイドラインを受けた詳細な内容を認定個人情報保護団体による個人情報保護指針や業界の自主ガイドラインで規定していくことも考えられるか。その場合、どのような手続で策定していくことが適当か。
- 本実証は通信の秘密に該当する位置情報を対象としたが、電気通信事業者が取り扱う位置情報のうち、通信の秘密に該当しない位置情報については、どのように対応していくべきか。
- 改正個人情報保護法の下での「匿名加工情報」と「十分な匿名化」の関係についてどう考えるか。
- 電気通信事業分野ガイドラインは、電気通信事業を行う者をその対象とするが、通信端末を介して取得される位置情報は、これにとどまらない多様な者によって活用され得る。これらの者による位置情報の安全な活用については、どう考えるべきか。
- 更に、位置情報の有効な利活用を促進するためには、安全性を確保した上で、多様なプレイヤーが位置情報を活用できる環境が重要ではないか。

5　取りまとめの方向性（案）

【総論】

- 今般、レポートを受けた実証により、「通信の秘密」に該当する位置情報に加工を施して個人の再特定化・再識別化のリスクを十分に軽減し、かつ、一定の有用性が維持されるユースケースが示された。また、加工の手法・管理運用体制の適切性の評価・検証（PIA）の在り方や、包括同意の上で利活用を行うに当たっての同意取得や利用者への周知・説明の方法等が検討された。
- これを受け、電気通信事業者が保有する位置情報の利活用を促す観点から、官民が連携して、レポートの内容や本実証の結果を反映した位置情報の利活用ルールを策定していくべきではないか。
- 具体的には、電気通信事業分野ガイドラインに基本的な規律を規定することとし、詳細な規律については、認定個人情報保護団体による個人情報保護指針又は業界の自主ガイドラインにおいて規定していくべきではないか。
- 個人情報保護指針や業界の自主ガイドラインの策定に当たっては、マルチステークホルダープロセスを活用していくことが重要ではないか。
- 官民のルールが位置情報の利活用の態様や技術の変化等に対応した適切なものであり続けるよう、それぞれの策定主体が緊密に連携していくことが必要ではないか。

【電気通信事業分野ガイドラインへの反映】

- 電気通信事業分野ガイドラインにおける位置情報の取扱いに係る規定を拡充するべきではないか。具体的には、以下を規定していくことが考えられるのではないか。
  - レポートで示された位置情報の取扱いに係るルール（位置情報の取得、利用又は第三者提供には個別かつ明確な同意が必要である旨、同意取得に際して利用者に表示・説明すべき事項、「十分な匿名化」を行った場合の取扱い等）
  - 「十分な匿名化」に当たっての原則的な要件（入口要件、出口要件、管理運用体制の要件等）に係る基本的な考え方
  - 加工の手法・管理運用体制の適切性の評価に係る基本的な考え方
  - 通信の秘密に該当する位置情報を包括同意で利活用するに当たっての同意取得や利用者への周知・説明の方法等に係る基本的な考え方
- 包括同意に基づき通信の秘密に該当する位置情報に「十分な匿名化」を行う場合における加工対象について、本実証により、「市区町村までの住所、性別、年齢」を含めてデータ加工を行った場合においても「十分な匿名化」が可能であることが確認できたことを踏まえると、加工対象に「市区町村までの住所、性別、年齢」を含めることは許容され得ると考えられるのではないか。

  ただし、この他の属性情報の中には機微性の高いものも含まれることから、加工対象を更に拡大することについては、慎重な検討が必要ではないか。

【ガイドラインの下での民間ガイドラインの策定】

- 「十分な匿名化」の具体的水準については、利活用のニーズや社会的な有用性が高いと考えられる事例について、電気通信事業分野ガイドラインで示す原則的ルールの下で、今般の実証結果も踏まえつつ、また、今般の実証で残された課題についての検討を行い、できる限り、認定個人情報保護団体による個人情報保護指針又は業界の自主ガイドラインにおいてルールを規定していくべきではないか。
- 「十分な匿名化」の水準のほか、同意取得や、利用者への周知・説明の方法、PIAの具体的な方法についても、認定個人情報保護団体による個人情報保護指針又は業界の自主ガイドラインにおいて詳細なルールを策定していくべきではないか。

【通信の秘密に該当しない位置情報の取扱い】

- 電気通信事業者が取り扱う位置情報のうち、通信の秘密に該当しない位置情報については、現状においても高いプライバシー性を有し、通信と密接に関連する事項であるほか、今後の技術進展によって一層高いプライバシー性を有することになると想定されることにも鑑み、通信の秘密に準じた規律内容としていくことが適当か。

※　現行の電気通信事業分野ガイドラインでは、「位置情報を通信の秘密に該当しないと解する場合であっても、ある人がどこに所在するかということはプライバシーの中でも特に保護の必要性が高い上に、通信とも密接に関係する事項であるから、通信の秘密に準じて強く保護することが適当である」として、位置情報の外部提供について、通信の秘密への該当性の有無にかかわらず、同じ要件を課している。

【改正個人情報保護法との関係の整理】

- 電気通信事業分野ガイドラインを改正するに当たっては、改正個人情報保護法の下で整備される政令、規則、ガイドライン等と整合的なものとしていく必要がある。
- 特に、匿名加工情報については、今後、改正法の施行に向けて規則等で詳細が規定されていく予定であり、規則等の整備に当たって、総務省は、個人情報保護委員会とも連携しつつ、「十分な匿名化」と「匿名加工情報」の関係等の整理を行っていくべきではないか。

【電気通信事業を行う者以外の者による位置情報の利用について】

- 位置情報の匿名化に係る今般の検討は、政府内では先進的なものであると考えられ、電気通信事業を行う者以外の者による位置情報の利用に関しても、その検討結果が役立てられることが期待される。総務省は、このような者による位置情報の利用に関しても、プライバシーが適切に保護され、事業者にとって使いやすいルールが整備されるよう、個人情報保護委員会をはじめとした関係省庁や、認定個人情報保護団体等の関係団体と連携を図っていくべきではないか。

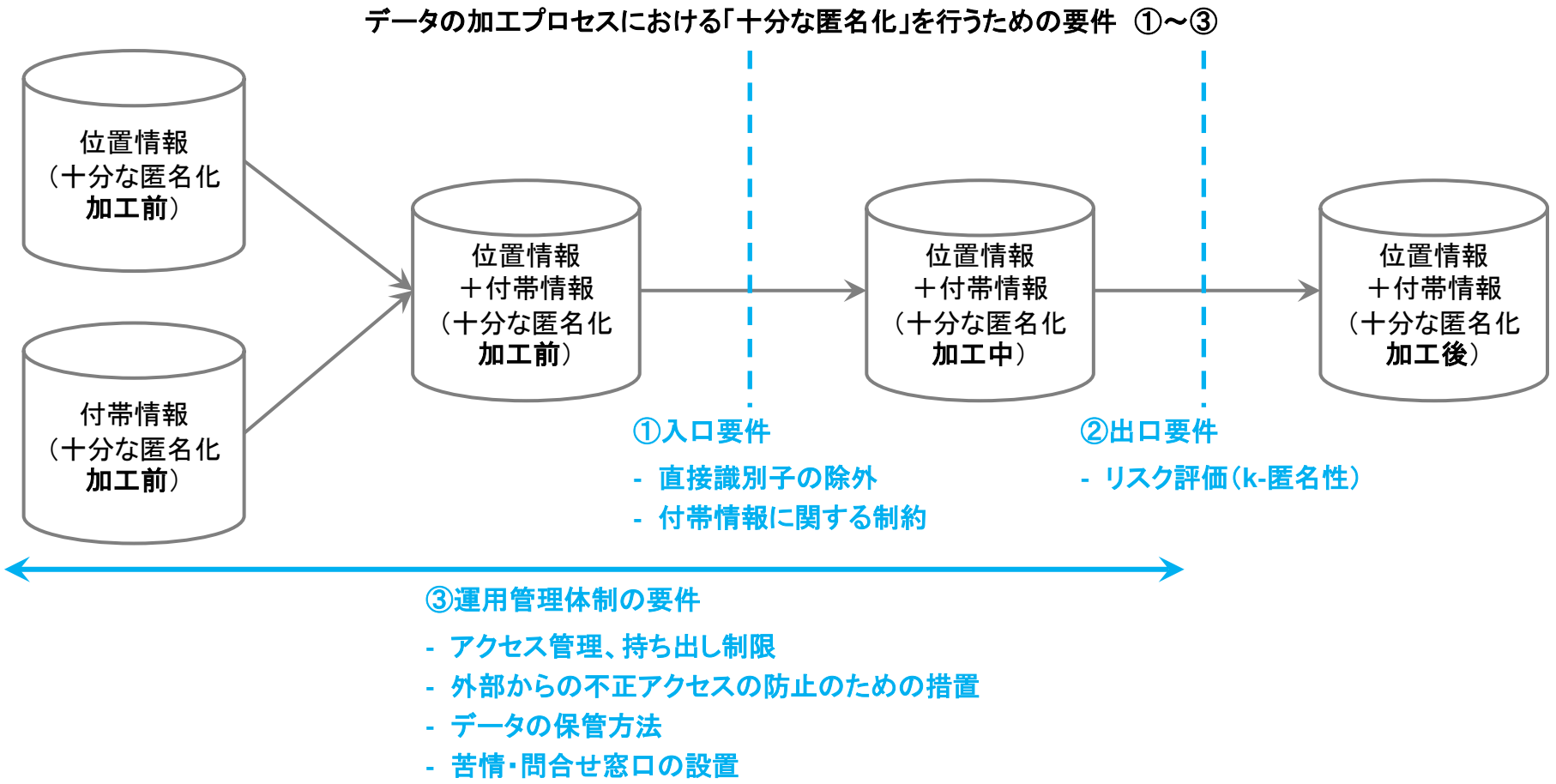
【多様なプレイヤーによる位置情報の活用の促進】

- 電気通信事業者が保有する位置情報については、安全な形で多様なプレイヤーによって利用されていくことが望ましいと考えられるところ、今般のルール整備を踏まえ、そのために必要な更なる方策について、諸外国の動向も踏まえつつ、検討を進めていくべきではないか。

参考①　位置情報の利活用に係る実証　各ユースケースの概要

	名称	概要	担当事業者	利用する位置情報
①	**震災等災害時の避難行動分析（防災）**	GPS測位した位置情報を用いて平常時の「流動人口」の集計を行い、そこから災害が発生した場合の被害を算出した後、内閣府公表の被害想定との比較を行う。	NTTドコモ	GPS位置情報
②	**都市交通整備への活用を想定した空港利用者の動態分析（交通）**	利用者の契約情報及び位置情報を用いて、首都高速中央環状線（大井JCT～初台IC）の開通前後の羽田・成田空港利用者の動態分析を行う。	KDDI	携帯電話基地局位置情報（通信の秘密に該当するものを含む）
③	**スポーツ観戦時におけるユーザの流動性調査（商用）**	九州地区での野球観戦キャンペーンへの応募者から、顧客情報と一定期間における位置情報を取得し、イベント施設周辺エリア及び商業エリア（博多駅等）に滞在した人の①属性、②施設来場頻度・滞在時間、③施設来場前後の立寄り等の分析を行った。	ソフトバンク	Wi-Fi位置情報（通信の秘密に該当するものを含む）
④	**観光客の滞留時間分析、導線分析（観光）**	交通要所及び観光スポットに設置しているWi-Fiエリアを活用して位置情報を取得し、訪日外国人等の各スポットでの接続時間を把握・分析する。	NTTブロードバンドプラットフォーム（NTT-BP）	Wi-Fi位置情報

参考①　データの加工プロセスにおける「十分な匿名化」の要件



参考①　入口要件、出口要件

○入口要件（加工を行う前の要件）

直接識別子の除外	直接識別子は削除する。なお、仮IDの生成に当たっては、可能な限り短い有効期限を設ける、ハッシュ化等一方向の置き換えを行うといった措置を講じる。
付帯情報	住所（市区町村名まで）、性別、年齢の3つを加えるユースケースを検討した。言語情報の追加については今後の検討課題とする。

○出口要件（加工を行った後の要件）

リスク評価	■加工後のデータでは、原則次の条件を満たす（k匿名性）： （ｉ）同一時刻のすべての間接識別子において非識別かつ （ii）すべての時間を通じた履歴において非識別 ■複数のkについて、特定の個人を識別できてしまうリスクを定性的に評価し、評価の結果十分にリスクが低減されるkの値を決める。なお、その際のkの値については、一定程度大きい値から減じていくものとする。 ■上記のリスク評価を行う際の指標には、下記を含むものとする。 ①データの項目、②場所の特性、③利用者の特性、④取得期間・時期、⑤位置データの精度、 ⑥追跡可能な移動履歴の長さ・仮IDの有効期間、⑦データを取得する際の時間間隔、⑧標本数 ■上記のリスク評価の結果、再特定化・再識別化に関するリスクが十分に低減されていることが判断された場合、k=1が許容される可能性がある。

参考①　本実証で用いたリスク評価指標

(a) 取り扱うデータの内訳に関する指標	
①データの項目	項目数が多いほどリスクが大きい。
②場所の特性	データに紐づく地図上の場所の特徴。機微情報にかかわる場所や詳細な住所等が含まれている場合はリスクが大きい。
③利用者の特性	データが対象にしている利用者の特徴。特定の母集団を対象とする場合はリスクが大きい。
(b) 取得･加工の内容に関する指標	
④取得期間･時期	データを取得した期間や時期。イベントや事件等が特定される場合リスクが大きい。
⑤位置データの精度	データ取得時の位置の精度（携帯電話基地局であれば数十メートル～数百メートル）や加工時のメッシュの間隔等。精度が上がるほどリスクが大きい。
⑥追跡可能な移動履歴の長さ･ 仮IDの有効期間	特定の利用者を追跡できる地図上の軌跡又は時間的長さ。長いほどリスクが大きい。
⑦データを取得する際の時間間隔	データを収集する際の時間的な間隔。間隔が狭いほどリスクが大きい。
⑧標本数	加工の対象となった利用者の数。少ないほどリスクが大きい。

参考①　管理運用体制の要件

〇下記の要件に基づきPIA評価を行うことで、適切な管理運用体制を担保することを想定。

分類	小分類	実施目的	実施内容の例
アクセス管理	ID管理	加工に関与する者を特定すること	• 一意のIDを割り当てる • 一定期間未使用のIDを失効させる　等
	認証管理	特定された者だけが作業できるようにすること	• パスワードの強度確保　等
	アクセス権管理	業務上必要な範囲の作業しかできないようにすること	• アクセス権を職務遂行に必要な最小限に制限する　等
	ログ管理	作業内容を追跡できるようにすること	• 加工前及び加工中データへの全てのアクセスの記録　等
持ち出し制限	—	加工前及び加工中におけるデータの持ち出し（漏洩や不正利用等）を防止すること	• 加工前及び加工中のデータを取り扱うシステム環境からの外部アクセスの禁止 等
外部からの不正アクセス防止のための措置	—	加工を行う環境の外からの、データの破壊・改ざん・漏洩等を防止すること	• 加工を行うシステム環境を他のシステム環境と物理的又は論理的に分離する　等
データの保管方法	—	加工前及び加工中のデータについて、権限が付与された者にアクセスを限定し、容易に個人を再識別できないように保存すること	• 加工前及び加工中のデータが格納されているDBやファイルを保存時に暗号化する等
苦情・問合せ窓口の設置	—	加工に関する苦情や問合せに適切に対応すること	• オプトアウトに対応する体制・手順・システム等の整備　等

参考①　本実証で検討された包括同意約款（案）

包括同意約款モデル（案）

※実際に運用する際には必要に応じてカスタマイズする。

【利用する情報】

当社は、通信の秘密に該当する位置情報（通信の場所、日時、端末識別符号に限ります。）を、電気通信役務の提供を目的に取得・利用するほか、お客様に関する契約者情報（市区町村名までの住所情報※1、年齢、性別に限ります※2）とともに、次の利用目的のために、十分な匿名化を行ったうえで利用します。（以下、匿名化利用）

匿名化利用の内容は、以下のとおりです。なお、詳細については、「Web等での説明事項案」をご参照ください。

【匿名化手法】

個人の再特定化・再識別化が極めて困難といえる程度に加工します。

具体的な匿名化手法は「Web等での説明事項案」に記載します。

【利用目的】

(1) 当社サービスの表示・配信

(2) 当社による〇〇サービスに関するマーケティング調査および分析

(3) 当社〇〇サービスの品質向上や、新商品・新サービスの企画・開発・提供

(4) 当社〇〇サービスについての当社によるご利用状況分析

(5) 官公庁、公共団体、一般企業等への人口動態分析、マーケティング分析等の各種分析結果の提供

《上記(1)～(5)は例示であり、特に各社にて状況に応じ変更する箇所になります。別途「プライバシーポリシー」等で記載されたものを参照することも可としますが、その場合、「プライバシーポリシー」において、本包括同意約款に基づいて通信の秘密に該当する位置情報を利用する場合の利用目的の項目が存在し、かつ利用者に分かりやすい場所に明記されている必要があります。》

【第三者提供】

上記位置情報およびお客様に関する契約者情報、端末識別符号は、特定の個人を容易に識別できないよう十分な匿名化を行ったうえで、上記利用目的の範囲内で官公庁、公共団体、一般企業等の第三者に提供することがあります。

【情報の利用・第三者提供の停止】

お客様は、当社が取得した位置情報、契約者情報、その他端末識別符号の当社における匿名化利用（加工後の情報の第三者提供を含みます。）について、別途定める方法により停止を申出ることができます。

【個人情報保護方針】

当社の個人情報保護方針は、別途当社の「プライバシーポリシー」に記載いたします。

【約款の変更】

利用目的の変更や取得するデータ項目の変更に伴い、本約款を変更する場合があります。

※1　対象範囲については、今後、利用するユースケースに応じて各社で検討することとする。

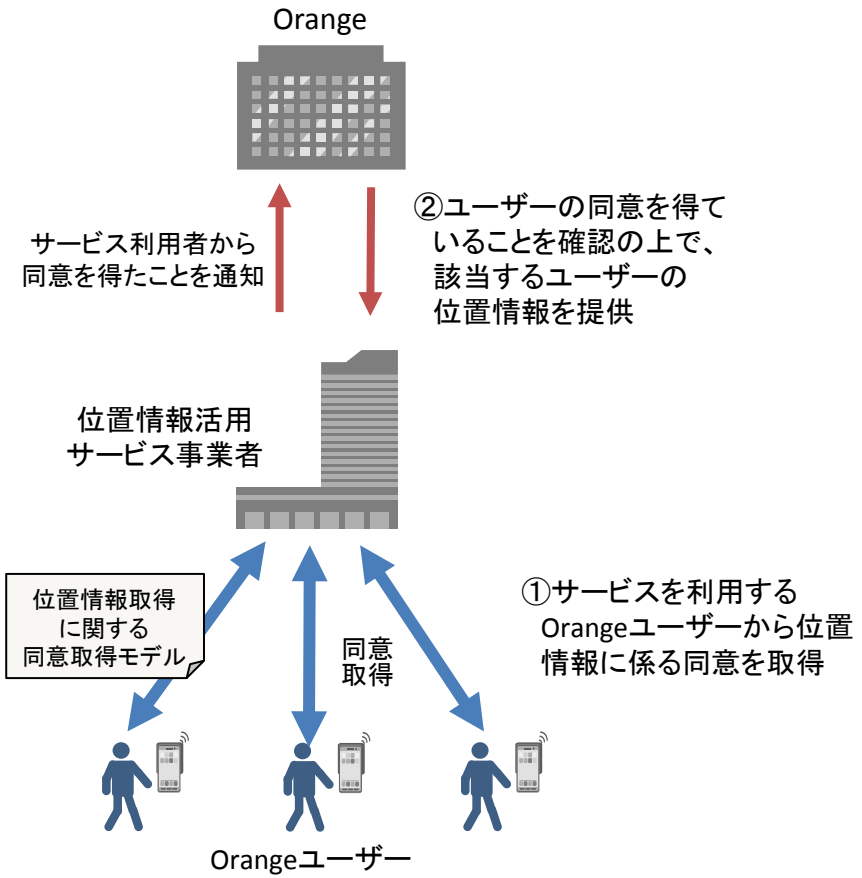
※2　利用言語情報は今後の継続検討課題。

参考②　諸外国の動向　-フランス-

位置情報の活用状況等

- EUデータ保護指令を受けた「情報処理と自由に関する法」により、個人データ（位置情報を含み得る）の取得に当たっては、基本的にユーザーからの同意が必要となる。匿名化した場合には、ユーザーから特に同意を得る必要はない。
- ユーザーからの同意を、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。

同意取得や位置情報の提供のイメージ（Orange社の例）



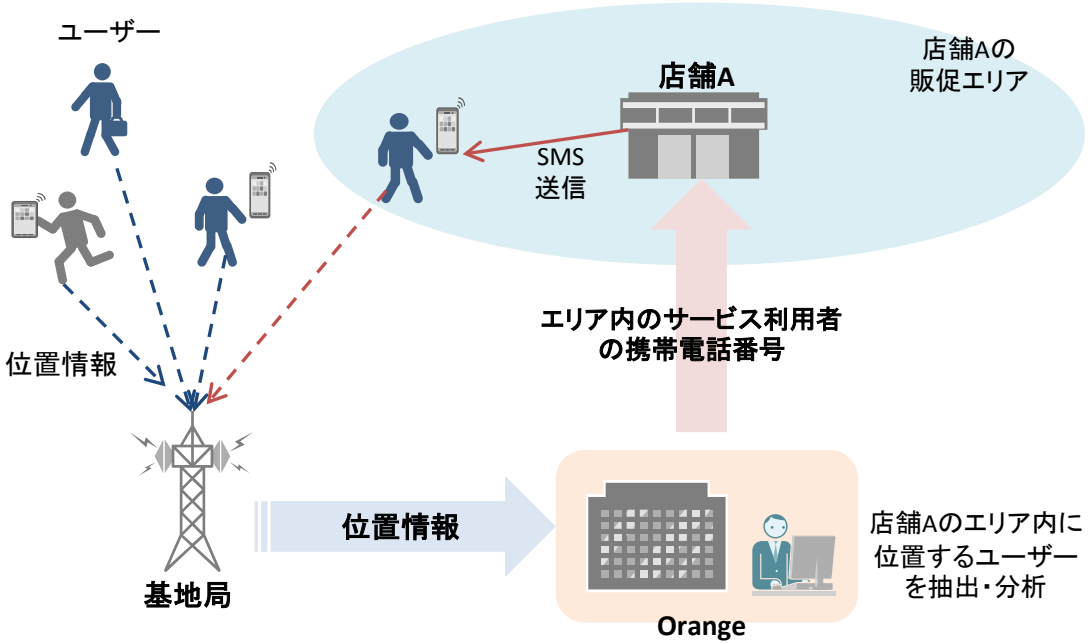
・Orange社の持つ位置情報を活用してサービスを提供しようとする事業者は、サービス利用者から位置情報取得に係る同意を取得することで、Orange社から当該個人の位置情報データを取得することができる。

・Orange社は、サービスを提供しようとする事業者に対し、個人データ取得に係る同意取得のひな形として、
①個人データの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種類を提示している。

サービス事例：Géo Présence （Orange社）

- 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。
- Orange社は、マーケティング事業者から予め伝えられた携帯電話番号のユーザーが、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。
- マーケティング事業者は、その情報を受けて当該ユーザーにSMSを送信。

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
- その際、サービス提供のために、Orangeから位置情報及び電話番号を取得することを明示

参考②　諸外国の動向　－韓国－

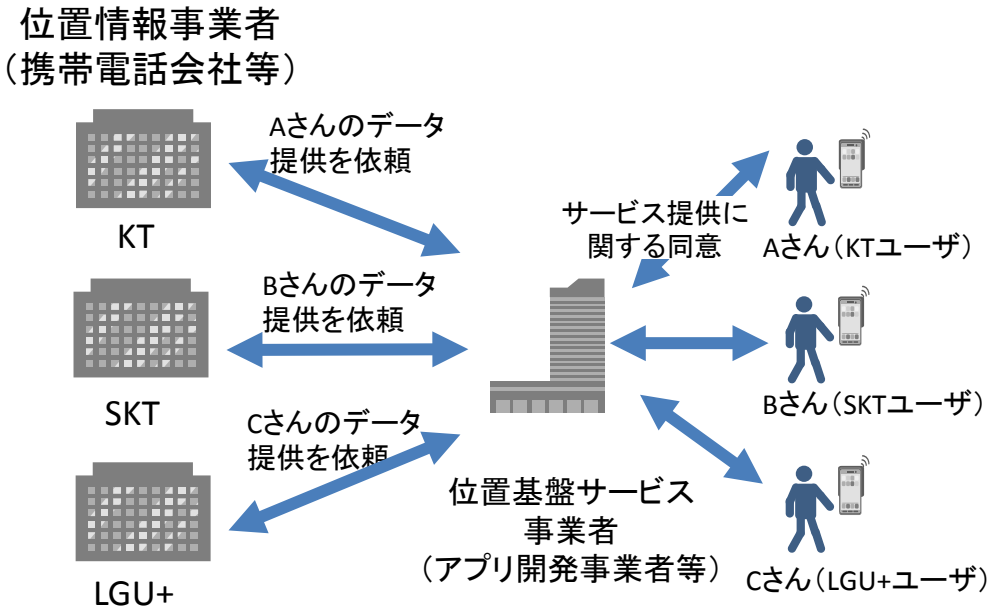
位置情報の活用状況等

- 位置情報の活用に関して「位置情報の保護及び利用等に関する法律」を2005年に制定。ビッグデータの処理・活用に係る個人情報保護等に関しては政府が別途ガイドラインを発行。
- 同法制定後、2010年に位置情報産業の活性化のため、「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」が策定され、2016年に改定が行われた。同計画では、①LBS(※)産業の育成、②社会安全網の高度化、③プライバシー保護という3つの推進目標が掲げられている。　※LBS：Location Based Service（位置基盤サービス）

「位置情報の保護及び利用等に関する法律」の概要・活用のイメージ

- 位置情報事業者：利用者の位置情報を直接収集する事業者
  位置基盤サービス事業者：位置情報を位置情報事業者から提供してもらいサービスを提供する事業者

  ※「位置情報事業者」については許可制、「位置基盤サービス事業者」については届出制。
- 位置基盤サービス事業者は、利用者から、位置情報を利用するサービスの提供に係る同意を得れば、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できない。



Ⅰ　位置情報の取扱いについて

Ⅱ　スマートフォンの利用者情報の取扱いについて

Ⅲ　電気通信事業分野ガイドラインのその他の改正事項について

Ⅳ　IoTとプライバシーについて

1　これまでの取組みについて

○　スマートフォンの普及に伴い、そのアプリケーション（以下「アプリ」という。）を利用したサービスが、情報通信分野における情報のやりとりにおいて大きな位置を占めてきているところ、アプリ等により取得・蓄積された利用者情報（アドレス帳、位置情報等）が、本人の意図しないかたちで外部送信されている事案が発覚し、社会問題化した。

○　総務省においては、平成24年8月に、「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」の議論を踏まえ、アプリごとのプライバシーポリシーの作成・掲載等を提言内容とする「スマートフォン プライバシー イニシアティブ（SPI）」を取りまとめて公表。

○　平成24年10月、民間主導でスマートフォンのプライバシーに関する業界ガイドラインの策定を促進し、利用者情報等の適正な取扱いを通じて安心安全なスマートフォンの利用環境を整備することを目的として、スマートフォンの利用者情報等に関する連絡協議会（SPSC）が発足。関係の業界団体、機関、学識経験者を構成員とし、また、関係の事業者、団体、省庁をオブザーバーとして、約40のステークホルダーが一堂に会した情報共有を定期的に実施。

○　平成25年9月、個々のアプリケーションにおける利用者情報の適正な取扱いを確保するために、運用面・技術面から第三者がアプリを検証する仕組みを民間主導で推進することを提言した「スマートフォン プライバシー イニシアティブⅡ」を公表。

○　平成25年度以降、SPIおよびSPIⅡの指針を受け、調査研究を継続的に実施し、その結果をスマートフォン　プライバシー　アウトルック（SPO）として取りまとめ、公表。調査研究の主な内容は、①アプリケーションの利用者情報の取扱いに関する実態調査、②民間、諸外国の取組状況に関する調査、③第三者検証システムに係る実証、④普及啓発方法等の検討である。

スマートフォン プライバシー イニシアティブ（SPI）の概要

○　SPIにおいては、利用者情報を取得する者（アプリ提供者等）に対して、次の取組を求めている。

基本原則

① 透明性の確保

関係事業者等は、対象情報の取得・保存・利活用及び利用者関与の手段の詳細について、利用者に通知し、又は容易に知りうる状態に置く。利用者に通知又は公表あるいは利用者の同意を取得する場合、その方法は利用者が容易に認識かつ理解できるものとする。

② 利用者関与の機会の確保

関係事業者等は、その事業の特性に応じ、その取得する情報や利用目的、第三者提供の範囲等必要な事項につき、利用者に対し通知又は公表あるいは同意取得を行う。また、対象情報の取得停止や利用停止等の利用者関与の手段を提供するものとする。

③ 適正な手段による取得の確保

関係事業者等は、対象情報を適正な手段により取得するものとする。

④ 適切な安全管理の確保

関係事業者等は、取り扱う対象情報の漏えい、滅失又はき損の防止その他の対象情報の安全管理のために必要・適切な措置を講じるものとする。

⑤ 苦情・相談への対応体制の確保

関係事業者等は、対象情報の取扱いに関する苦情・相談に対し適切かつ迅速に対応するものとする。

⑥ プライバシー・バイ・デザイン

関係事業者等は、新たなアプリケーションやサービスの開発時、あるいはアプリケーション提供サイト等やソフトウェア、端末の開発時から、利用者の個人情報やプライバシーが尊重され保護されるようにあらかじめ設計するものとする。

利用者の個人情報やプライバシーに関する権利や期待を十分認識し、利用者の視点から、利用者が理解しやすいアプリケーションやサービス等の設計・開発を行うものとする。

（１）プライバシーポリシーの作成・掲載

① 情報を取得するアプリケーション提供者等の氏名又は名称
- アプリケーション提供者等の名称、連絡先等を記載する。

② 取得される情報の項目
- 取得される利用者情報の項目・内容を列挙する。

③ 取得方法
- 利用者の入力によるものか、アプリケーションがスマートフォン内部の情報を自動取得するものなのか等を示す。

④ 利用目的の特定・明示
- 利用者情報を、アプリケーション自体の利用者に対するサービス提供のために用いるのか、それ以外の目的のために用いるのか記載する。
- 広告配信・表示やマーケティング目的のために取得する場合には、その旨明示する。

⑤ 通知・公表又は同意取得の方法、利用者関与の方法
- 通知・公表の方法、同意取得の方法：プライバシーポリシー等の掲示場所や掲示方法、同意取得の対象、タイミング等について記載する。
- 利用者関与の方法：利用者情報の利用を中止する方法等を記載する。

⑥ 外部送信・第三者提供・情報収集モジュールの有無
- 外部送信・第三者提供・情報収集モジュールの組込みの有無を記載する。

⑦ 問合せ窓口
- 問合せ窓口の連絡先等（電話番号、メールアドレス等）を記載する。

⑧ プライバシーポリシーの変更を行う場合の手続
- プライバシーポリシーの変更を行った場合の通知方法等を記載する。

（当初取得した同意の範囲が変更される場合、改めて同意取得を行う。）

（２）適切な安全管理措置

（３）その他（情報収集モジュール提供者、広告事業者に対する特記事項等）

また、アプリ提供サイト運営事業者（移動通信事業者が当該サイトを運営する場合を含む）及びOS提供事業者に対し、アプリ提供者等に対して適切なプライバシーポリシーの作成・公表の対応を促すこと等を求めている。

2　SPIの実効性確保に向けて検討すべき事項（案）

- アプリのプライバシーポリシーの掲載について、重要性が認識されてきてはいるものの、法的な義務としては定められておらず、掲載や内容の適切さなど実効性あるプライバシーポリシーの掲載率は低い。
- 諸外国の例をみると、米国では、個人情報の取扱いに関して表明したプライバシーポリシーと、実際の情報の取扱いが異なる場合には、不公正又は欺瞞的取引について規律するFTC法5条に基づく処分の対象になるなど、強制力を持って実効性を担保する取り組みがなされている。
  また、米国商務省・電気通信情報局（NTIA）が主導し、FTCもオブザーバとして参加するマルチステークホルダープロセスで、自主規制ルールとして、モバイルアプリの通知に関する行動規範が制定されている。
- 我が国においては、景品表示法をはじめとして個別の法令において表示義務を課している場合があるが、アプリのプライバシーポリシーの掲載について同等の強制力を持たせることは、社会的に理解が得られる状況に至っているとは考えられない。
- このような状況に鑑みると、電気通信事業分野ガイドライン第14条に、電気通信事業者が自ら提供するアプリのプライバシーポリシーの作成・掲載をすることを明記し、掲載の実効性を高めることが有効ではないか。
  また、電気通信事業者がアプリ提供サイトを運営する場合も増えてきているところ、同サイト運営事業者から、アプリ提供者等に対して、適切なプライバシーポリシーの作成・公表の対応を促すことが有効ではないか。
- さらに、マルチステークホルダープロセスを活用して、民間主導で自主規制ルールを策定し、認定個人情報保護団体の個人情報保護指針や、業界団体の自主ガイドラインに反映することも検討できるのではないか。
- 電気通信事業者以外にも、自主規制ルールを及ぼすことが有効ではないか。

3　本タスクフォースでの主な意見

- プライバシーポリシーの掲載などについては、現行の個人情報保護法、改正個人情報保護法においても、法的な義務としては定められておらず、あくまでも基本方針で定められているに過ぎない。一方、諸外国の例を見ると、米国ではFTC第5条に基づく処分の対象とするなど、ある程度強制力を持って実効性を担保する取組も行われている。
- プライバシーポリシー掲載の実効性を高めるため、今後も自主的な取組を進めることが必要となるが、そのような自主的な取組の礎とするため、例えば電気通信事業分野ガイドラインにポリシー掲載について明記をするといったようなことも含めて、いかにポリシーの掲載に実効性を持たせるかを検討すべき段階にきている。
- プライバシーポリシーの掲載事態は法的義務ではないが、それとは別に、一定の情報を取得するとプライバシー侵害になるという問題も防ぐという目的もあってSPIを策定した。したがって、実効性が確保されないと事業者の方も大変混乱することになるので、SPIを電気通信事業分野ガイドラインに位置付けて、実効的な方法を検討すべき。
- NTIAにおいても透明性に係る行動規範が策定されているが、今後は、通知した後に同意をどのように取得し、利用者にどのような選択期間を与えるのか、そのタイミングはどうあるべきかといった点が議論になると考えられる。
- 現在、ビジネスの世界ではプラットフォーマーを志向する傾向が強く、その傾向の下では個別のアプリに対するプライバシーポリシーを書き分けるのが困難であるということが、大手の事業者からよく聞かれる話であり、今後、グローバルなトレンドの中では調整が必要になってくるのではないか。
- ソフトウエア産業を育成する観点から言うと、海外のプライバシーポリシーについて、国で調査をするなり、動向を調べることも重要。また、SPIの提言時に比べ、個人情報保護法の改正がなされるなど、日本の個人情報保護に係る状況が変わってきていることを踏まえて、新たな調査なり、方針を出していけば良いのではないか。

4　取りまとめの方向性（案）

【電気通信事業分野ガイドラインへの反映】

- スマートフォンの利用者情報の取扱いにおける透明性確保において重要な役割を担うアプリのプライバシーポリシー掲載の実効性を高め、また、自主的な取り組みによる対応を推進するため、電気通信事業者がアプリを提供する場合には、当該アプリの情報取得等について明確かつ適切に記載したプライバシーポリシーを作成・掲載することをガイドラインに記載すべきではないか。
- 電気通信事業者がアプリ提供サイトを運営する場合も増えてきているところ、掲載の実効性を高めるため、かかる場合には、電気通信事業者はアプリ提供者に対して、明確かつ適切なプライバシーポリシー作成・公表の対応を促すことが有益である旨をガイドラインに記載すべきではないか。

【民間ガイドラインの策定】

- ガイドライン及びその解説で、アプリのプライバシーポリシーに関するユーザーインターフェースのデザイン・仕様など、運用の詳細まで定めることは困難である。したがって、運用の詳細については、SPI等を参考にしつつ、マルチステークホルダープロセスを利用して、民間ガイドラインを作成する方向で検討すべきではないか。具体的には、スマートフォンの利用者情報等に関する連絡協議会（SPSC）等の場で、ガイドライン及びその解説について、具体的な運用を検討することが考えられるのではないか。

【利用者に対する情報提供・周知啓発について】

- マルチステークホルダープロセスを利用し、関係の行政機関、認定個人情報保護団体、業界団体、消費者団体等が連携し、利用者への情報提供・周知啓発方法を検討することが望ましいのではないか。

【電気通信事業者以外への対応について】

- 電気通信事業者以外にもアプリ提供事業者など多様な関係者が存在するため、マルチステークホルダープロセスを利用して自主ガイドラインを作成するなど、電気通信事業者以外にも効力を持たせる方向で、上記の関係者等が連携して取り組むことが望ましいのではないか。

現行ガイドラインにおけるプライバシーポリシーに関する規定

●電気通信事業分野ガイドライン

（プライバシーポリシー）

第14条　電気通信事業者は、プライバシーポリシー（当該電気通信事業者が個人情報保護を推進する上での考え方や方針をいう。）を公表し、これを遵守するものとする。

（解説）

(1) 本条は、電気通信事業者の個人情報保護についての社会の信頼を確保するため、電気通信事業者は自らの個人情報保護を推進する上での考え方や方針についての宣言をプライバシーポリシーとして公表し、これを遵守するものとすることを規定したものである。

(2) プライバシーポリシーは、それぞれの電気通信事業者が、分かりやすい表現で記載すべきものであるが、プライバシーポリシーに記載すべき事項としては、次のようなものが考えられる。

① 個人情報保護法及び通信の秘密に係る電気通信事業法の規定その他の関係法令の遵守

② 本ガイドラインの遵守

③ 第16条第1項各号に定める公表すべき事項

（ⅰ）電気通信事業者の名称

（ⅱ）個人情報の利用目的

（ⅲ）利用目的の通知又は開示若しくは訂正等の本人からの求めに応じる手続

（ⅳ）苦情の申出先

（ⅴ）認定個人情報保護団体の名称及び苦情の解決の申出先

④ 第11条の安全管理措置に関する方針

⑤ 利用者の権利利益の保護に関する事項

（ⅰ）保有個人情報について本人から求めがあった場合には、ダイレクト・メールの発送停止など、自主的に利用停止等に応じること

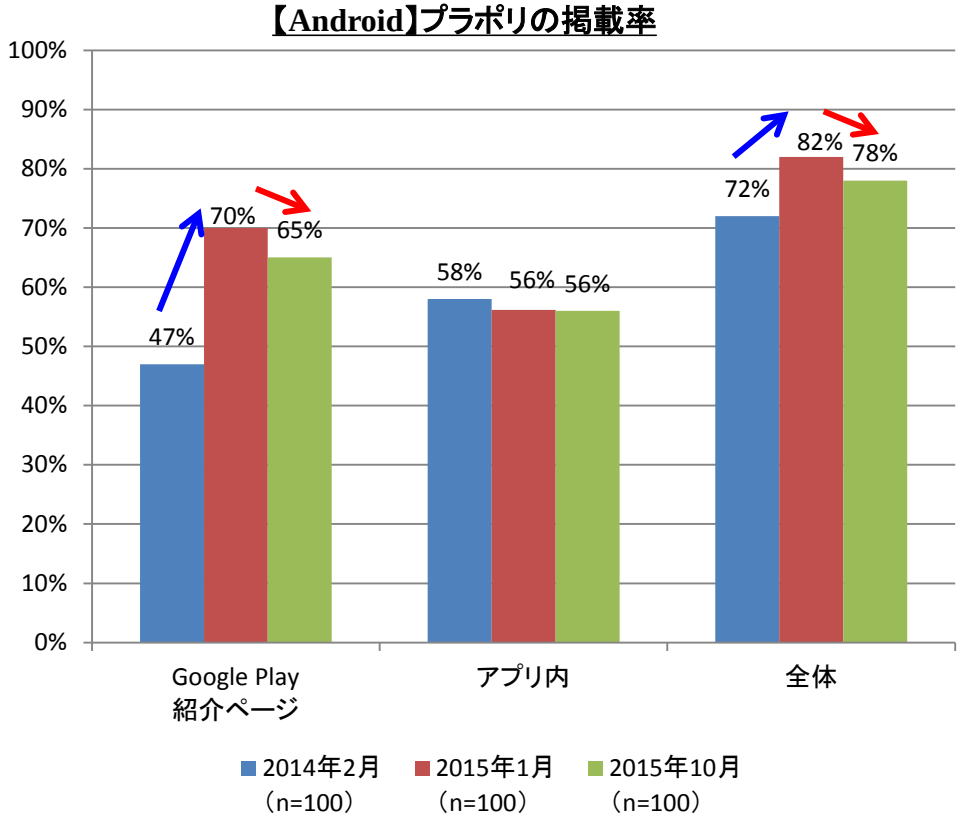
（ⅱ）委託の有無、委託する事務の内容を明らかにする等、委託処理の透明化を進めること

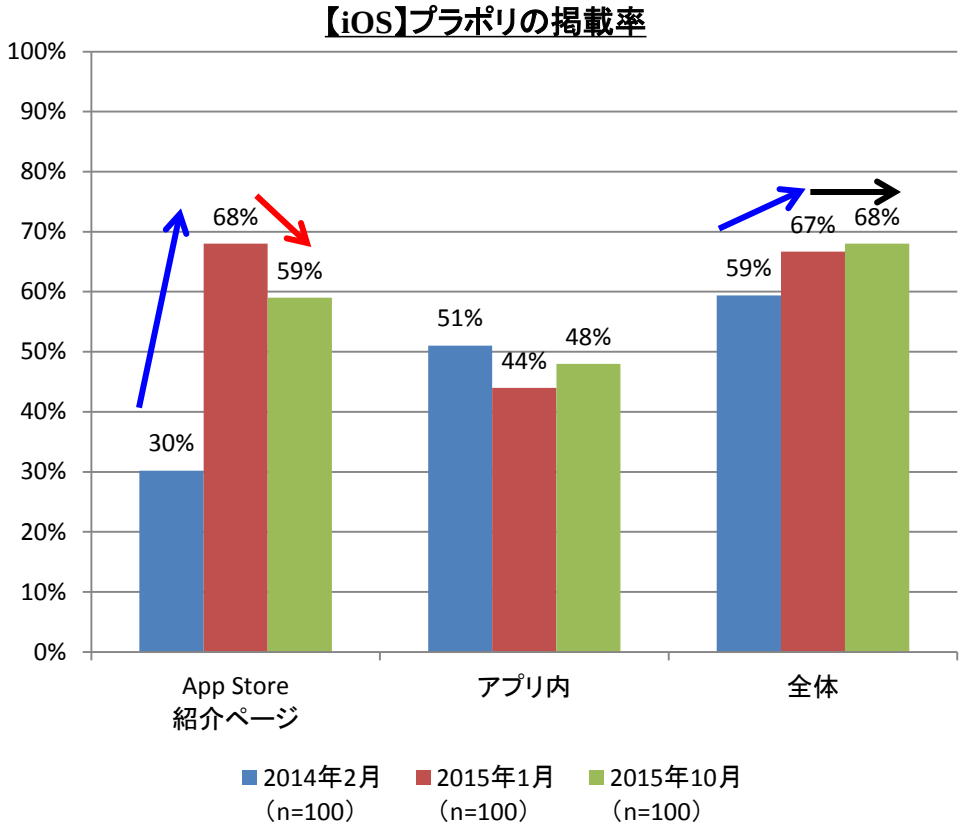
（ⅲ）電気通信事業者がその事業内容を勘案して利用者の種類ごとに利用目的を限定して示したり、電気通信事業者が本人の選択による利用目的の限定に自主的に取り組むなど、本人にとって利用目的がより明確になるようにすること

（ⅳ）個人情報の取得元又はその取得方法（取得源の種類等）を、可能な限り具体的に明記すること

（参考1）アプリプラポリ調査結果① 人気アプリ：作成・掲載状況の経年比較

全体においてAndroid、iOSともに2014年2月から2015年1月にかけてプラポリの掲載率は伸びたものの、2015年1月から2015年10月にかけては横ばい・微減で推移している。





※掲載率：以下の「A」から「F」までのうち、「F」判定以外であれば、「プラポリ有り」と判断。
（「個々のアプリに関するプラポリが作成されていること」、「SPI8項目が適切に記載されていること」を示すものではない）
A：個々のスマホアプリ専用のプラポリが用意されている。B：サービス全体のプラポリがあり、その中に個々のスマホアプリに関する記述がある。
C：サービス全体のプラポリがあり、その中に個々のスマホアプリに関する記述がない。D：一般的なWebサイトのプラポリがあるだけ。
E：会社としての抽象的なポリシー（個人情報保護方針）があるだけ。F：プラポリが記載されていない。
※紹介ページの掲載率：「紹介ページのリンク」か「紹介文内での記載」のどちらかで「F」以外の判定となったアプリの割合。
※アプリ内の掲載率：「初回起動時」、もしくは、「アプリ内のメニューやヘルプ等」のどちらかが「F」以外の判定となったアプリの割合。
※全体の掲載率：「紹介ページ」、もしくは、「アプリ内」のどちらかが「F」以外の判定となったアプリの割合。

アプリプラポリ調査結果②　人気アプリ・新着アプリ：SPI8項目の比較

- AndroidではSPI8項目の中で特に重要性が高い4項目のうち、②において、人気アプリと新着アプリの記載率の差は10%以上であった。
- iOSでは特に重要性が高い4項目のうち、②、④及び⑥において、人気アプリと新着アプリの記載率の差は10%以上であった。

SPI8項目の記載率※

番号	項目		Android		iOS	
			人気アプリ（n=78）	新着アプリ（n=32）	人気アプリ（n=68）	新着アプリ（n=13）
①	情報を取得するアプリケーション提供者等の氏名または住所		98.7%	93.8%	98.5%	100.0%
②	取得される情報の項目		70.5%	56.3%	58.8%	46.2%
③	取得方法		35.9%	25.0%	26.5%	23.1%
④	利用目的の特定・明示		80.8%	75.0%	79.4%	53.8%
⑤	通知・公表又は同意取得の方法	送信停止の手順の記載状況	26.9%	21.9%	22.1%	23.1%
		利用者情報の削除の記載状況	38.5%	37.5%	44.1%	46.2%
⑥	外部送信・第三者提供の有無	利用者情報の第三者への送信の有無の記載状況	79.5%	71.9%	85.3%	38.5%
		利用者情報の送信先の記載状況	38.5%	28.1%	22.1%	7.7%
		情報収取モジュールに関する記載状況	12.8%	12.5%	14.7%	0.0%
⑦	問合せ窓口		65.4%	59.4%	61.8%	76.9%
⑧	プライバシーポリシーの変更を行う場合の手続き		69.2%	43.8%	57.4%	53.8%

SPI8項目において、特に重要性が高いと考えられる項目

特に重要性が高い項目の中で、人気アプリと新着アプリの記載率の差が10%以上ある項目

※プラポリが存在していたアプリ数を母数として割合を算出。

アプリプラポリ調査結果③　全アプリに関する総括

- プラポリの記載状況について4点の基準を定め、それぞれの基準を満たすアプリの比率を記載した。
- 「基準①プラポリの掲載」、「基準②重要4項目の記載」の基準を満たしている人気アプリの割合は新着アプリや20カテゴリのアプリよりも高くなっている。
- 「基準③全8項目の記載」、「基準④概要版の掲載」については、全ての調査対象で基準を満たしている割合が10%以下。

		基準① プライバシーポリシーが作成・掲載されている（プラポリの掲載）	基準② SPI8項目の内、重要度の高い4項目を記載している（重要4項目の記載） 「①提供者名」、「②取得される情報」、「④利用目的」、「⑥外部送信・第三者提供、情報収集モジュール」	基準③ SPI8項目の全項目について記載している（全8項目の記載） 基準②に加えて、「③取得方法」、「⑤利用者関与」、「⑦問合せ窓口」、「⑧変更の手続き」を記載	基準④ 基準③に加えて、概要版のプライバシーポリシーを作成・掲載している※（概要版の掲載）
Android	人気	78%	51%	10%	1%
	新着	64%	26%	10%	0%
	20カ	63%	33%	10%	1%
iOS	人気	68%	32%	9%	2%
	新着	46%	10%	4%	0%

10%以下

※「20カ」:「20カテゴリ」の略。

※概要版が存在するアプリプラポリの中には基準③も満たしていないアプリも存在するため、基準④は概要版の掲載率と一致しない。

（参考2）モバイルアプリの通知に関する米国の取組み①

米国商務省・電気通信情報局（NTIA）によるマルチステークホルダープロセス（MSP）

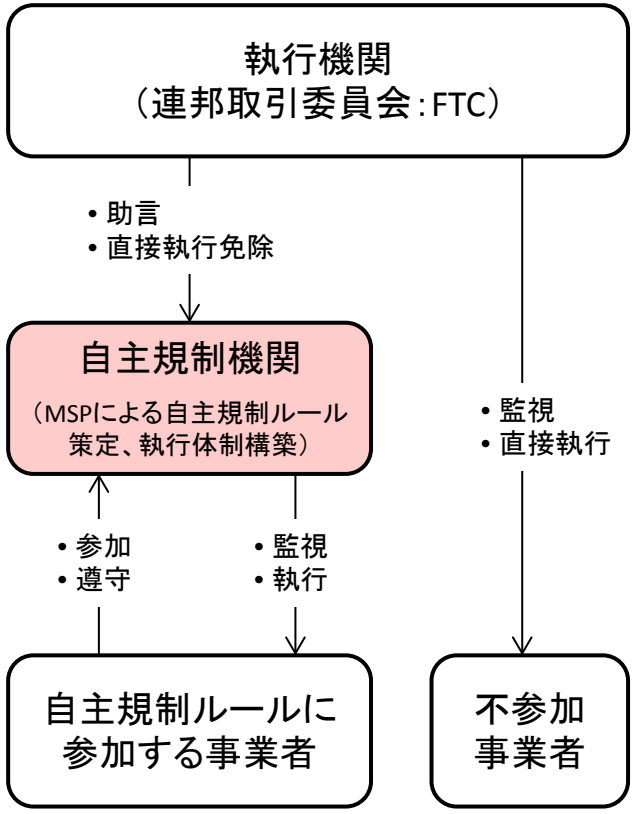
- 自主規制の構造的な問題
  - 団体に参加する事業者の都合のいいようにルールが作られる。
  - 執行体制に独立性が欠けて、エンフォースメントが機能しづらい。
  - 不参加企業が出る（正直者が損をする）。

- NTIA・MSPは、自主規制の問題を解消するため、ホワイトハウスの指示を受けて取り組まれた。
  - 多様なステークホルダーの意見を調整。
  - 執行機関が、MSPに参加して意見や助言をする。
  - ルールへの参加事業者は、直接執行を免除される。

  ※最終的に、FTCは直接執行免除を約束せず。

  ＜事例＞
  - モバイルアプリの通知に関する行動規範
  - 顔認証技術に関する行動規範
  - セキュリティ脆弱性の開示に関する行動規範

NTIA・MSPによる自主規制スキーム（目標像）



（第6回会合　小林構成員提出資料）

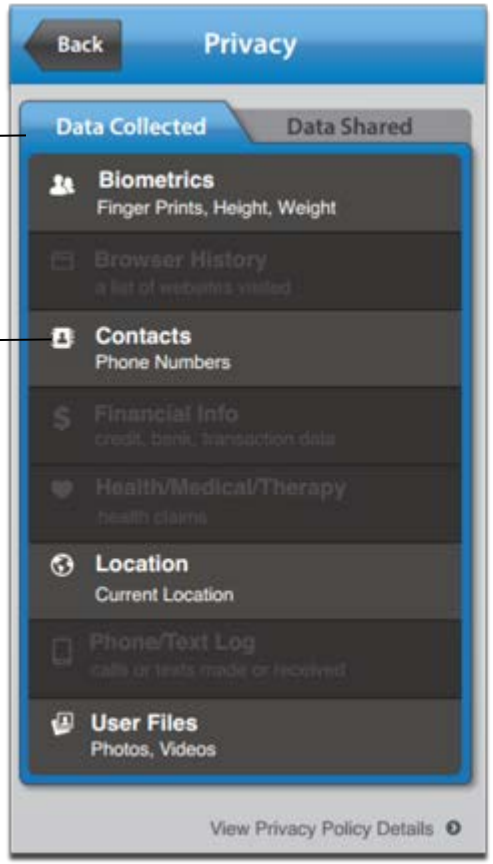
モバイルアプリの通知に関する米国の取組み②

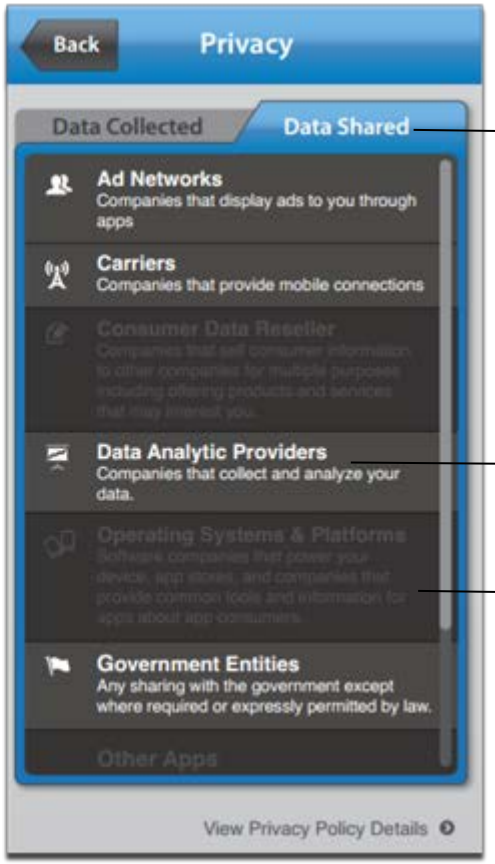
MSP終了後に作成されたモバイルアプリの通知画面のインターフェースデザイン

モバイルアプリの通知画面のデザイン

取得するデータ項目を表示

データ項目をアイコンで表示





データを共有する外部事業者カテゴリを表示

共有する事業者をハイライト表示

共有しない場合はグレイアウトして表示

出所）NTIAウェブサイトの情報をもとに作成

（第6回会合　小林構成員提出資料）

（参考3）スマートフォンの利用者情報等に関する連絡協議会（SPSC）

- 平成24年8月に、SPIが公表後、速やかに同年10月、民間主導で、「スマートフォン市場において様々なビジネスが連携し様々な業界団体が関係している環境を考慮し、緊密な情報交換及び相互の知見を結集してスマートフォンのプライバシーに関する業界ガイドラインの策定を促進し、利用者情報等の適正な取扱いを通じて安心安全なスマートフォンの利用環境を整備する」ことを目的としてSPSCを組成。
- 「スマートフォンのプライバシーに関する業界ガイドラインの検討・策定を進める意向がある業界団体、スマートフォンの利用者情報の取扱いに関係する業界団体及び関係機関」、学識経験者を構成員として、関係事業者・団体・省庁を含めたオブザーバー、計約40団体で、等のスマートフォンに係るステークホルダーが一堂に会した情報共有を定期的に実施している。

議長
新保 史生 慶應義塾大学総合政策学部　教授
副議長
森 亮二 弁護士法人英知法律事務所　弁護士

構成員
一般社団法人 IPTVフォーラム
安心ネットづくり促進協議会
一般社団法人 インターネット広告推進協議会
一般社団法人 コンピュータソフトウエア協会
独立行政法人 産業技術総合研究所
一般社団法人 JPCERTコーディネーションセンター
一般社団法人 情報サービス産業協会
独立行政法人 情報通信研究機構
一般社団法人 情報通信ネットワーク産業協会
独立行政法人 情報処理推進機構
セキュリティ対策推進協議会
一般社団法人 ソーシャルゲーム協会
一般社団法人 テレコムサービス協会
一般社団法人 電気通信事業者協会
日本Androidの会
一般社団法人 日本インターネットプロバイダー協会
一般社団法人 日本オンラインゲーム協会
一般社団法人 日本ケーブルテレビ連盟
一般社団法人 日本広告業協会
一般財団法人 日本情報経済社会推進協会
一般社団法人 日本スマートフォンセキュリティ協会
一般社団法人 日本ソフトウエア産業協会
一般財団法人 日本データ通信協会
一般社団法人モバイルコンテンツ審査・運用監視機構
一般社団法人モバイル・コンテンツフォーラム
モバイルコンピューティング推進コンソーシアム

事務局
一般社団法人日本スマートフォンセキュリティ協会(JSSEC)
一般社団法人モバイル・コンテンツ・フォーラム(MCF)
社団法人電気通信事業者協会(TCA)

オブザーバー
アンドロイダー株式会社
株式会社NTTドコモ
KDDI株式会社
情報セキュリティ格付け制度研究会
ソフトバンクモバイル株式会社
株式会社電通
株式会社日本総合研究所
株式会社博報堂
BSA | ザ・ソフトウェア・アライアンス

オブザーバー（関係省庁）
総務省、経済産業省、消費者庁

Ⅰ　位置情報の取扱いについて

Ⅱ　スマートフォンの利用者情報の取扱いについて

Ⅲ　電気通信事業分野ガイドラインのその他の改正事項について

Ⅳ　IoTとプライバシーについて

1　電気通信事業分野ガイドラインに関する検討の視点

○　電気通信事業分野ガイドラインは、個人情報保護法に基づく規定のほか、「通信の秘密」に係る電気通信事業法第４条その他の関連規定に基づく規定から構成。

○　改正個人情報保護法の施行に向け、電気通信事業分野ガイドラインについて、主に以下の観点から検討を行う必要がある。

（１）　個人情報保護法関連の事項

①　改正法成立に伴い、電気通信事業分野ガイドラインの既存規定との関係の整理、規定の見直し

【主な検討事項】

- 本ガイドラインの適用対象（個人情報、個人データ、保有個人データの区別等）
  －安全管理措置（第１１条等）、第三者提供の制限（第１５条）、個人情報の開示及び訂正等（第１７条）　等
- 要配慮個人情報の取扱い（第４条）
- 小規模取扱事業者の取扱い（第２条）　等

②　改正法の成立に伴い、電気通信事業分野ガイドラインに新たに反映させるべき事項の整理

【主な検討事項】 匿名加工情報、トレーサビリティの確保　等

※　上記①及び②の具体的な検討については、今後、個人情報保護委員会が定める改正法の政令、規則、ガイドラインを踏まえて検討を行う必要がある。このため、①については現時点ではあくまで検討の方向性を示すにとどめるとともに、②については委員会が定める関係規定が明らかになった段階で改めて検討を行うこととする。

（２）　上記（１）以外の事項

電気通信事業に係る最近の動向を踏まえて、電気通信事業分野ガイドラインに反映させるべき事項の整理

【主な検討事項】

- 「電気通信サービス」の範囲（第２条）
- 位置情報の取扱い（既述）
- スマートフォンのアプリケーションの取扱い（既述）　等

主な意見

- 個人情報保護法は全事業分野を規律する最低限のルールを定めたもの。これに対して、電気通信事業分野について独自のガイドラインが規定されてきた趣旨は、電気通信事業における通信の秘密、あるいは、差別的取扱いの禁止などを確保するという観点から、様々なある種の上乗せ的な規律が置かれてきたものと認識。
  そうだとすれば、今般の個人情報保護法の改正によって、全体的に保護のレベルが上がる部分や逆に利活用が広がる部分があるが、それらの規定との関係で、電気通信事業分野の個人情報保護ガイドラインにおいて、なお事業法的規律の観点から見て維持すべき部分があるのか、あるいは、他の事業者と連携していくという観点から見て改正法に合わせた方がよいのか、その基本的な考え方に基づいて洗い出し作業を進めることが必要ではないか。

- 通信の秘密は社会活動の基盤としてのコミュニケーションを可能にするというために必要な保護であり、他方、個人情報の保護は事業者と消費者の関係でデータ保護の観点が核心にあったもの。これに対して、プライバシーは、もともとの出発点が私生活の平穏であるが、この部分が電気通信、さらにはIoTの進展によって穴があいてくるという事態が考えられる。このような状況において、これまで個人情報保護に加え、通信の秘密についても記述してきた電気通信事業分野のガイドラインにおいて、さらにプライバシーの観点から議論するということは、時宜を得ているのではないか。

電気通信事業分野ガイドラインの規定

○ 電気通信事業分野ガイドラインは、個人情報保護法と同内容の規定のほか、同法に上乗せ・横出しの規律が設けられている規定及び「通信の秘密」等の電気通信事業法の規律に基づく規定から構成（下線部参照）。

第1章　総則
- 第1条　（目的）
- 第2条　（定義）
- 第3条　（一般原則）

第2章　個人情報の取扱いに関する共通原則
- 第4条　（取得の制限）
- 第5条　（利用目的の特定）
- 第6条　（利用目的による制限）
- 第7条　（適正な取得）
- 第8条　（取得に際しての利用目的の通知等）
- 第9条　（正確性の確保）
- 第10条　（保存期間等）
- 第11条　（安全管理措置）
- 第12条　（従業者及び委託先の監督）
- 第13条　（個人情報保護管理者）
- 第14条　（プライバシーポリシー）
- 第15条　（第三者提供の制限）
- 第16条　（個人情報に関する事項の公表等）
- 第17条　（個人情報の開示及び訂正等）
- 第18条　（理由の説明）
- 第19条　（開示等の求めに応じる手続）
- 第20条　（手数料）
- 第21条　（苦情の処理）
- 第22条　（漏えい等が発生した場合の対応）

第3章　各種情報の取扱い
- 第23条　（通信履歴）
- 第24条　（利用明細）
- 第25条　（発信者情報）
- 第26条　（位置情報）
- 第27条　（不払い者等情報）
- 第28条　（迷惑メール等送信に係る加入者情報）
- 第29条　（電話番号情報）

第4章　雑則
- 第30条　（ガイドラインの見直し）

2　主な検討事項（案）

1　個人情報、個人データ、保有個人データの区別

- 個人情報保護法が適用対象を「個人情報」、「個人データ」、「保有個人データ」と区別しているのに対して、現行の電気通信事業分野ガイドライン　（その解説を含む。以下、単に「ガイドライン」という。）においては、適用対象を一律に「個人情報」としている。改正法施行後もかかる差異を維持すべきか。
- 特に、以下の事項について検討が必要ではないか。
  ①　安全管理措置（第１１条等）
  ②　第三者提供の制限（第１５条）
  ③　個人情報の開示及び訂正等（第１７条）　等

2　要配慮個人情報の取扱い（第4条）

- 改正個人情報保護法においてはセンシティブ情報の取得には原則として本人同意が必要とされているところ、現行のガイドラインにおいては「社会的に相当と認められる場合」にのみ取得が限定されているという差異がある。この点について、どのように考えるべきか。

3　小規模取扱事業者の対応（第2条）

- 現行のガイドラインは取り扱う個人情報が5000人以下の小規模取扱事業者についても適用。改正個人情報保護法により、小規模事業者に法的義務が課せられることになるが、ガイドラインにおいて何らかの対応が必要か。

4　「電気通信サービス」の範囲（第2条）

- 現行のガイドラインにおいては、対象となる電気通信サービスの範囲を「電気通信サービス及びこれに付随するサービス」と規定。電気通信サービスの動向等を踏まえて、具体的な内容を検討することが必要ではないか。

3－1　個人情報、個人データ、保有個人データの区別

問題提起

- 個人情報保護法が保護対象を「個人情報」、「個人データ」、「保有個人データ」に区別して規律しているのに対して、現行のガイドラインにおいては、かかる区別を設けることなく、一律に「個人情報」を保護対象としている。

  ※　平成15年の個人情報保護法制定前から制定されていた電気通信事業保護法制定前から制定されていたガイドラインにおいては、従前より、個人情報全般を対象としており、また、通信の秘密の法理は「個人データ」及び「保有個人データ」に該当しない散在情報にも及ぶこと等の経緯を踏まえ、現行のガイドラインにおいても「個人情報」全体を保護対象としているものと考えられる。

- 現在では、電気通信事業者は個人情報を個人情報データベースの形態で保有・管理していることが一般的であると考えられること等から、ガイドラインが定める保護対象についても、「個人情報」、「個人データ」、「保有個人データ」に区別した上で規律する方向で改正することが考えられるのではないかとも考えられる。
- ただし、画一的に検討するのではなく、ガイドラインにおける各規定が定められた経緯、各規定が設けられている趣旨、「通信の秘密」等の電気通信事業法との関係等を踏まえて、個別の検討を行うことが必要ではないか。

個人情報保護法の適用対象

個人情報保護法の規定	改正個人情報保護法の規定	適用対象
第15条（利用目的の特定）	第15条（利用目的の特定）	個人情報
第16条（利用目的による制限）	第16条（利用目的による制限）	個人情報
第17条（適正な取得）	第17条（適正な取得）	個人情報
第18条（取得に際しての利用目的の通知等）	第18条（取得に際しての利用目的の通知等）	個人情報
第19条（データ内容の正確性の確保）	第19条（データ内容の正確性の確保）	個人データ
第20条（安全管理措置）	第20条（安全管理措置）	個人データ
第21条（従業者の監督）	第21条（従業者の監督）	個人データ
第22条（委託先の監督）	第22条（委託先の監督）	個人データ
第23条（第三者提供の制限）	第23条（第三者提供の制限）	個人データ
（新設）	第24条（外国にある第三者への提供の制限）	個人データ
（新設）	第25条（第三者提供に係る記録の作成等）	個人データ
（新設）	第26条（第三者提供を受ける際の確認等）	個人データ
第24条（保有する個人データに関する事項の公表等）	第27条（保有個人データに関する事項の公表等）	保有個人データ
第25条（開示）	第28条（開示）	保有個人データ
第26条（訂正等）	第29条（訂正等）	保有個人データ
第27条（利用停止等）	第30条（利用停止等）	保有個人データ
第31条（個人情報取扱事業者による苦情の処理）	第35条（個人情報取扱事業者による苦情の処理）	個人情報

主な意見

- ガイドラインの保護対象については、安全管理措置義務の対象、開示等請求権の対象、漏えい等の報告義務の対象という観点から検討をする必要がある。
- 個人情報保護法は全事業分野を規律する最低限のルールを定めたもの。これに対して、電気通信事業分野について独自のガイドラインが規定されてきた趣旨は、電気通信事業における通信の秘密、あるいは、差別的取扱いの禁止などを確保するという観点から、様々なある種の上乗せ的な規律が置かれてきたものと認識。
  そうだとすれば、今般の個人情報保護法の改正によって、全体的に保護のレベルが上がる部分や逆に利活用が広がる部分があるが、それらの規定との関係で、電気通信事業分野の個人情報保護ガイドラインにおいて、なお事業法的規律の観点から見て維持すべき部分があるのか、あるいは、他の事業者と連携していくという観点から見て改正法に合わせた方がよいのか、その基本的な考え方に基づいて洗い出し作業を進めることが必要ではないか。（再掲）
- これまで個人情報を規律してきた電気通信事業分野のガイドラインについて、個人データ、保有個人データという個人情報保護法の概念を持ち込むことは基本的に賛成であるが、他方、ガイドラインの第3章が規定する各種情報の取扱い、例えば通信履歴について、個人情報、個人データのどちらを保護対象とするのかについては、慎重に検討すべき。

取りまとめの方向性（案）

【ガイドラインと個人情報保護法の統一性の確保について】

- 分野横断的なデータ利活用の促進のためには、分野毎にデータの取扱いのルールを異ならせることはできる限り避けるべきと考えられる。また、特段の事情なく事業者にコストを課すことは適当でない。
- このため、通信の秘密の保護等の電気通信事業法の規律に基づく規定や、プライバシーのうち特に保護の必要性が高く、通信の秘密に準じて扱うこととされている位置情報に係る規定など、電気通信事業に係る特有の観点からの規律を除き、保護対象は個人情報保護法におけるものと揃えることを原則とし、ガイドラインはできる限り個人情報保護法と統一のとれたものとすべきではないか。

  ※　なお、個人情報保護法成立時の附帯決議において、特に適正な取扱いの厳格な実施を確保する必要があるとされた医療、金融・信用、情報通信等のうち、医療、金融・信用の各分野のガイドラインにおいては、個人情報保護法と同様に「個人情報」、「個人データ」、「保有個人データ」の区分を行っている。
- ガイドラインの各規律が「電気通信事業に係る特有の観点からの規律」であるか否かは、改正法の下で整備される下位法令や汎用的なガイドラインの内容も踏まえて、今後、詳細な検討を行う必要があると考えられるが、例えば、安全管理措置、第三者提供の制限、個人情報の開示及び訂正等については、以下のように考えることができるのではないか。

【安全管理措置に関連する規定（「安全管理措置」、「従業者及び委託先の監督」、「個人情報保護管理者」、「保存期間等」）】（第10条～第13条）

- 電気通信事業は通信の秘密と直接かかわる事業であり、電気通信事業者が取り扱う個人情報は、通信の秘密と密接にかかわるものと言うことができる。また、「通信の秘密」に該当する個人情報は、電気通信事業法により、罰則の下で通常の個人情報よりも厳格に保護されることとなる。
- これを踏まえ、ガイドラインの安全管理措置に関する規律は、①個人情報一般に係る安全管理措置を規定しつつ、それを基礎として、通信の秘密に該当するもの等についてより厳格な措置を求めているほか、②その内容に通信の秘密の保護の観点も含めた通信の安定的な提供、通信の疎通の確保、通信の不正使用の防止等を目的とする「情報通信ネットワーク安全・信頼性基準（昭和62年郵政省告示第73号）」の活用を求めるなど、通信の秘密に該当する個人情報の取扱いにも関連する内容を含むものとなっている。
- 以上を踏まえれば、ガイドラインの安全管理措置に関する規律は、個人データだけでなく、個人情報にも及ぼすことを維持することが適当ではないか。

【第三者提供の制限】（第15条）

- 現行ガイドラインの第三者提供の制限に係る規律において、通信の秘密に該当する個人情報については、確認的な規定又は解説が行われているに過ぎない。
- 電気通信事業者が取り扱う個人情報は個人データ化されていることが一般的であることを踏まえると、通信の秘密に該当しない個人情報については、個人情報保護法の規律と第三者提供の制限に係る規律を異ならせるべき特段の事情は認められないのではないか。
- したがって、ガイドラインをできる限り個人情報保護法と統一のとれたものとする観点から、その対象を「個人データ」とすることが適当ではないか。

【個人情報の開示及び訂正等】（第17条）

- ガイドラインにおける開示及び訂正等の規律は「保有個人データ」だけでなく「個人情報」をその対象とするが、通信の秘密の保護のように、電気通信事業法の具体的規律を背景としているものではない。
- 開示については、現行のガイドラインは、「電気通信事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合」として適用が除外される場合に該当する例として「個人データに該当しない個人情報」（以下「散在情報」という。）の開示が求められた場合を例示するとともに、開示の対象を電気通信事業者がその権限を有している情報に限定しており、実質的には、その対象を「保有個人データ」に絞っているということができる。
- 訂正等については、電気通信事業者がその権限を有している情報に限定する一方で、散在情報を除外する記載はないものの、開示の実質的な対象が「保有個人データ」に絞られており、また、電気通信事業者が取り扱う個人情報が個人データ化されていることが一般的であることを踏まえると、散在情報を訂正等の対象とする特段の必要性は見出しがたい。
- また、改正法により開示及び訂正等の求めが請求権として明確化されるが、明確化の対象は「保有個人データ」に限定されるため、散在情報に対する開示及び訂正等の求めの相対的な重要性は、改正法の施行により一層小さくなると考えられる。
- 以上を踏まえると、散在情報を開示及び訂正等の対象とする必要性は高くないと考えられ、ガイドラインをできる限り個人情報保護法と統一のとれたものとする観点から、その対象を「保有個人データ」とすることが適当ではないか。

3－2　要配慮個人情報の取扱い（第4条関係）

問題提起

- 改正個人情報保護法においては、要配慮個人情報の概念を導入し、原則として、本人の同意を得ないで要配慮個人情報を取得してはならないとしている。
- これに対して、現行のガイドラインにおいては、社会的に相当と認められる場合を除き、センシティブ情報を取得しないものとされており、かかる規律は本人同意がある場合にも適用されると考えられる。
- 現行のガイドラインの規定を改正しない場合、改正個人情報保護法との整合性、事業者のサービスの提供・充実等の観点から（例えば、電気通信事業者が、訪日外国人向けの多言語サービスや健康・医療関係サービスを提供する場合）、何らかの問題が発生すると考えられるか。
- 他方、ガイドラインの現行の規律を維持した場合に、改正個人情報保護法との整合性、事業者負担の観点等から、何らかの問題が発生すると考えられるか。

主な意見

- 個人情報保護法改正との関係で、対象情報の整合性、本人同意要件を追加するかどうか、一段上乗せして規制をするかどうかを検討する必要がある。
- 電気通信事業法における利用者に対する差別的取扱いの禁止を確保するという観点から必要なのか、通信の秘密の保護を十全なものにするという観点から必要なのか、整理が必要である。

取りまとめの方向性（案）

- センシティブとされる個人情報（以下「センシティブ情報」という。）に関する規定（ガイドライン第４条第２項）は、センシティブ情報は電気通信サービスを提供するために不要と考えられるため、社会的に相当と認められる場合を除いて取得しないものとし、利用者に対する差別的取扱いの禁止を確保するものである。この規律は、電気通信事業の公共性に鑑み、電気通信事業者全般に課されている重要な規律である、利用の公平について定めた、電気通信事業法第６条を確実なものとするために重要な役割を果たしている。
- 改正個人情報保護法で新設された、要配慮個人情報に関する規定（改正個人情報保護法第２条第３項、第１７条第２項）は、その取扱いによっては差別や偏見を生じる恐れがあるため、特に慎重な取扱いが求められる個人情報について、本人が取得に関与できるようにしたものである。
- これらの観点からすると、センシティブ情報に関する規定と要配慮個人情報に関する規定はその趣旨が類似すると考えられ、電気通信事業者が異業種と連携してサービス提供する事案が増加していくと考えられること、電気通信事業と異業種とで差別的取扱いにつながる情報に大きな相違はないと考えられることからすると、両者で別の規律を設けることは煩雑である。
- したがって、センシティブ情報に関する規律は、要配慮個人情報に関する規律に一本化させる方向で検討すべきではないか。もっとも、要配慮個人情報に関する規律については、政令、ガイドライン等でより詳しく定められる予定であるため、その内容を注視する必要がある。

３－３　小規模取扱事業者（第2条関係）

問題提起

- 電気通信事業分野ガイドラインでは、規律対象を「電気通信事業を行う者」とし（第２条）、識別される個人の数による除外対象を設けていない。これは、電気通信事業法で、事業規模にかかわらず規律が及ぶとされていること（電気通信事業法第２条）と、整合性を持たせるためと考えられる。
- 改正個人情報保護法では、５千人分以下の個人情報を取り扱う事業者について法の適用を除外する規定を廃止しており（同法第２条第５項）、それにともない、個人情報保護委員会がガイドラインを定めるにあたっては、特に事業規模の小さな事業者の事業活動が円滑に行われるよう配慮するものとされている（改正法附則第１１条）。
- 特に事業規模の小さな事業者については、個人情報保護委員会が定めるガイドラインにおいて、安全管理措置などについて、事業規模の大きな事業者と同等の措置までは求められないという配慮がされる可能性があるところ、同規律は「電気通信事業を行う者」についても適用されるべきと考えられるか。

取りまとめの方向性（案）

- 電気通信事業法の規律が事業規模にかかわらず及ぶとされていることからすると、特に事業規模の小さな事業者であっても、事業規模の大きな事業者と同じ規律が及ぶと考えるべきではないか。このように考えても、現在と同等の措置を取れば足り、新たな負担は生じず、問題はないのではないか。

3－4　「電気通信サービス」の範囲（第2条関係）

問題提起

- 現行の電気通信事業分野ガイドラインにおいては、ガイドラインが対象とする「電気通信サービス」について、「電気通信役務及びこれに付随するサービス」と規定している。
- 他方、「付随するサービス」の範囲については、必ずしもガイドラインにおいて、明らかにされていない。また、タスクフォース事務局が実施したアンケート結果を踏まえると、事業者サイドにおいても様々な解釈がなされている状況にある。
- 現在、電気通信事業者は、電気通信役務そのもののみならず、電気通信役務の機能に影響を及ぼすサービスのほか、電気通信役務と密接に関連する多様なサービス（決済代行、アプリ・コンテンツ系サービス、電子マネーポイント還元サービス等）を提供し、利用者へのサービス向上を図っている。また、今後は、異業種と連携したサービスの提供も広がっていくことが予想される。
- このような状況を踏まえ、本ガイドラインが対象とする「電気通信役務及びこれに付随するサービス」の範囲について、どのような基準に基づき、明確化を図るべきであると考えられるか。
  - 例えば、電気通信役務に特有の性質等を踏まえ、①電気通信役務と一体的に提供されていて切り離すことができないもの、②利用者の保護及び利便性向上の観点から一体的に取り扱うことが望ましいものといった基準が考えられるのではないか。その他に考慮すべき基準はあるか。
  - また、上記の付随するサービス以外のもの（例えば、異業種のサービスに対して個人情報を提供する場合等）について、どのように考えるべきか。
  - さらに、現行ガイドラインの利用目的の特定・変更（第5条第1項～第3項）、利用目的による制限（第6条第1項）等の規定との関係についても検討する必要があると考えられるが、どのような観点に基づいて整理を行うべきか。

主な意見

- ガイドラインにおいては、個人情報の取得を電気通信サービスを提供するために必要な場合に限定し、利用目的の変更もその範囲においてのみ認めており、個人情報保護法とのギャップが大きいのではないか。
- ガイドラインの対象となる「電気通信サービス」の定義について、「付随するサービス」の範囲を含め、必ずしも明確になっていない。取得の制限等を検討する前提として、定義・範囲の明確化を図ることが必要ではないか。
- 今後、電気通信事業者は、シナジー効果を狙って、多様な業種と連携していくことが考えられるが、ガイドラインではこのような場合についても視野に入れるべき。
- 通信端末が非常に高度化・高機能化している状況において、電気通信サービスの範囲を古い意味での通信に限定して考えていいのか、という問題がある。また、サードパーティとの関係も含めた市場性の問題といったこともあり、これらの点について、総合的に検討する必要があるのではないか。

取りまとめの方向性（案）

- ガイドラインは個人情報保護法の制定以前から策定・改正が行われて来ているが、このような電気通信事業分野を特に対象とした個人情報保護の検討の背景として、これまでの累次の研究会等では、電気通信事業にかかる個人情報の特殊性やその保護の必要性等を挙げている。その内容は概ね以下のとおりである。
  - 電気通信分野においては、電気通信事業の公共性に加え、通信の秘密という通信にかかわる個人情報の中核を取り扱う電気通信事業者の責務として、個人情報の保護が図られることに対する国民の期待が大きい。
  - 電気通信役務を提供する日常的な業務の過程において、通信履歴をはじめとする個人情報が時々刻々大量に作り出され、蓄積される。さらに、個人を特定するための鍵となる個人情報として広く一般に利用されている電話番号情報等を個人に付与し、データベースに蓄積している。

- このうち、特に後者に関しては、近年、電気通信事業者による異業種を含む多様なサービスの提供や、こうしたサービスを提供する多様な事業者との連携が進んでいること、また、IoTの進展によりネットワークを通じて流通･蓄積されるデータが多様かつ膨大となっていることによって、個人に関する様々なデータが電気通信事業者に集約され得るという特殊性が一層際立つようになっており、そのデータの保護の必要性は更に高まっていると考えられる。
- また、このような状況の中で、通信の秘密に該当するデータも多様かつ膨大に発生するようになっており、前者の観点の特殊性も強まっていると考えられる。
- 以上を踏まえると、ガイドラインが規律対象とする「電気通信サービス」には以下を含めることが適当ではないか。
  - 電気通信役務と一体的に提供されていて切り離すことができないサービス
  - 当該事業者が提供する電気通信役務の利用を前提としているサービス
  - 上記のいずれにも該当しないが、当該事業者が提供する電気通信役務に係るシステムと連携し、又は、当該事業者が提供する電気通信役務に係る利用者情報との紐付けが行われるサービス
- なお、「電気通信サービス」の範囲を上記のように捉えた場合、電気通信事業者が保有する個人情報の利用目的を「電気通信サービスを提供するために必要な範囲」に制限するガイドライン第５条第３項の規定によって、電気通信事業者が提供するサービスの範囲が実態以上に狭められることにはならないと考えられる。

（参考）電気通信役務に「付随するサービス」に該当し得るサービス（例）

○電気通信役務と一体的に提供されていて切り離すことができないサービス	・ネットワークでのフィルタリング ・ルータ等接続機器の貸与 ・システムの開発、保守
○当該事業者が提供する電気通信役務の利用を前提としているサービス	・端末の位置検索 ・セキュリティ ・決済代行 ・端末の販売、端末の保証 ・アプリ、動画配信、音楽配信、クーポン配信 ・電子マネーポイント還元サービス ・ID連携による自動ログインサービス ・電力等のセット割 ・電話帳
○上記のいずれにも該当しないが、当該事業者が提供する電気通信役務に係るシステムと連携し、又は、当該事業者が提供する電気通信役務に係る利用者情報との紐付けが行われるサービス	・異業種のサービス －電力 －保険 －総合生活サポート －ネット宅配サービス －グルメ、旅行 ・アプリ、動画配信、音楽配信、クーポン配信

※　想定され得る例であり、個別サービスに応じた検討が必要。

Ⅰ　位置情報の取扱いについて

Ⅱ　スマートフォンの利用者情報の取扱いについて

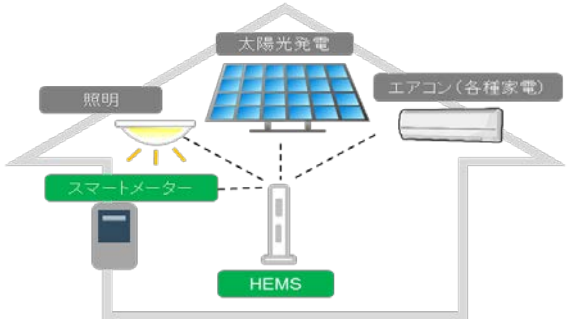
Ⅲ　電気通信事業分野ガイドラインのその他の改正事項について

Ⅳ　IoTとプライバシーについて

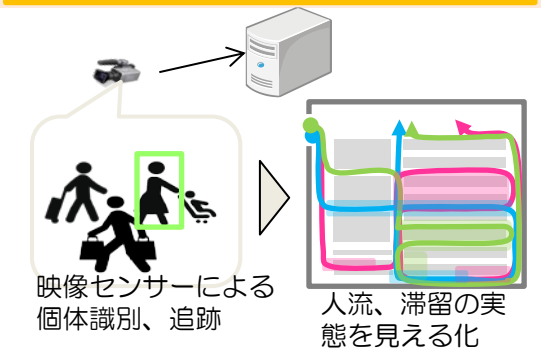
1　IoTとプライバシー（事例）

	エネルギー	自動車	映像センサー
サービス概要	• HEMS 電力の見える化サービスによって、節電を喚起。 • 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。	• 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。 • 走行実態から、事故リスクを判定し、ユーザごとの保険料を最適化。	• 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。
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。	• 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は、プライバシー性が高い。 • 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がトレースされる可能性。	• 本人が撮影を回避する手段が無い一方、明示的な同意取得が難しい。 • 取得されたデータを、本人が閲覧･修正することが難しい。

HEMS（ホームエネルギー・マネジメントシステム）



デバイス



（第1回会合　小林構成員提出資料に基づいて事務局作成）

2　IoTの特徴（プライバシーの観点から）

問題提起

- IoTの進展がもたらすプライバシー上の課題を検討する前提として、多様なデバイスやサービスを通じて大量のパーソナルデータを取得・分析・利用するIoTのデータには、プライバシーとの関係でどのような特性があるか。
- IoTの進展は、従前は本人とデータ利用者の2者間の問題であったプライバシーについて、どのような変化をもたらすか。

①　IoTが収集するパーソナルデータの特性

主な意見

- パーソナルデータは、① 個人が生成し明示的に共有される「主体提供データ」、② 個人の過去の行動に基づく「観測データ」、③ ①、②から推定・プロファイリングされる「推定データ」に分類できる。IoTと特に関わってくるのは、②の個人の行動履歴に係る「観測データ」。
- IoTが収集するデータの中には、長期間貯めることで個人が見えてくるデータや、解釈によって個人の行動履歴となるデータ、個人を特定するリスクが高いデータが存在。
- PCやスマートフォンに加え、家電、自動車、健康機器等から個人の行動履歴データが集約できるようになり、詳細な生活パターン、趣味嗜好、行動範囲といったプライバシー性の高いデータが蓄積され、高い精度でプロファイリングされる可能性がある。他方、行動履歴や位置情報については、他人に知られたくないという意識が高いという調査結果もある。

- IoTによって収集されるデータの一部は、個人情報保護法改正の議論の過程で提案された「（仮称）準個人情報」、すなわち、その情報だけでは個人を特定しないが、一人一人の個人を区別できる情報が含まれており、外部情報との照合やデータの組み合わせ方により、個人の特定やプライバシー侵害に至る可能性が高いのではないか。

主な意見（続き）

- IoTでは、現実世界における空間的位置と時刻が名寄せの起点となりやすく、複数の情報の突合により照合が容易になるという特徴がある。IoTにより現実世界は、サイバー空間よりも個人の特定可能性が高くなる。
- IoTによるデータの取得を個人本人が分かるとは限らない。また、利用目的や利用者が明示されていない場合が多く、データ取得の回数や種類も膨大となる。
- スマート家電、機器・デバイスがデータを収集しているという事実を本人は十分に認識していない、できない場合が発生。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も困難な場合が発生。
- IoTのデータは本人の知らない間にセンシングされる（センサーは本人の身体から離れるほど認知されにくくなり、接触頻度も少なくなる）。また、個別にセンシングされないようにするのは不可能。
- パーソナルデータは「個人情報」への該当性が不明確であり、プライバシーリスクが千差万別。さらに、IoTの進展により、データそのものよりもコンテキスト（ものごとの経緯）が、プライバシーリスクを大きく左右。

② IoTの進展によるセンサー等の飛躍的増大

主な意見

- 今後、IoTの進展により、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。
- IoTの発展について、スマートフォンやスマートフォンと接続するセンサーの普及が大きく寄与。また、ZigbeeやBluetooth等の近距離で安いコストで通信できる規格が普及。
- IoTの進展によりセンサーが増える、あるいは家電がセンサーになると考えた場合、家電製品にはディスプレイがない。このことが本人への説明や同意取得を困難にする。

③ 多数の関係者（マルチステークホルダー）の出現

- IoTによるデータの取得・分析・利用においては、本人とそのデータの利用者の二者にとどまらず、データの対象者、所有者、設置者、分析者、分析結果の利用者等の多くのステークホルダーが存在することになり、その調整が必要。
- IoTにおいては、多種多様なステークホルダーが存在。例えば、モバイル、ソーシャルネットワーク、ビッグデータでは、キャリア、プラットフォーマー、分析事業者等の様々な主体がサービスの提供に関与。IoTの台頭により、さらに、自動車、住宅、家電など、消費者へのタッチポイントが増大。サービス提供に関与する一連の事業者が、消費者団体や監督機関と連携して消費者保護のあり方を考えることが必要。
- これまで個人情報やプライバシー保護に関わってこなかった事業者もIoTでは関わってくることになり、知らない間にプライバシー侵害を引き起こすリスクがある。

意見のまとめ

- IoTが収集するデータには、個人の行動履歴を中心としたパーソナルデータが多く存在。これらのデータはそれ自身もプライバシー性が高いほか、外部情報との照合等により個人を特定する可能性が高いもの。
- IoTの進展により、身の回りのセンサーの数が飛躍的に増大。本人が十分に認識しないままにセンシングされ、データを取得される可能性がある。また、個別にデータ取得を回避することも困難。
- IoTにはデータの対象者、所有者、分析者、分析結果の利用者、機器の設置者等、多くの関係者（マルチステークホルダー）が存在。
- IoTに関するプライバシー保護を検討するに当たっては、このようなIoTのデータの特性やプレーヤーの存在を前提として、検討を進める必要がある。

（参考1）パーソナルデータの分類

○ Volunteered data（自発的生成データ）
個人が生成し、明示的に共有されるデータ
例）ユーザ登録、SNSの書き込み

→ ○個人情報保護法の範囲
ただし、同法の対象は、特定の個人を識別する情報であり、プライバシーではない。

○ **Observed data（観測データ）**
個人の過去の行動に基づくデータ
例）防犯カメラ画像、購買履歴

→ ○**IoTが生むパーソナルデータ**
個人は観測されていることに気づくとは限らないし、利用目的や利用者は明示されていないことが多い。

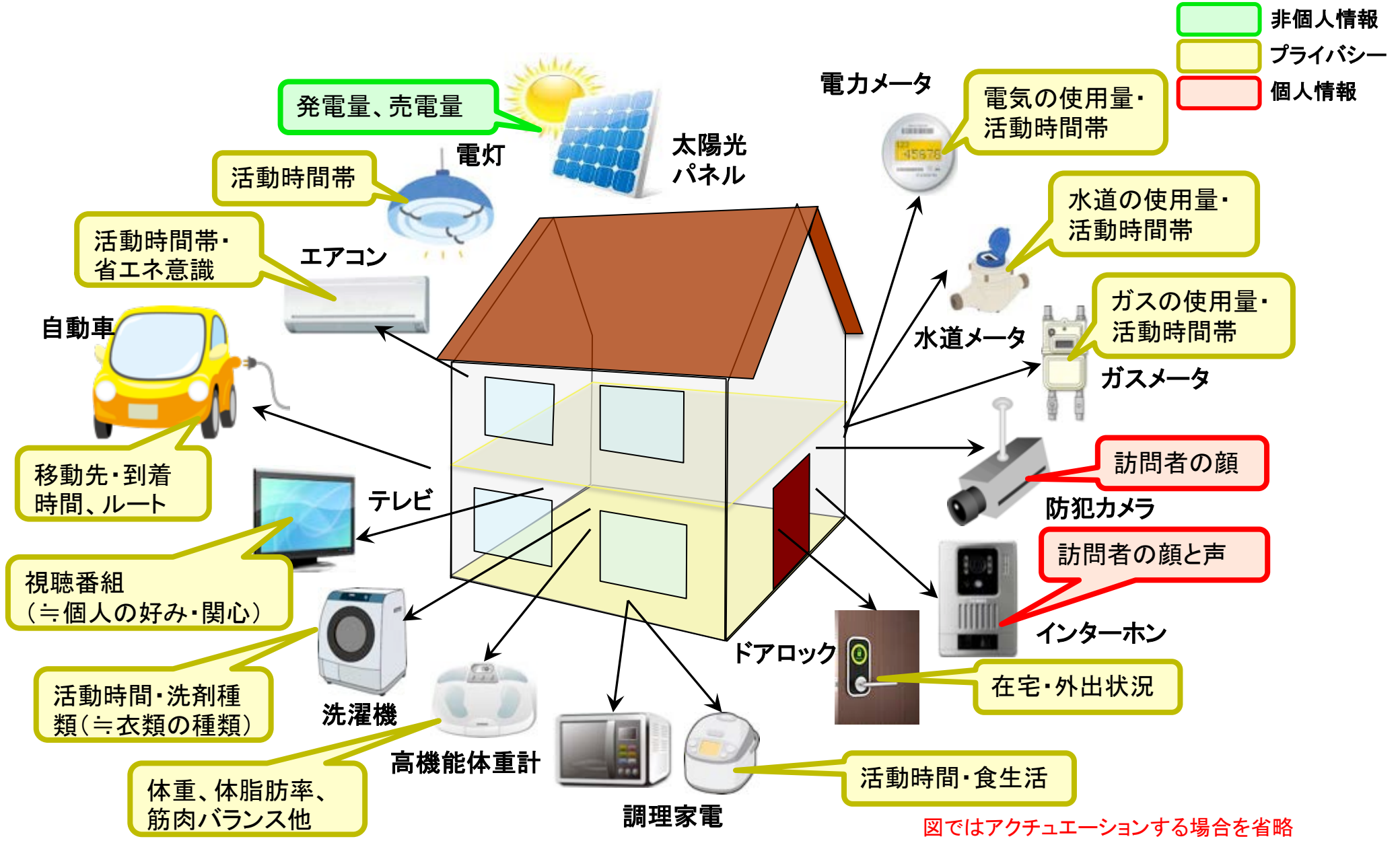
○ Inferred data（推定データ）
自発的生成データ及び観測データから、推定・プロファイリングされたデータ
例）SNSのユーザプロファイリング、
クレジットカードの与信情報

→ ○個人はデータの存在さえ知らない。このためオプトアウト的取り扱いは向かない。
○間違った推測による権利侵害が起きうるが、損害賠償による事後救済しかない。

※この3分類はThe World Economic Forumが2011年に出した報告書「Personal Data: The Emergence of a New Asset Class」による。

（第4回会合　佐藤構成員提出資料に基づいて事務局作成）

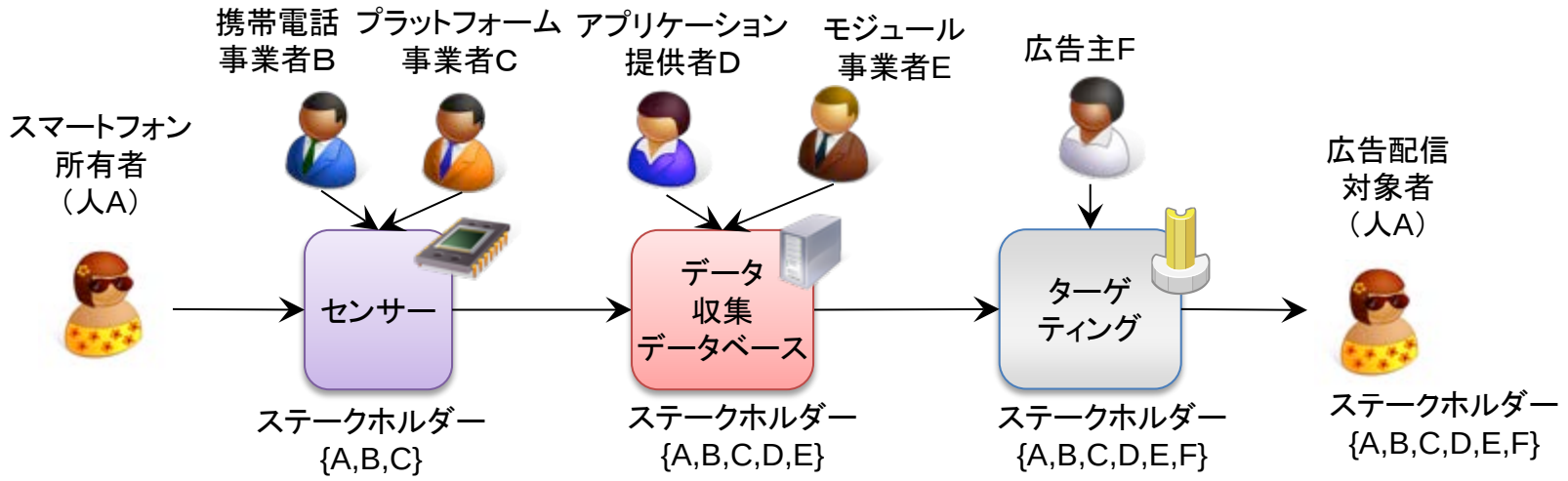
（参考2）IoTが取り扱うパーソナルデータの例



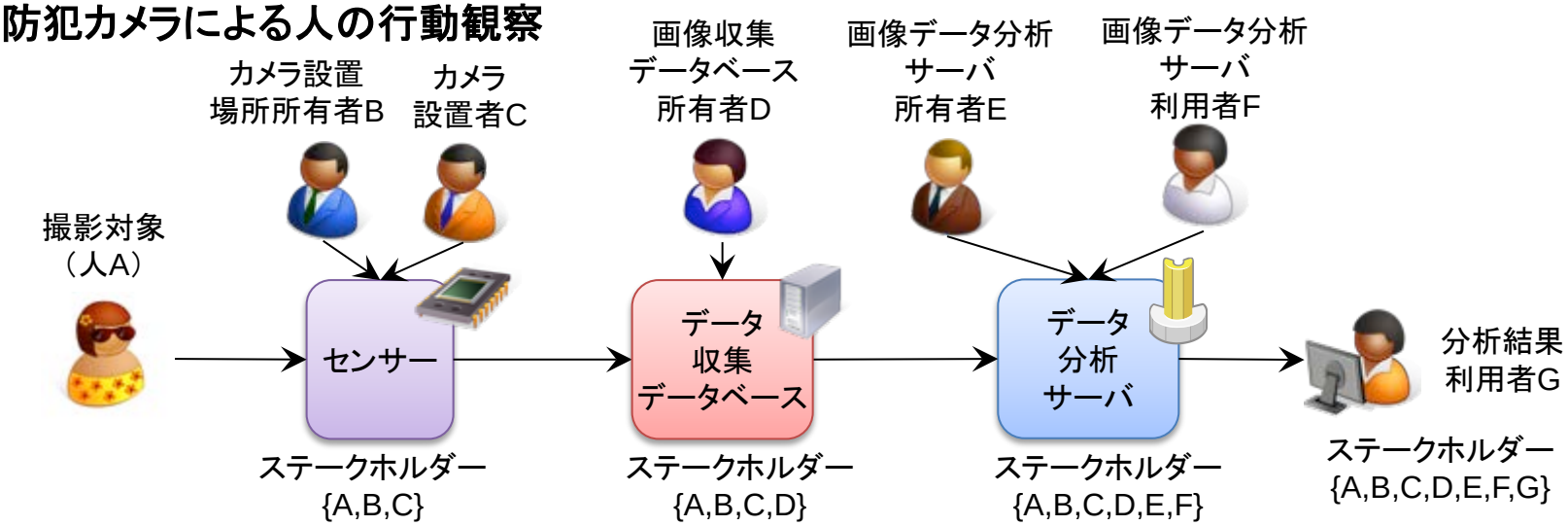
（第4回会合　佐藤構成員提出資料）

（参考3）IoTにおけるマルチステークホルダー（イメージ）

例：スマートフォンのGPS位置情報を利用したターゲティング広告



例：防犯カメラによる人の行動観察



（第4回会合　佐藤構成員提出資料に基づいて事務局作成）

3　IoTがもたらすプライバシー上の課題

（1） 透明性の確保及び同意取得との関係

問題提起

- IoTの進展は、プライバシー保護の重要な原則である「透明性の確保（事前の説明等）」及び「同意取得」にどのような影響を及ぼすか。
- 特に、IoTが収集するデータの特性を踏まえると、実効性のある説明や同意取得が困難になる場合があるのではないか。

① 透明性の確保（事前の説明等）

主な意見

- 複雑化、多重化する利用者への説明が透明性の低下をもたらしており、本人への説明がどんどん難しくなっている。
- 具体的には、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の二重化、利用規約と約款等のその他の重要な規約、消費者とのタッチポイントの増大が発生し、透明性の確保が困難となっている。
- プライバシー保護の原則に「目的の限定とデータ最小化」があるが、IoTではあらかじめ目的を明確化することが困難なケースが発生。例えば、研究開発において、目的の限定や限定された目的を分かりやすい言葉で表現するのは難しい。
- IoTの進展によりセンサーが増える、あるいは家電がセンサーになると考えた場合、家電製品にはディスプレイがない。このことが本人への説明や同意取得を困難にするのではないか。
- 透明性の確保を図るため、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に係る取組が進められているが、形式化の拡充を図ることには限界。
- IoTにおける説明や同意取得の困難は非常に大きな問題。今後、その原因や対策を検討していく必要。
- 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ではないか。ただし、基本的な「透明性の確保」についての指針は必要で、その上で考えることが前提。

主な意見（続き）

- 現行法においても、防犯カメラの問題一つとってみても、誰がどこに書けばいいのかということで利用目的の通知というのが難しくなってきている。
- IoTにおいて取得を委託あるいは再委託している場合に、本人に何らかのかたちで利用目的を通知・公表しなければならないのかといった点について整理が必要なのではないか。また、ある者が一つのセンサーで複数の者のためにデータを取得している場合についても整理が必要なのではないか。

② 同意の取得

主な意見

- IoTが収集するデータの特性上、そもそも本人がデータ取得に気づかない、あるいは、逐次同意を取得することは現実的ではないケースが多く、従来の方法による同意取得が困難になる場合もでてくる。
- 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、本人はその事実を十分に認識しない、あるいは、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（閲覧）したり、訂正したりすることが難しい場合がある。
- サービス及び事業者数の増大、パーソナルデータの取得ポイントの増大、IoT進展に伴う非接触のデータ取得等により、同意取得や本人関与がどんどん難しくなっている。
- IoTの進展により、データそのものよりもコンテキスト（ものごとの経緯）が、プライバシーリスクを大きく左右。その一方で、実効性のある本人同意の取得はより困難になっていく。
- 現在でも監視カメラなど、実質的に事前の同意取得が困難な場合がある。今後、IoTの進展により、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。
- データ取得について本人にどう知らせるか、どう同意を取るかを決めるべきだが技術的にも難しい問題。
- IoTでは、取得のところの透明性の確保と同意は重要。その原因と対策を今後検討すべき。（再掲）

② 同意の取得

主な意見（続き）

- 同意に関する議論は、米国でも、とりわけ行動経済学の知見で「ナッジ」の議論がなされており、そのような手法でどこまでカバーできるのかということは考える必要があるのではないか。
- 現実的かつ有意な確認の仕組みが必要であり、権限委譲やトラストに至る問題ではないか。
- IoTにおいて、あらかじめの完全な同意取得は「十分な透明性」が前提となり、事業者、利用者ともに負担が重く、形式的なものになってしまう。これを認識した上で、取得規制から行為規制への移行が必要ではないか。

意見のまとめ

- **IoTにおいては、収集するデータやセンサー等の特性上、実効性のある透明性の確保（本人への説明等）や同意取得が困難になるケースが増えていくことが想定される。そのような状況において、透明性の確保や同意取得を形式的に求めるだけでは、かえって本人や事業者等の関係者の負担を重くするおそれがあるのではないか。**
- **実効性のある透明化の確保や同意取得が困難になっていくことを踏まえ、透明性の確保や同意取得の重要性を十分に認識しつつ、IoTの特性を踏まえた新たなルールの確立が必要になるのではないか。**

（2） 多数の関係者間（マルチステークホルダ）の調整

問題提起

□ IoTによるデータの取得・分析・利用には、本人をはじめ多くの事業者等が関与。このことにより、どのような課題が発生するか。

主な意見

- 取得したデータの帰属（誰のデータを、どのような権限に基づいて誰が管理するのか）、いわゆるステークホルダーの問題はIoTの本質的な問題。IoTによるデータの取得・分析・利用においては、本人とそのデータの利用者の二者にとどまらず、データの対象者、所有者、設置者、分析者、分析結果の利用者等の多くのステークホルダーが存在することになり、その調整が必要。
- プライバシー保護は、マルチステークホルダ問題の中に含まれる問題であることを認識することが必要。
- IoTにおいては、多種多様なステークホルダーが存在。例えば、モバイル、ソーシャルネットワーク、ビッグデータでは、キャリア、プラットフォーマー、分析事業者等の様々な主体がサービスの提供に関与。IoTの台頭により、さらに、自動車、住宅、家電など、消費者へのタッチポイントが増大。サービス提供に関与する一連の事業者が、消費者団体や監督機関と連携して消費者保護のあり方を考えることが必要であり、マルチステークホルダープロセスの確立・活用が重要。

意見のまとめ

- IoTにおいては、データの対象者、所有者、設置者、分析者、分析結果の利用者等、多くの関係者（マルチステークホルダー）が出現。
- プライバシー保護の問題についても、これら多数の関係者間の調整を図ることが重要であり、そのための新たな枠組みを検討していくことが必要ではないか。

プライバシー原則（ISO/IEC 29100等）とIoTにおける課題の関係（案）

○ IoTがもたらす課題について、プライバシー原則に照らし合わせて整理することが有効ではないか。

原則	IoTにおける課題
1　同意と選択	• 本人がデータ取得を認識しない場合や回避できない場合が発生し、実効性のある同意取得等が困難。
2　目的の正当性と詳述	• 目的の特定やサービス開始後にデータに新たな価値が発生した場合の対応等に関するルールが必要。
3　収集の制限	• IoTデータの特性上、実効性のある同意取得等の本人関与が困難。 • サービス提供に直接関係しないものの、一体的に取得されるデータの取扱いルールが必要
4　データ最小化	• データの限定取得の技術的難しさ（コストを含む）が発生。 • データ最小化の手法としての匿名化の活用に関する検討が必要。
5　利用、保持、開示の制限	• 多数のステークホルダーが関与。責任分担も含め、関係者間における利用等のルールが必要。
6　正確性と品質	• プライバシー性の高い情報が蓄積され、高い精度のプロファイリングが行われる場合、リスク対策が必要。
7　オープンさ、透明性、通知	• 実効性のある事前の説明等の透明性確保が困難。
8　個人の参加とアクセス	• 開示の範囲に関するルールが必要。 • 多数のステークホルダーが関与。開示の範囲も含め、関係者間における開示等のルールが必要。
9　説明責任	• 多数のステークホルダーが関与。関係者間の責任分担のルールが必要。
10 情報セキュリティ	• 機能及び性能の制約が大きいIoTデバイスでは、高度なセキュリティ技術を導入することは容易ではない。
11 プライバシー法令遵守	• 多数の法令、ガイドライン、契約約款等が存在し、多重化・複雑化している。

（参考）プライバシー保護の原則

OECD8原則

原則	原則の内容
1.目的明確化	収集目的を明確にし、データ利用は収集目的に合致するべき
2.利用制限	データ主体の同意がある場合、法律の規定による場合以外は目的以外に利用使用してはならない
3.収集制限	適法・公正な手段により、かつ情報主体に通知又は同意を得て収集されるべき
4.データ内容	利用目的に沿ったもので、かつ、正確、完全、最新であるべき
5.安全保護	合理的安全保護措置により、紛失・破壊・使用・修正・開示等から保護するべき
6.公開	データ収集の実施方針等を公開し、データの存在、利用目的、管理者等を明示するべき
7.個人参加	自己に関するデータの所在及び内容を確認させ、又は異議申立を保証するべき
8.責任	管理者は諸原則実施の責任を有する

出所）個人情報保護法制化専門委員会（2000年）

ISO/IEC 29100 プライバシーフレームワークの11原則

原則	主な内容
1. 同意と選択	本人に、明確で分かりやすくアクセスしやすい選択の仕組みを提供し、データ処理に対する同意を取得する。 本人が同意時に、自分の好みにあった設定をできるようにする。 ※OECD8原則に対応する原則は無い。
2. 目的の正当性と詳述	OECD8原則「目的明確化の原則」と同等
3. 収集の制限	OECD8原則「収集制限の原則」と同等
4. データ最小化	データの処理を必要最低限にする。 処理する者を最低限にする。 個人の特定、他データとの照合、属性推定を制限する。 ※OECD8原則に対応する原則は無い。
5. 利用、保持、開示の制限	正当な利用目的の範囲の中で、データの利用、保持、開示をする。 必要最低限の期間だけデータを保持し、期間が過ぎたら安全に廃棄するか匿名処理をする。 ※OECD8原則「利用制限の原則」に対応
6. 正確性と品質	利用目的に沿ったもので、正確、完全、最新のものとする。 不正確なデータによって、個人に実害が生じうる場合は、特に重要。 ※OECD8原則「データ内容の原則」に対応
7. オープンさ、透明性、通知	OECD8原則「公開の原則」と同等
8. 個人の参加とアクセス	OECD8原則「個人参加の原則」と同等
9. 説明責任	OECD8原則「責任の原則」と同等
10. 情報セキュリティ	OECD8原則「安全保護の原則」と同等
11. プライバシー法令遵守	個人情報・プライバシー保護の関連法令を遵守する。 ※OECD8原則に対応する原則は無い。

出所）小林慎太郎「パーソナルデータの教科書」日経BP

4　具体的な解決方策の検討

IoT の特徴

IoTデータの特性
- 個人の行動履歴
- 外部情報との照合により個人特定の可能性

センサーの飛躍的増大等
- 本人がデータ取得を認識できない
- 個別のデータ取得回避が困難

多数の関係者の出現
- 多種多様なステークホルダーが存在

IoTがもたらすプライバシー上の課題

- 透明性の確保の困難（事前の説明等）
- 本人関与の困難（同意取得等）
- 多数の関係者間の調整の必要

具体的な解決方策の方向性

- マルチステークホルダープロセスの活用
- 行動規範等の策定
- 本人によるデータ管理の仕組み
- プライバシー保護技術の活用

検討事項（案）

（1） マルチステークホルダープロセス（MSP）の活用

- IoTにおいては、従来の本人とデータ利用者という2者間の関係にとどまることなく、多種多様なステークホルダーが出現。データの自由な流通を確保しつつプライバシー保護を図るためには、IoTに関与する利用者、事業者等の一連の関係者が連携することが必要との認識の下、マルチステークホルダープロセス（MSP）を積極的に活用すべきではないか。
- MSPの実施に当たって、これまでの経験及び諸外国の取組状況等を踏まえ、どのような点に留意すべきか。

（2） 行動規範等の策定

- IoTにおいては、個人の行動履歴等に係るプライバシー性の高いデータが取得されると考えられる。一方で、本人がデータの取得に気付かない場合やそもそもデータの取得を回避することが難しい場合が発生することも想定され、実効性のある本人への事前の説明や同意取得には限界があると考えられる。
- 実効性のある透明性確保や同意取得には一定の限界があることを認識した上で、そのような状況を補完し、消費者が望まない利用やプライバシー侵害を回避するため、関係者が連携して行動規範等の策定に取り組むことが必要ではないか。

（3） 本人によるデータ管理の仕組み

- IoTにおいては、多種多様なサービスが出現し、透明性の確保が困難になること等を踏まえれば、本人のデータ提供に関するポリシー管理を行うなど、利用者自らがデータの提供をコントロールする仕組みは有効な解決方策となり得るのではないか。

（4） プライバシー保護技術の活用

- データの自由な流通を確保しつつプライバシー保護を支援する取組に係る技術について、どのような動向があるか。

主な意見①

（1） マルチステークホルダープロセス（MSP）の活用

- 欧米ではMSPについて政府と民間が連携して試行錯誤を続けている。
- 米国では、米国商務省電気通信庁（NTIA）がホワイトハウスの指示を受けてMSPによる自主規制スキームについて、モバイルアプリの通知に関する行動規範、顔認証技術に関する行動規範、セキュリティ脆弱性の開示に関する行動規範等に取り組んでいる。また、オランダでは、個人情報保護の領域で業界団体が起草して、個人情報保護の監督機関が認定する行動規範の制度を導入。
- MSPの長所として、オープン性及び透明性の確保、法令の枠組みと比べてルール策定を迅速に行うことができることがあげられる。課題として、参加者には消費者団体や業界団体など、誰の利益を代弁しているかが明確である必要がある。
- 我が国においても、初期段階では国が積極的に関与し、我が国の制度・慣習に適した方法でMSPを進めるべき。
- ステークホルダーが多数いて特定困難な場合、国民の大エージェントとして政府が規制を行う。マルチステークホルダープロセスは、政府の権限を小さくする代わりに、できるだけ民間サイドで問題を解決するという流れの中に、ステークホルダーが見つからない場合には、同プロセス自体に政府が関与していく局面も考えられるのではないか。
- 全体としては自主規制に寄っていきつつ、関係の行政機関も自主規制に協力していくということになるのではないか。その意味では、司会進行をNTIAがやって、FTCがそれに関わっているというのは興味深い取組。
- MSPの策定に当たっては、①ゴールの明確化、②オープン性の確保、③非公式な会合の活用、④執行機関/行政機関の確保、⑤参加者の代表性への配慮、⑥執行性の確保といった点がポイントになるのではないか。

主な意見②

（2） 行動規範の策定

- 実効性ある同意の取得が困難であることを踏まえ、データの取扱いに関する行動規範（Code of Conduct）等の策定が必要。
- 行動規範の策定に当たっては、分野ごとの専門的なプライバシーリスクの評価と対応が求められるため、法令等の枠組みでは対応が困難。法令等を補完する仕組みとして民間の自主規制ルールを活用していくべき。
- 諸外国においてもプライバシー保護の取組として行動規範等のルール策定を推進。我が国においても改正法による「個人情報保護指針」の活用の促進、あるいは、民間の自主ルール作成を支援する施策を推進すべきではないか。
- 改正個人情報保護法は個人が主体的に提供した情報を仮定しているのではないか。IoTによるデータ取得については、取得するデータの特性等を踏まえたガイドラインなどで補完することが望まれる。
- IoTの進展によってプライバシーの部分に穴があいてくるという事態が考えられる。このような状況において、これまで個人情報保護に加え、通信の秘密についても既述してきた電気通信事業分野のガイドラインにおいて、さらにプライバシーの観点から議論するということは、時宜を得ているのではないか。（再掲）
- 同意に関する議論は、米国でも、とりわけ行動経済学の知見で「ナッジ」の議論がなされており、そのような手法でどこまでカバーできるのかということは考える必要があるのではないか。
- 事前の完全性を確保することは無理。そのことを前提として補完する仕組みとして、常時の制御可能性について検討することが必要なのではないか。米国の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においても、通知と同意を中心とした規制から行為規制、情報へのアクセス拡充に移行する傾向。
- これまで個人情報やプライバシー保護に関わってこなかった事業者もIoTでは関わってくることになり、知らない間にプライバシー侵害を引き起こすリスクがある。政府や業界団体による啓蒙活動が重要。
- ルール策定に当たっては、プライバシー保護の基本に立ち返って、OECD８原則やISO/IEC29100プライバシーフレームワークを活用して、バランスよく取り組むことが必要。

主な意見③

（3） 本人によるデータ管理の仕組み

- IoTにおいて「同意と選択」を確保することは非常に難しく、結局は権限委譲やトラストに至る問題ではないか。権限委譲の仕組みとしてパーソナルエージェントが個人情報の可否等を判断する仕組みが考えられるが、高度な判断が求められる。
- 権限委譲等の仕組みとして、例えば、スマートフォンに自らの情報が集約されて、そこで判断するかたちが考えられるのではないか。
- IoTで取得されたデータに関して、本人がアクセスしたり訂正することができない場合や難しい場合があり、対処について検討することが必要。
- データトレーサビリティの確保、具体的にはデータ流通の透明化及び本人によるデータコントロール実現は有効な方策。また、これらの方策を進めるための技術開発の推進も必要。
- データの取得、流通、廃棄に至る「データのライフサイクル」に対して、本人がいつでも簡単に閲覧し操作できる仕組みが必要。例えば、①各事業者のパーソナルデータを一カ所で直接操作するポータル、②パーソナルデータを操作する各事業者の保有する各事業者のインフォメーションポータルへ誘導するポータルといった方法が考えられる。
- IoT特有のプライバシー上の課題を踏まえると、本人の同意を取得するという基本原則の下、本人がパーソナルデータ提供のためのポリシー管理を行い、利用者自らがデータの提供をコントロールできる機能を持つ仕組みであるPPM（プライバシーポリシーマネージャー）は有効な方策なのではないか。
- PPMにおいては、①ユーザ支援機能：プライバシーポリシーの設定の簡素化、サービス規約の表示の最適化等による有効な同意の取得、②可視化機能：パーソナルデータの利用状況を見える化、削除機能の提供等を行う。
- PPMといった取組が普及することは有益。今の段階ではなかなか難しいだろうが、将来的には同意取得のところは自動化していくという方向がよいのではないか。
- PPMのような取組について、どうすれば普及していくのか、利用者が使うのかといた点がポイントになってくるのではないか。

主な意見④

（4） プライバシー保護技術の活用

- IoT機器から得られるデータの保護については、①機器レベルの保護、②データレベルの保護、③加工プロセスの保護、④加工データの保護といった類型に分けて考えることができる。
- 他者に必要以上のデータを開示しないようにする匿名認証や、IoT機器から得られるデータを暗号化し、そのデータに開示制御機構（特定の日付以降に特定の者にのみ開示する等）を埋め込む技術、IoT機器がデータをプライバシー保護が守られた形式に加工する技術、④暗号（秘密計算）で加工プロセスを保護するといった技術の活用は有効と考えられる。
- IoTのデバイスは高性能なネットワークやプロセッサーが使えないので、現時点において高度なセキュリティ技術をIoTに導入することは容易ではない。セキュリティに関しては、閉じたネットワークと接続するか、外部ネットワークとつながるゲートウェイに集約するなど、IoT機器のセキュリティに頼らない構成が必要。
- 個人との帰属を切って匿名化した状態で収集することもデータ最小化の手法とみなすことができ、今後、検討の視点として取り入れていくべき。

取りまとめの方向性（案）①

（1）マルチステークホルダープロセス（MSP）の活用

- IoTにおける多様な関係者間におけるルール策定に当たり、マルチステークホルダープロセス（MSP）は有効な手法。改正個人情報保護法においてもMSPの活用を想定しており、今後、同プロセスを積極的に活用して行動規範等のルール作りに策定に取り組むべきではないか。
- ルール策定の初期段階においては、官民が連携しつつ、必要な場合には国がリードする等の積極的な関与を行うことも必要なのではないか。
- MSPの実施に当たっては、ゴールの明確化、オープン性の確保、行政機関の関与、参加者の代表性の確保、執行性の確保等が重要なポイントになると考えられ、そのために必要となる環境整備を進めることが必要ではないか。
- 電気通信分野においては、位置情報やスマートフォン上のアプリをユースケースとして、MSPを活用して行動規範等のルール策定の取組を進めるべきではないか。

（2）行動規範等の策定

- IoTにおいて事前の説明や同意取得には限界があるとの認識の下、プライバシー保護を図りつつデータの利活用を促進するための行動規範等の策定が必要となるのではないか。
- 行動規範等は、法令や政府の関係ガイドライン等を踏まえつつ、それらを補完するものとして、策定・活用していくことが有効と考えられる。具体的には、改正個人情報保護法における認定個人情報保護団体の個人情報保護指針や業界のガイドラインの策定・活用等の取組を進めるべきではないか。
- 電気通信分野においては、これまで一定の取組が進められている位置情報やスマートフォン上のアプリをユースケースとして、官民が連携して更なる行動規範等の策定の取組を進めるべきではないか。

取りまとめの方向性（案）②

（3）本人によるデータ管理の仕組み

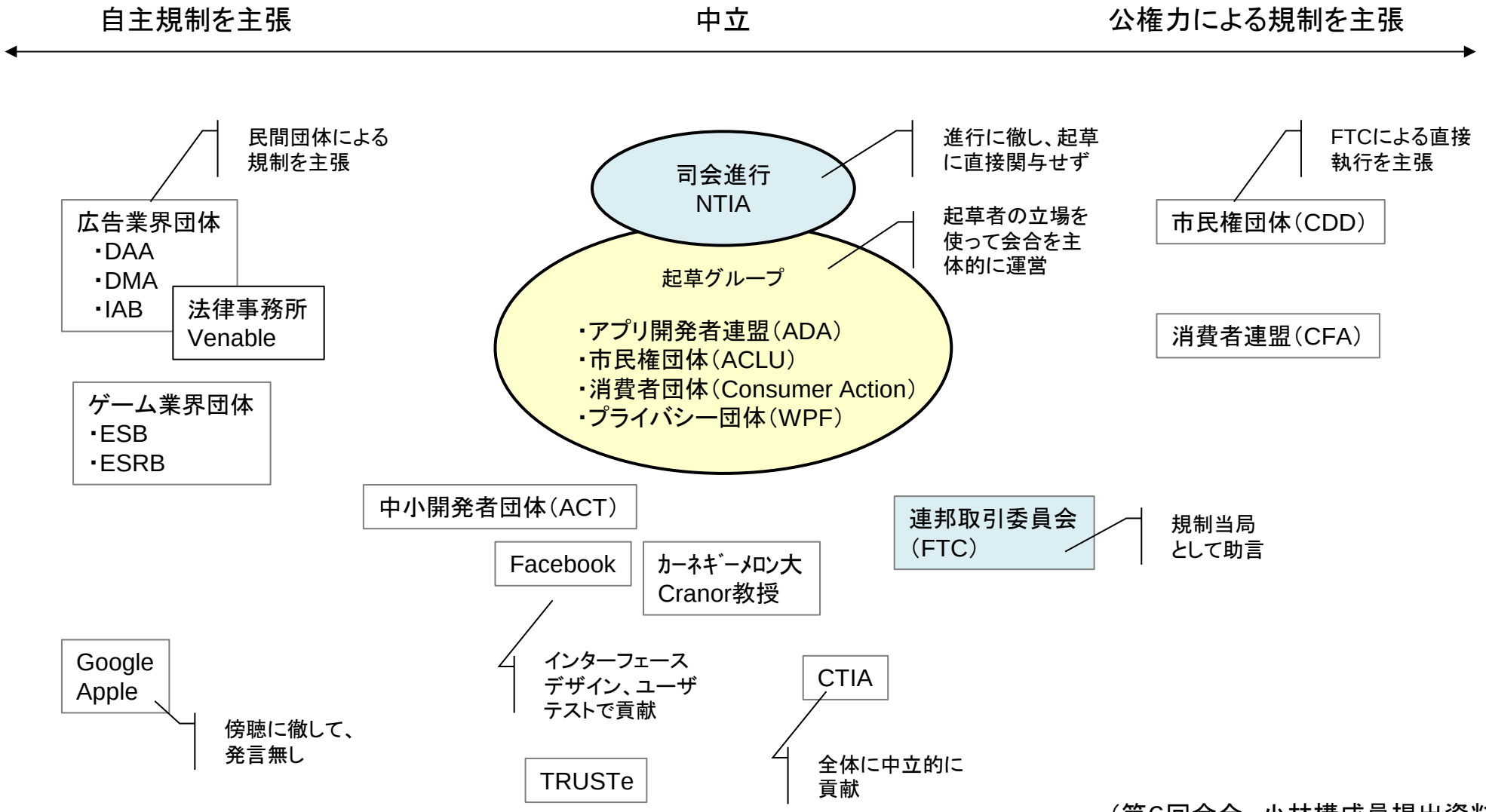
- IoTにおける実効性のある透明性の確保及び本人関与（同意取得等）の課題に対応するため、本人が自らのパーソナルデータを適切に管理できる仕組みは有効な解決方策になり得るものと考えられるのではないか。
- 現在、国内外において様々な試みが進められている（例：米国のSmart Disclosure、プライバシーポリシーマネージャー（PPM）等）。
- 今後、このような仕組みが備えるべき諸機能（プライバシーポリシー等の簡素化・最適化による有効な同意取得の実現、開示に基づくデータ利用状況の見える化等）を抽出・整理し、必要な取組を進めるとともに、その社会実装に向けた諸課題等についても検討・検証を進めるべきではないか。

（4）プライバシー保護技術の活用

- IoTにおけるデバイスやネットワークを踏まえ、プライバシー保護に有効な技術について、国内外における動向をフォローし、必要な取組を進めるべきではないか。

（参考1）米国におけるマルチステークスホルダープロセスの例

モバイルアプリの通知に関する行動規範のマルチステークホルダープロセス参加者の関係



（第6回会合　小林構成員提出資料）

（参考）「ナッジ（nudge）」について

概要

- 「ナッジ（nudge）」とは、行動科学や行動経済学などの分野において、人々がよりよい行動を選ぶよう促すことを表す用語として使われている。
- 選択肢が多すぎる場合やその内容が複雑な場合等において、本人の利益になる選択を促す仕組みや仕掛けとしての「ナッジ」を活用することの有効性が注目されている。

※「ナッジ（nudge）」とは、本来、「ヒジで軽く突く」という意味を持つ。

諸外国の動向

- OECDによれば、政府や規制機関によるナッジの利用は英国や米国を中心に、世界的に拡大しているとされている。

※OECDは、2015年1月に” Behavioral Insights and New Approaches to Policy Design”と題するセミナーを開催。150以上の政府機関、規制機関、有識者、関係団体等が参加。

- 英国では、2010年に、政府組織として「ナッジ・ユニット（Behavioral Insights Team）」を設立。選択の仕組みにナッジを組み込んで国民によりよい行動を促すとともに、コスト効率良く政策効果を高める試みが進められてきた。
- 米国では、2014年に、国際科学技術会議の下に専門組織として「社会及び行動科学チーム（Social and Behavioral Sciences Team）」を設置。同会議の報告書においては、社会保障、教育、健康、環境等の幅広い政策分野において、情報提供方法の改善や望ましい選択肢の優先表示、手続きの容易化等を通じ、政策効果を高めた事例等が紹介されている。

オバマ大統領は、上記の取組等を踏まえ、2015年9月、国民へのより良いサービスのために行動科学の知見を生かすことを求める大統領令を発出。

※The White House “Executive Order”– Using Behavioral Science Insights to Better Serve the American People

（大和総研公表資料「IoT社会に広がるナッジ」等に基づいて事務局作成）

（参考3）諸外国の動向①　-事例（アメリカ）-

Smart Disclosure

- 連邦政府により、政府機関や企業が保有するデータをコンピュータが読み取り可能な電子形式でユーザーに提供しようとする取組が進められている。
- 提供されたデータを基にして、消費者がサービス等を選択する際の意思決定に役立つ、新しいサービスの開発を企業に促すことを企図。

Green Button　Initiative

- Green Button Initiativeは、Smart Disclosureの取組の一例であり、エネルギー会社が電気利用データを利用したい第三者に対して提供をする仕組み。
- エネルギー会社は、利用者の同意を得ることで第三者に電力利用データを提供することができ、当該第三者は当該データを利用したサービスを利用者に対して提供。
- 利用者は、エネルギー会社からデータをダウンロードすることも可能。

Green Button Connect My Data

〇Smart Disclosureで提供されているデータ、ツール

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	Ⅱ ・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） ・College Navigator（教育） ・What's in the Food You Eat（食品） ・Healthcare.gov（医療）	Ⅰ ・Blue Button（医療） ・MyData（教育） ・my Social Security（社会保険）
非政府分野	Ⅲ ・Billshrink.com（携帯電話） ・Hello Wallet（金融）	・Green Button（電力） ・Mint.com（金融） Ⅳ

データ開示イニシアティブ　データ利活用ツール

（第4回会合　株式会社オプト寺田氏提出資料）
（原典：国際社会経済研究所）

諸外国の動向②　-IoTとプライバシーに係る検討-

■ 下記のとおり、IoTとプライバシーに係る検討が行われている。各成果文書では、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た上で、消費者の同意を得ることなくデータが取得されてしまう事態が起き得ると指摘し、そのような行為への対応方法の検討を求めている。

発行年	発行主体	タイトル	概要等
2014年9月	**EU** 29条作業部会	• Opinion 8/2014 on the on Recent Developments on the Internet of Things	• 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。
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**	• Internet of Thingsに関するモーリシャス宣言	• 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	• Internet of Things – Privacy and Security in a Connected World （FTC Staff Report）	• 2013年11月に、IoTに係るプライバシーやセキュリティに関する課題についてのシンポジウムを開催。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議論。 • 同シンポジウムを受けて、2015年１月にスタッフレポートを発行。 • スタッフレポートでは、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。

諸外国の動向③　-事例（自動車関係）-

フランス

- **高級車のリースをしている事業者が、利用者からの十分な同意を得ずに、自動車の位置情報等を収集していたとしてCNILから制裁（5,000ユーロの罰金）を受けた事案がある。**

【事案の概要】

- CNILへの届出なしにリースを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。

ドイツ

- **自動車会社が、販売した自動車に係る情報を必要以上に取得していたことが問題化している。**

【事案の概要】

– 2015年11月に、国際自動車クラブ連盟とドイツ自動車クラブによる調査により、ある自動車会社の特定車種において、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。

※　取得されていたデータ：運転情報、車両位置、メンテナンス情報、同期された携帯電話の個人情報　等

– 車両の購入契約書にデータ転送に関する項目が設けられ、車両購入に際し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契約となっていた。

- **2016年１月には、連邦及び各州のデータ保護専門官と自動車産業連盟がコネクティッドカーに関して共同声明を発表。**

※　①データの個人性、②データ取得及びデータ加工の妥当性、③データの開示、④データの権限等について、データ保護法に関連する諸点に特別に留意することを合意

（参考4）プライバシーポリシーマネージャー（PPM）について

ＰＰＭの主な機能

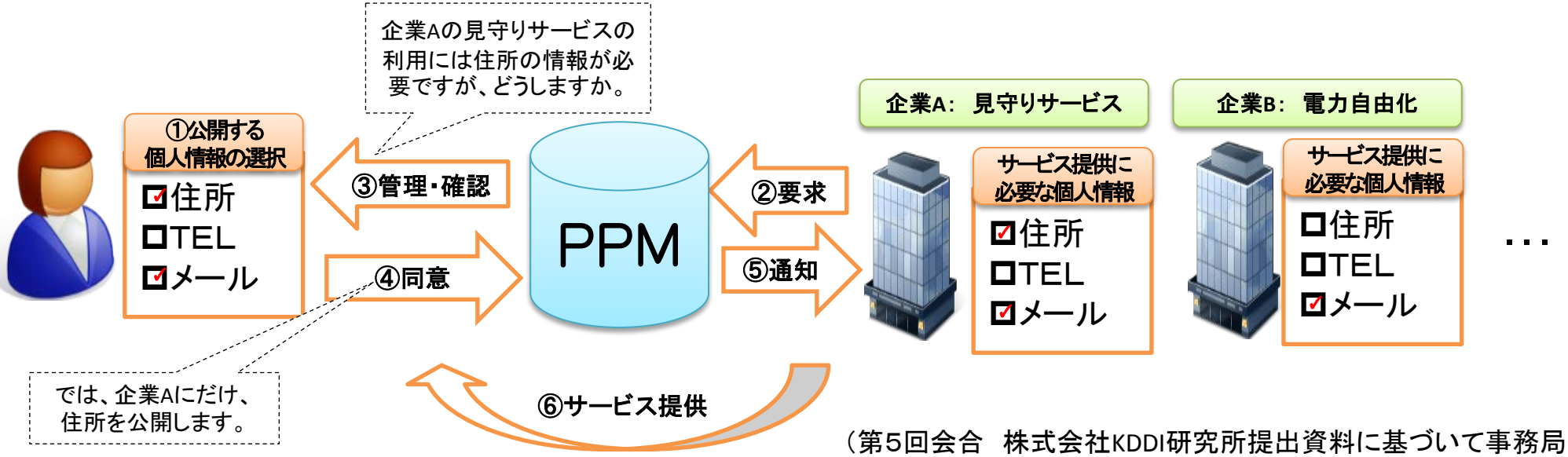
- 利用規約のわかりやすい表示
- 同意取得を代行
- データ提供履歴を「見える化」
- データ取得事業者に削除依頼

わかりやすい表示

※簡略で一覧性のある表示も可能

データ提供履歴

※サービス名で履歴の検索が可能



（第5回会合　株式会社KDDI研究所提出資料に基づいて事務局作成）

「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」構成員等

○構成員（敬称略・五十音順）

東　博暢	株式会社日本総合研究所 リサーチ・コンサルティング部門 上席主任研究員/融合戦略グループ長
石井　夏生利	筑波大学図書館情報メディア系准教授
板倉　陽一郎	弁護士
小林　慎太郎	株式会社野村総合研究所 上級コンサルタント
佐藤　一郎	国立情報学研究所教授/所長補佐
宍戸　常寿（主査代理）	東京大学大学院 法学政治学研究科教授
新保　史生	慶應義塾大学総合政策学部教授
高崎　晴夫	KDDI総研取締役
高橋　克巳	NTTセキュアプラットフォーム研究所 主席研究員
田中　里沙	事業構想大学院大学学長/ 宣伝会議取締役メディア・情報統括
長田　三紀	全国地域婦人団体連絡協議会 事務局長
新美　育文（主査）	明治大学法学部教授
森　亮二	弁護士

○オブサーバ

（一社）電気通信事業者協会

（一社）テレコムサービス協会

（一社）日本インターネットプロバイダー協会

（一社）日本ケーブルテレビ連盟

（一財）日本データ通信協会

（一社）情報通信ネットワーク産業協会

個人情報保護委員会事務局

消費者庁消費者制度課

経済産業省商務情報政策局情報経済課

タスクフォースでの検討経過

	開催日	主な議題
第1回	平成27年 11月5日	○ 改正個人情報保護法を踏まえた「電気通信事業における個人情報保護に関するガイドライン」に係る検討等について ○ 構成員等からの報告 ・「プライバシー保護に係る最近の動向」（小林構成員） ・「コネクテッドカーにおけるプライバシー保護について」（株式会社KDDI総研 平林氏）
第2回	12月18日	○ 事業者団体へのアンケート結果について ○ 位置情報に関するプライバシーの適切な保護と社会的利用の両立に向けた調査研究について ○ 構成員等からの報告 ・「匿名加工情報の利活用に向けて」（ニフティ株式会社） ○ 電気通信事業分野ガイドラインに係る検討等について
第3回	平成28年 1月25日	○ 個人情報等の取り扱いに係る電気通信事業者からのヒアリング（非公開）
第4回	4月6日	○ 本タスクフォースの今後の進め方について ○ 構成員等からの報告（IoTの進展等を踏まえたプライバシー保護） ・「IoTが生み出すパーソナルデータの利活用と保護」（佐藤構成員） ・「IoTプライバシーの技術的考察」（高橋構成員） ・「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」（株式会社オプト 寺田氏）
第5回	4月21日	○ タスクフォースの主な検討事項等について ○ ゲストスピーカーからの報告 ・「プライバシーポリシーマネージャーについて」（株式会社KDDI研究所） ○「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調査研究」の結果について
第6回	5月12日	○「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調査研究」の結果について ○ 構成員等からの報告 ・「スマートフォンアプリに係るプライバシー保護について」（東構成員） ・「諸外国におけるパーソナルデータ流通のための自主規制ルールづくりの動向」（小林構成員） ・「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」（株式会社三菱総合研究所）
第7回	6月８日	○ 構成員からの報告 ・「IoTと改正個人情報保護法」（板倉構成員） ○ 議論の取りまとめの方向性（案）について