資料５

本タスクフォースにおける検討の視点（案） IoT関連部分
（第5回会合資料からの再掲）

平成２８年５月１２日
事　　務　　局

本タスクフォースにおける検討の視点（案）　IoT関連部分

主な検討事項

IoTの進展を背景に、今後、多様な端末やサービス間での大量のパーソナルデータの取得・流通・活用が想定されるが、パーソナルデータの適切な保護を図りながらデータの自由な流通を推進するという観点から、本TFでは、以下の事項について、最新の動向を把握しつつ、課題の抽出・整理及び対応方策の方向性について議論を行う。

- **IoTにより収集されるデータにはどのような特性があるか。**

【主な御意見等】

- パーソナルデータは「主体的提供データ」、「観測データ」、「推定データ」に分類できるが、IoTと特に関わってくるのは「観測データ」。また、ビッグデータの世界においては、プロファイリングによる「推定データ」も問題となる。IoTによって収集される情報の一部は、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」（個人を特定しないが、一人の個人を区別できる情報）に含まれるのではないか。（佐藤構成員）
- 「（仮称）準個人情報」に関しては、総務省の「パーソナルデータの利用・流通に関する研究会」においても「実質的個人識別性」としてかつて議論された。このような情報のプライバシーリスクが高いのであれば、電気通信事業分野ガイドラインによって上乗せ的な行為規範を自主的に遵守してもらう、共同規制で遵守してもらうといった枠組みも検討すべきではないか。（宍戸構成員）
- IoTでは 現実世界の空間的位置と時刻が名寄せの起点となり易く、ネット上のサービスと比較して複数の情報の突き合わせにより、照合が容易になってしまう（現実世界が名寄せの起点になりやすい）。（佐藤構成員）
- 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、単なるデータであっても、解釈することで人の行動履歴となるデータがある。また、IoT機器と「個」との関係は単純ではない。（高橋構成員）

本タスクフォースにおける検討の視点（案）　IoT関連部分

● パーソナルデータやその利用目的の多様化・複雑化等に伴い、利用者に対する説明・同意取得がますます重要になると考えられるが、**利用者に信頼されるプライバシーポリシーや同意取得のあり方**についてどのように考えるべきか。そもそも有効な同意取得が困難になる場合もあるのではないか。**プライバシーバイデザインによる対応**も考えられるか。また、**利用者が自らのパーソナルデータを管理**するという視点からは、どのような方策が考えられるか。

【主な御意見等】

- 情報の取得についてどう知らせるか、どう同意をとるかを決めるべきだが、技術的にも難しい課題。（佐藤構成員）
- 「同意と選択」を確保することはIoTにおいては非常に難しく、権限委譲やトラストに至る問題ではないか。権限委譲としては、例えば、パーソナルエージェントが個人情報の提供の可否等を判断する仕組みが考えられるが、パーソナルエージェントにおいて非常に高度な判断が求められる。（高橋構成員）
- 権限委譲やトラストの具体的な形として、例えば、スマートフォンに自らの情報が集約されて、そこで判断をする形が考えられるか。（森構成員）
- どの局面での同意、説明なのか詰める必要がある。教育により情報提供を行うシステムも考えられ、しっかりとした情報提供を前提に、例えば、「この機器を買ったら同意があったと見なす」という構成もあり得るのではないか。（新美主査）
- IoTにおいては、実効性ある透明化、同意取得は困難。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。また、「事前の完全性」よりも「常時の制御可能性」を実現すべきで、自らのデータを閲覧し操作できる仕組みが必要ではないか。（オプト寺田氏）

● プライバシー保護のためには**データの最小化も有用と考えられるが、これについてどう考えるか。**

【主な御意見等】

- 「目的の限定とデータ最小化」は、研究開発において目的を限定することは難しく、限定されたとしても、分かり易い言葉で表現することが難しい。また、データを限定取得することに技術的な困難もある。（高橋構成員）
- ISO/IEC 29100が示す原則は、データ最小化も含んでおり、今後の検討の参考となる。データ最小化の手法として、個人との帰属を切った状態で、匿名化した状態で取得する手法もある。（小林構成員）

本タスクフォースにおける検討の視点（案）　IoT関連部分

● 今後、パーソナルデータの取扱いについてより多くの事業者が関与することになるが、**情報の帰属（誰の情報をどのような権限で誰が管理するのか）と責任分界（どこまでが誰の責任か）**について、どのように考えるべきか。

- **利用者も含めた関係者間のルール**をどのように確立すべきか。例えば、個別分野ごとに、関係者が集うマルチステークホルダープロセスを活用することが有効であり、ニーズが高い分野について速やかに取り組むべきなのではないか。

【主な御意見等】

- 情報の帰属は本質的な問題。IoTにおいては、データの本人と、そのデータを利用する者の二者にとどまらず、多くのステークホルダーが存在し、その調整が重要。（佐藤構成員）
- ステークホルダーが多数いて特定困難な場合、行政分野では、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、民間でできるだけ問題を解決するという流れの中にあるが、ステークホルダーが見つからない場合であれば、マルチステークホルダープロセス自体に政府が1ファクターとして関与していく局面も考えられるのではないか。（宍戸構成員）

- **個人情報が収集され、流通される基盤の信頼性**について、何らかの担保措置が必要ではないか。

【主な御意見等】

- IoTにおいては、実効性ある透明化、同意取得は困難。これを認識した上で、信頼できる事業者の認定や、信頼できる事業者同士による連携促進といったトラストフレームワークの構築が必要ではないか。（オプト寺田氏）
- トラストフレームワークが多数出現すると、トラストフレームワークの間での連携が課題になる。（佐藤構成員）

● 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。**

【主な御意見等】

- 技術の進歩を丁寧に見るべき。例えば次世代GPSが登場すると、高精度測位により位置情報が人を識別する手段となる。ここ数年よりもはるかに速い技術進展も想定すべきで、技術の開発段階から制度を含めた検討が必要。（佐藤構成員）
- 「IoT機器の保護」と「IoT機器から得られるデータの保護」のいずれも必要。「IoTから得られるデータの保護」については、データプライバシー原則のうち、「同意と選択」、「目的の限定とデータ最小化」、「開示の制限・利用の制限」に当てはめて考えることができる。（高橋構成員）

- 例えば、「開示の制限・利用の制限」の課題解決のための技術として、他社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）を埋め込む技術が有用と考えられる。（高橋構成員）
- 高度なセキュリティー技術は、IoTに導入することが容易でないため、プライバシーに関わる情報は、外部ネットワークに繋がるIoTのエッジ側のデバイスに置くべきではない。セキュリティに関しても、閉じたネットワークと接続するか、外部ネットワークと繋がるゲートウェイに集約するなど、IoTデバイスのセキュリティに頼らない構成が求められる。（佐藤構成員）

● 公益性の高い目的のために有用に活用され得る情報もあると考えられるが、公益性とプライバシー保護のバランスについて、どのように考えるべきか。

● **諸外国ではどのような取組**が行われており、その成果と課題はどうなっているか。

【主な御意見等】

- 同意に関して、米国における行動経済学の知見を用いた「ナッジ」の議論が参考になるのではないか。（宍戸構成員）
- 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では、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が提案されている。（オプト寺田氏）

● **その他、検討すべき事項や視点**はあるか。

【主な御意見等】

- 通信の秘密は、社会活動の基盤としてコミュニケーションを可能にするために必要な保護であり、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る。他方で、プライバシーは、私生活の平穏が出発点。IoTの進展により、電気通信を通じてプライバシーに穴が空く事態が考えられ、改正個人情報保護法を踏まえ、通信の秘密についても記述してきた電気通信事業分野ガイドラインをプライバシー保護の観点から議論することは、時宜を得たもの。（宍戸構成員）
- クラウド化や仮想化により、設備、ネットワーク、プラットフォームの境界が曖昧になってきており、このような状況において通信役務とは何を指すのか考える必要があるのではないか。（オプト寺田氏）