IT-Report
2019 Winter

IT-REPORT

2019 Winter

Contents

JIPDEC
一般財団法人日本情報経済社会推進協会

今年度第２号となる「JIPDEC IT-Report 2019 Winter」は、「Society5.0実現を支えるデータの利活用」と題し、特集を組みました。

2016年１月22日に閣議決定された「2016年～2022年の第５期基本計画」において、サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する人間中心の社会、「Society5.0」の実現が提唱されました。

Society5.0で実現する社会とは、

- IoTの活用による人とモノのつながり、さまざまな知識や情報の共有化と、それに伴う新たな価値の創造
- 人工知能（AI）を活用したロボット、自動走行車等の技術の発展により、少子高齢化、地方の過疎化などの課題克服
- 社会の変革（イノベーション）を通じた世代を超えて互いに尊重し合える社会、一人ひとりが快適で活躍できる社会

と定義（内閣府ホームページ「Society 5.0」より）されており、すべての人とモノがIoTでつながり、AIを活用して個人が必要とするときに、必要な情報の提供を受けられる社会の実現を目指すことになります。

Society5.0実現のためには、AI解析に必要なビッグデータをいかに取捨選択し、さまざまな環境、立場、分野、業態、地域等において活用させられるか、そのために何をすべきか、どういう点に注意すべきか、を見極めなければなりません。ビッグデータの利活用により、ユーザは個人の視点にたった便利、かつきめ細やかなサービスの提供を受けられる一方で、サービス提供側は、たとえばカメラ画像や医療情報等を基とした個人データを利用した解析にあたっては、個人のプライバシーへの配慮、プライバシー侵害などのリスクについて十分配慮する必要があると考えます。

そこで、今回のIT-Reportは、「Society5.0実現を支えるデータの利活用」をテーマに、Society5.0のしくみと、政府が主導するデータ利活用のサービス例としてMaaSや活用上の問題点（データ・ダブル）を解説し、次章以降では、パーソナルデータをビジネスで取り扱う企業が取り組むべきプライバシー施策、AI倫理指針とプライバシー保護、パーソナルデータを使った新たな認証技術の具体例と今後の課題について、有識者の方に解説、紹介していただきました。

また、巻末には、資料として国内外の個人情報保護関連の年表と2019年４月から９月の情報化動向を掲載しています。

本誌をビジネスでビッグデータを活用する企業の方はもとより、個人の皆様にも参考としていただければ幸いです。

2019年12月
一般財団法人日本情報経済社会推進協会

JIPDEC IT-Report 2019 Winter

Contents

特 集

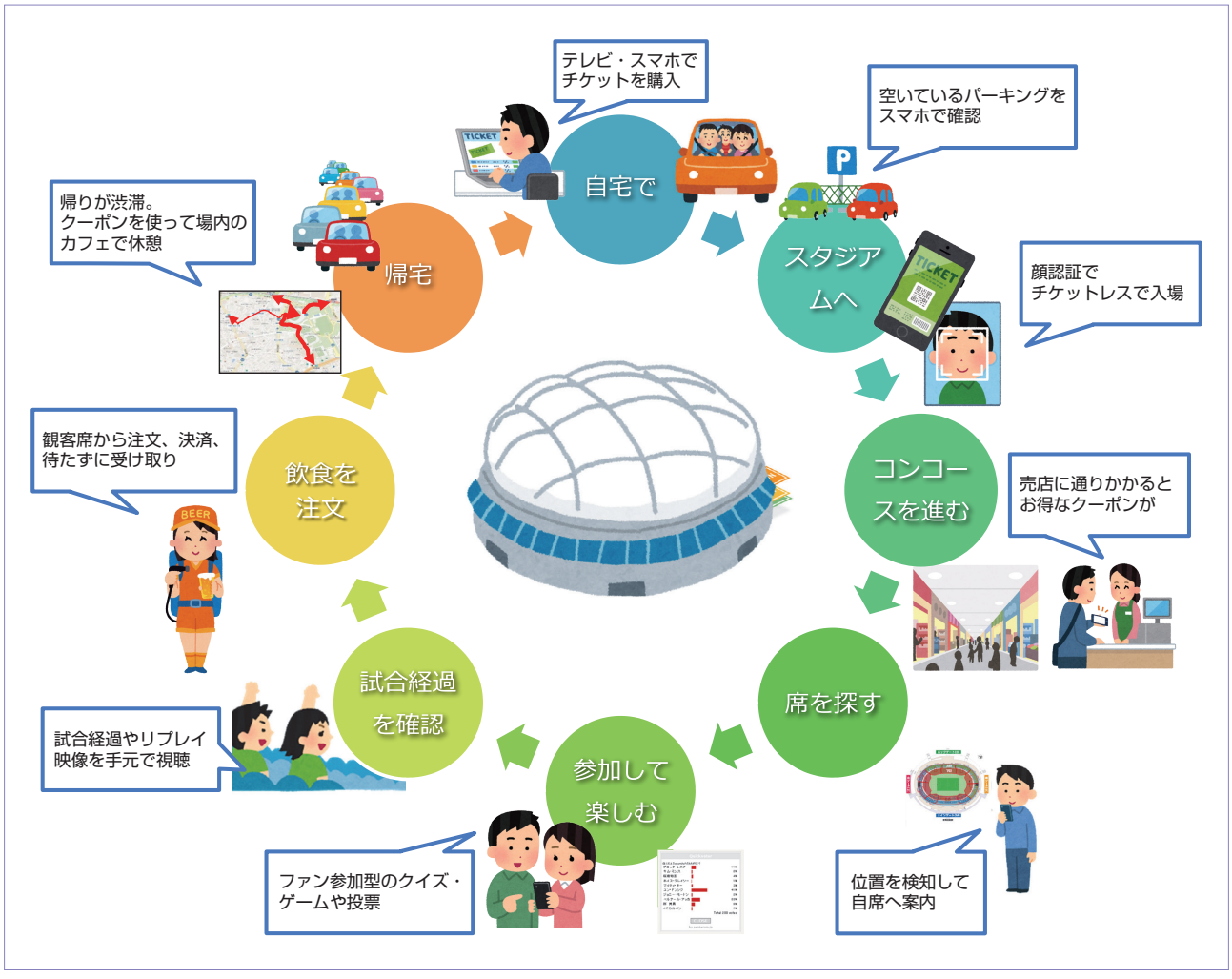
Society 5.0実現を支えるデータの利活用

Ⅰ Society 5.0実現を構成するデータ活用の将来見通し

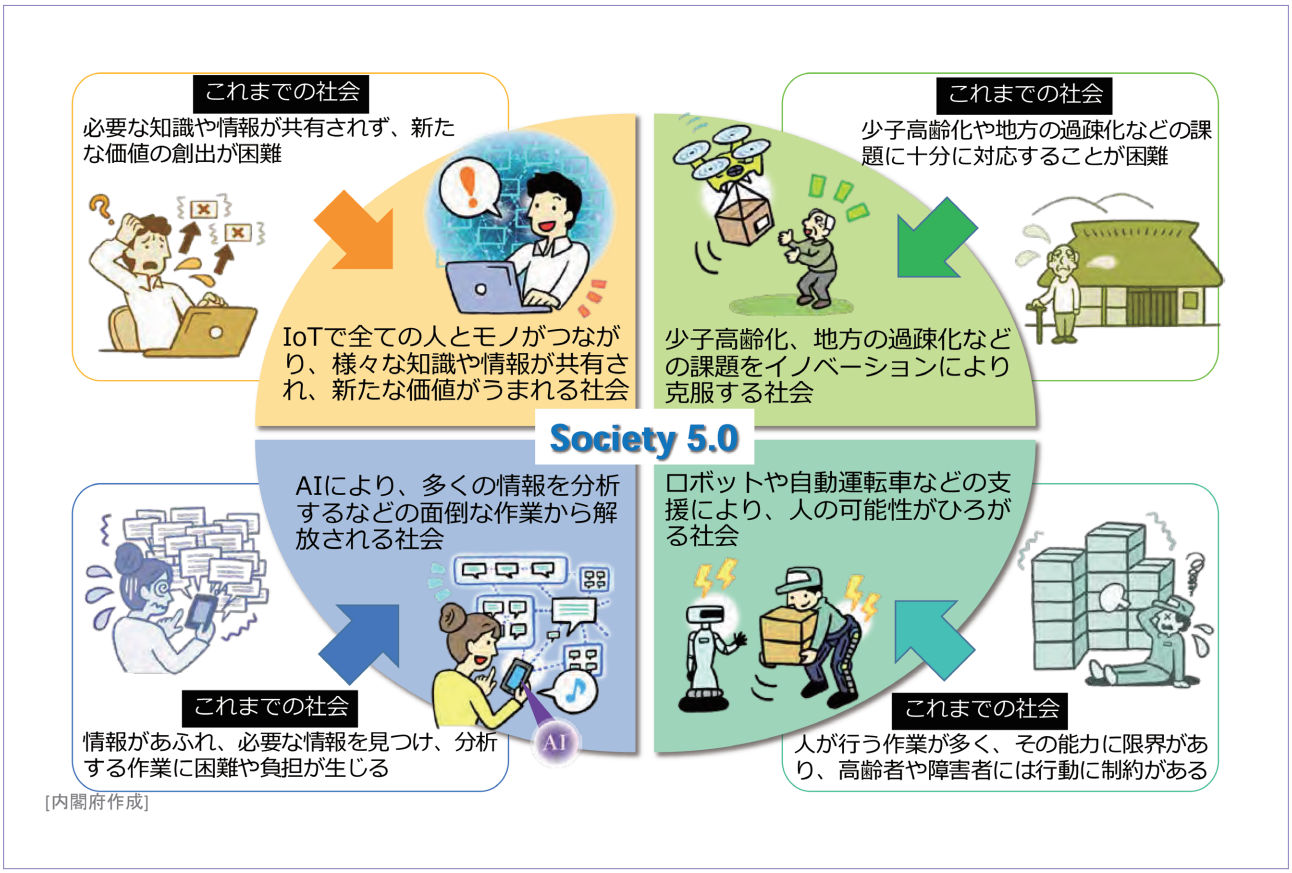
一般財団法人日本情報経済社会推進協会　電子情報利活用研究部　次長　**保木野 昌稔**

1．Society 5.0とは、どのような社会になっていくのか

インターネットの登場、スマートフォンの普及によって、生活の中であらゆるサービスがネットワークを通じて受けられるようになった。近年のIoT・AIの急速な発展により、これらの技術を活用したサービスが登場したことで、人はサービスを利用する時だけではなく、常時ネットワークに繋がった状態で生活するという変化が起きている。それは生活者が、自分の好みに合った最適なサービスを、必要とするタイミングで、享受できる社会といえる。そのような社会が今まさに実現しようとしている。（図表１-１）



図表１-１．実現しつつある社会のイメージ



図表 1 - 2．内閣府のSociety 5.0のイメージ

出典）内閣府ホームページ「Society5.0 のしくみ」（https://www8.cao.go.jp/cstp/society5_0/index.html）

政府が展望する日本の未来として、「Society 5.0」を提唱している。Society 5.0とは、「サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会課題の解決を両立する、人間中心の社会（Society）」[1]とされている。（図表 1 - 2 ）

政府の説明によると、以下のような社会の変化が起きるとされる。

> Society 5.0では、フィジカル空間のセンサーからの膨大な情報がサイバー空間に集積されます。サイバー空間では、このビッグデータを人工知能（AI）が解析し、その解析結果がフィジカル空間の人間に様々な形でフィードバックされます。今までの情報社会では、人間が情報を解析することで価値が生まれてきました。Society 5.0では、膨大なビッグデータを人間の能力を超えたAIが解析し、その結果がロボットなどを通して人間にフィードバックされることで、これまでには出来なかった新たな価値が産業や社会にもたらされることになります[2]。

言い換えると、「Society 5.0は、フィジカル空間をサイバー空間へコピーし、サイバー空間からフィジカル空間を制御する社会」となり、日本で深刻な課題となっている超高齢化・人口減少が進み、2030年には生産年齢人口が7,000万人を切ることが推計される中でも、持続発展ができる社会を創出することを目指している。（図表 1 - 3 ）

Society5.0へと向かう変化の一つに、デジタルツインがある。デジタルツインとは、フィジカル空間にある現実の機器や設備の稼働状況、環境情報などを、IoTを活用してリアルタイムで収集し、サイバー空間上で機器や設備をモデリングすることで再現し、フィジカル空間で起きている事象をモニタリングすることや現実に起こりうる事象をシミュレーションすることである。このような技術は、現場レベルで実際に活用が始まっている。

1，2　https://www8.cao.go.jp/cstp/society5_0/index.html

図表 1 - 3．フィジカル空間がサイバー空間上に投射されるイメージ

出典）内閣府ホームページ「Society5.0 のしくみ」（https://www8.cao.go.jp/cstp/society5_0/index.html）の一部を抽出・編集

現在では、製品開発やプラント監視など特定の対象についてこのような活用が行われているが、Society 5.0が実現される社会では、その対象が社会全体へと変化していく。社会全体を対象として活用が行われていくということは、当然のように個人についてもサイバー空間上に人物像が構築される。この人物像を対象に、パーソナライズされたサービスが開発され、個人ごとに提供されるようになる。

では、具体的にどのようなサービスがあるのか。現在、政府主導によりパーソナルデータを活用した実用化に向けた技術開発、実証実験が行われているものとして、マイカー以外の移動手段（MaaS）や、情報銀行が挙げられる。以下、これらのサービスの概要、プライバシー保護上の留意点、将来動向について紹介する。

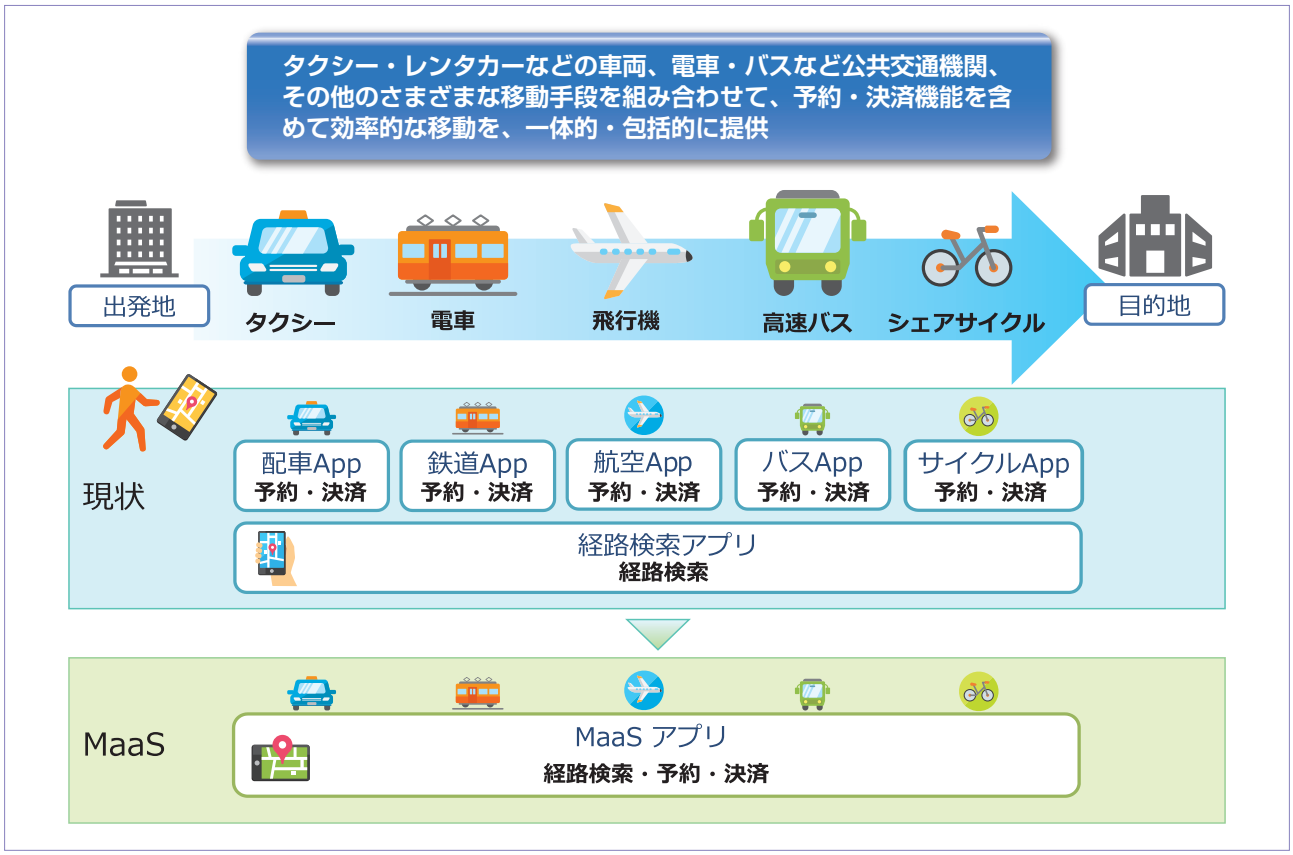
2．Society 5.0におけるMaaS（Mobility as a Service）

Society 5.0の実現に向けた政府の取組みの一つに、MaaSが取り上げられる。成長戦略実行計画には「MaaSの実現」が明記され、日本版MaaS推進の具体的取組みが進められているところである。

そもそもMaaSとは、ICTを活用することで、マイカー以外の電車やバスなどの公共交通機関、タクシーやレンタカーなどの車両、その他のさまざまな移動手段を、その運営主体にかかわらずシームレスに組み合わせてルート検索・予約・決済機能等を含めた効率的な移動サービスを提供する新しい概念である。（図表 1 - 4 ）

MaaSは、フィジカル空間での移動・輸送をサイバー空間上で再構築し、フィジカル空間の移動・輸送を制御するプラットフォームともいえる。サイバー空間上に蓄積された移動・輸送をはじめとするさまざまなデータを活用することで、モビリティサービスの調和と社会全体の最適化を図る可能性が期待されている。

現在、日本が抱えている超高齢化・人口減少の影響は、交通インフラに対しても大きくなっており、特に地方では、高齢化・過疎化が進み、移動手段を利用する人そのものが減っている。それによって、



図表 1 - 4．MaaSのしくみ

既存のバス路線などの収支がマイナスとなり、自治体が公共交通を維持できない状況となっている。また、地域の高齢化に伴い、バスやタクシーの運転手の高齢化や人員の減少もみられ、その結果、運行可能な車両も減少している。このような移動に関する社会課題の解決に期待されているのが、MaaSである。

交通事業者のほか、自動車メーカー、通信事業者、IT事業者等、幅広い業種の事業者がMaaS関連ビジネスに参入または参入意向を示している。

（1）国内で進む実証実験

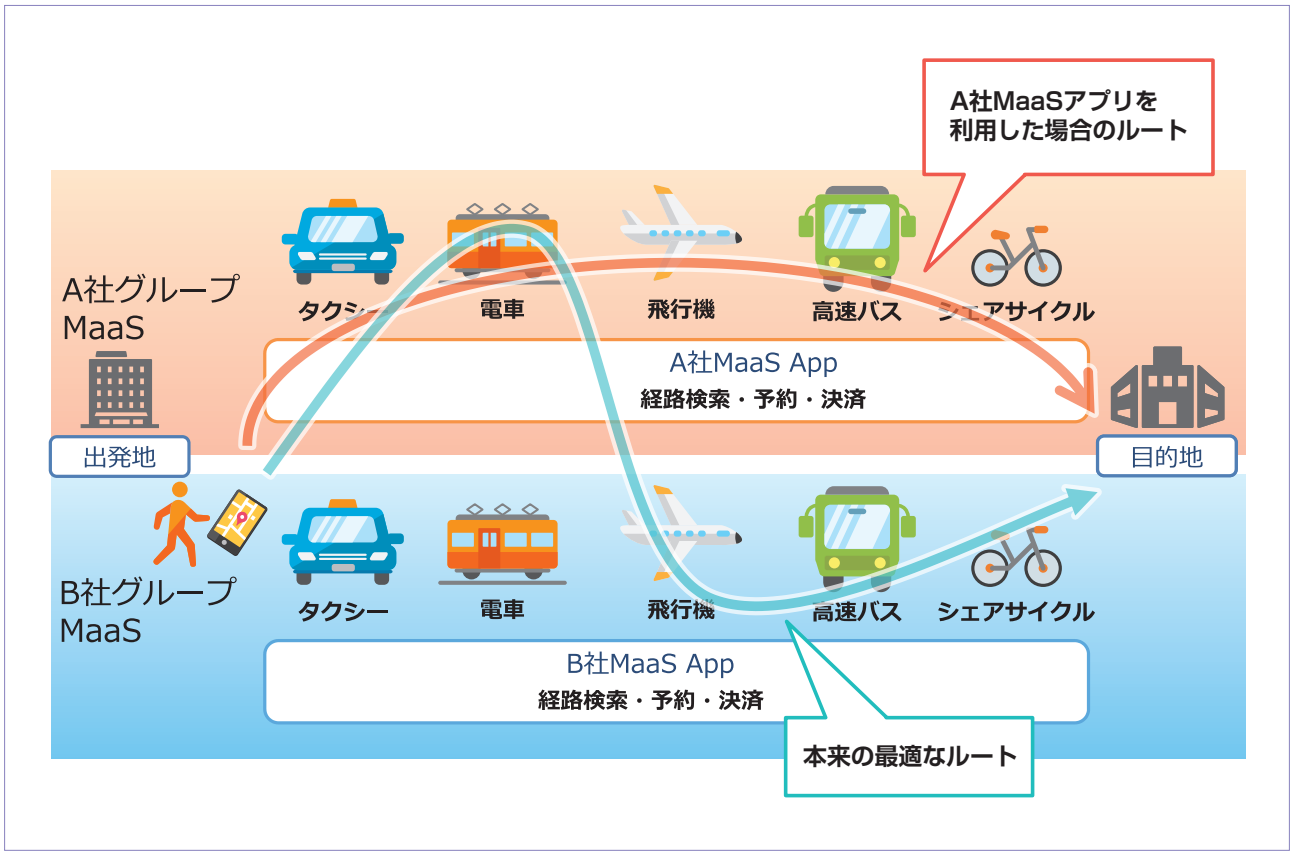
国土交通省では、日本版MaaSの実現に向けてモデル事業の実証実験[3]をスタートさせた。地域や観光地の移動手段の維持・充実や公共交通機関の維持・活性化のため、地域特性に応じたMaaSを全国に普及することが必要とされており、大都市近郊型・地方都市型、地方郊外・過疎地域型、観光地型の３つの類型について15のMaaS事業が対象となっている。

一方、民間においても鉄道事業者を中心として、各地で実証実験が行われている。

西日本鉄道（株）とトヨタ自動車（株）は、「人がもっと移動したくなる環境」を作ることを目的とし、福岡市および周辺地域においてMaaSの実証実験を行っている。実証実験では、マルチモーダルルート検索、予約・決済、お出かけ情報検索という「my route[4]」を提供し、2018年11月から2019年12月まで行われている。

東日本旅客鉄道（株）と東京急行電鉄（株）は、観光行動のシームレス化だけではなく、自治体等と連携した新しい交通手段の開発等により、少子高齢化や移動サービスの質的維持困難等の地域課題の解消に取り組むため、観光型MaaSの実証実験を2019年４月から６月、９月から11月の計６カ月間実施[5]した。伊豆エリアを対象に観光型MaaSアプリ

3　https://www.mlit.go.jp/report/press/sogo12_hh_000152.html
4　https://www.myroute.fun/
5　https://www.kantei.go.jp/jp/singi/keizaisaisei/miraitoshikaigi/sankankyougikai/mobility/dai3/sankou2.pdf



図表 1 - 5．MaaSが乱立してしまうことによる弊害

「Izuko」で、検索・予約・決済に加え、観光施設および宿泊施設の予約・決済を提供する。

小田急電鉄（株）は（株）ヴァル研究所と共同開発し、MaaSプラットフォームのためのオープンな共通データ基盤「MaaS Japan」を2019年５月に発表した。同年10月には、このMaaS Japanを活用したMaaSアプリの「EMoT[6]」を利用して、郊外（新百合ヶ丘エリア）および観光地（箱根エリア）における実証実験を開始した。EMoTでは、MaaSの基本機能である経路検索、予約、決済に加え、電子チケットサービスを提供する。

（２）MaaSによる移動のパーソナライズ化

日本の三大都市といわれる東京都区部、大阪市、名古屋市においては、交通網が毛細血管のように発達し、経路検索サービスと交通系ICカードが普及した現在において、移動について不便を感じることはないだろう。しかし、日本版MaaSの推進においては、前述のように交通事業者を中心にやや乱立気味に実装が進んでおり、このまま協調領域が整理されずに進んでしまうと、利用者にとっては悲しい結果を迎えてしまうことが危惧される。（図表１- ５）

たとえば、異なるグループのMaaSアプリが利用したいエリアで展開されていた場合、本来の最適なルートはグループを跨ぐ移動であったとしても、利用するMaaSアプリの提供するルートしか提案されない可能性がある。このような事態を起こさないために、国土交通省では、MaaS関連データ検討会[7]を開催し、協調領域・競争領域のデータ・APIについて検討している。MaaSの実装と共に、プラットフォーム間の連携に関するデータ・APIおよびルールが整備されることに期待したい。

一方、MaaSにおけるパーソナライズ化はより深

6　https://www.odakyu.jp/news/o5oaa1000001mstg-att/o5oaa1000001mstn.pdf
7　https://www.mlit.go.jp/report/press/sogo12_hh_000155.html

化していくことが予想される。MaaSアプリを常用することで、その人の移動履歴を中心としたさまざまな行動情報からMaaSプラットフォーム上にデジタルツイン（人物像）が作られ、その人が好んで使用する移動手段などの嗜好性が分析され、その人にとって心地よい移動ルートが提供される。さらに、MaaS×〇〇といった複合型のMaaSアプリが普及すれば、移動に関してだけではなく、観光、宿泊、飲食など生活のさまざまな側面を観測し、その人にとって最適なサービスが提供されるようになるだろう。

3．新たなプライバシー問題

フィジカル空間では、人は場面に応じて自然に、人物像を使い分けている。

- 行政における個人：行政手続きを受けるときなど
- パブリックにおける個人：ビジネスをしているときなど
- プライベートにおける個人：私生活を送るときなど

このように真の人物像は一つではあるが、場面に応じた人物像を使い分けて生活を行っている。（図表1-6）

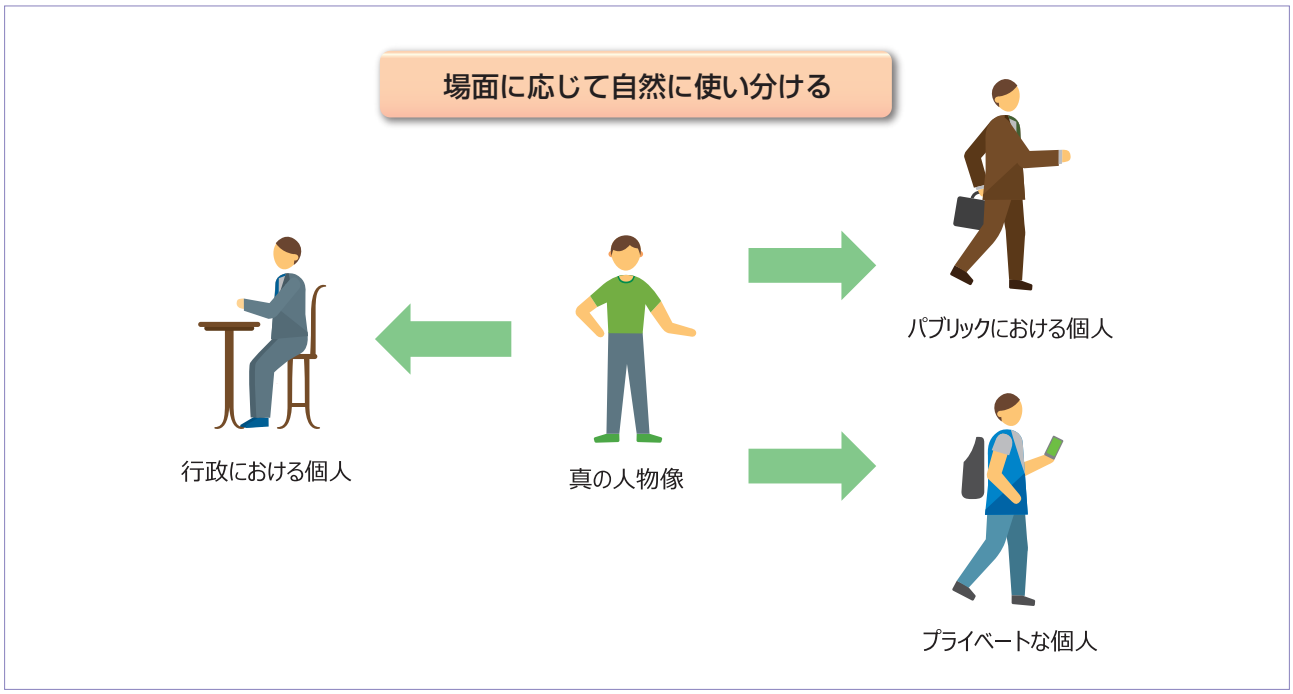
Society5.0より前の社会では、インターネットサービスの利用において、サービスごとに意図的にIDを使い分けるなどして、サイバー空間上の人物像の使い分けを行ってきた。

しかし、フィジカル空間とサイバー空間の融合が一層進むSociety 5.0においては、サイバー空間上のデジタルツインが本人の認知していないところで構築され、デジタルツインを基にしてサービスが提供されるようになっていくだろう。

個人情報が記録されたデータベースの中のデータによって、データ主体のもう一つの分身を作ってしまう人に対するデジタルツインのことをデータ・ダブルという。インターネット上のデータをもとに、本人が知らないところで作り上げられた個人の一定のイメージ像（データ・ダブル）を作ることで、この状況が本人にとってのプライバシー侵害となり得る。

データ・ダブルを利用すること自体には問題がないが、本人が全く関与することができない状態（データ・ダブルの状態）を回避するためには、本人による関与の機会を提供する必要があるのではないか。

また、前述のMaaSのようにさまざまなサービスを統合し、高度にパーソナライズされたサービスを提供することを可能にするプラットフォームでは、



図表1-6．人物像の使い分け

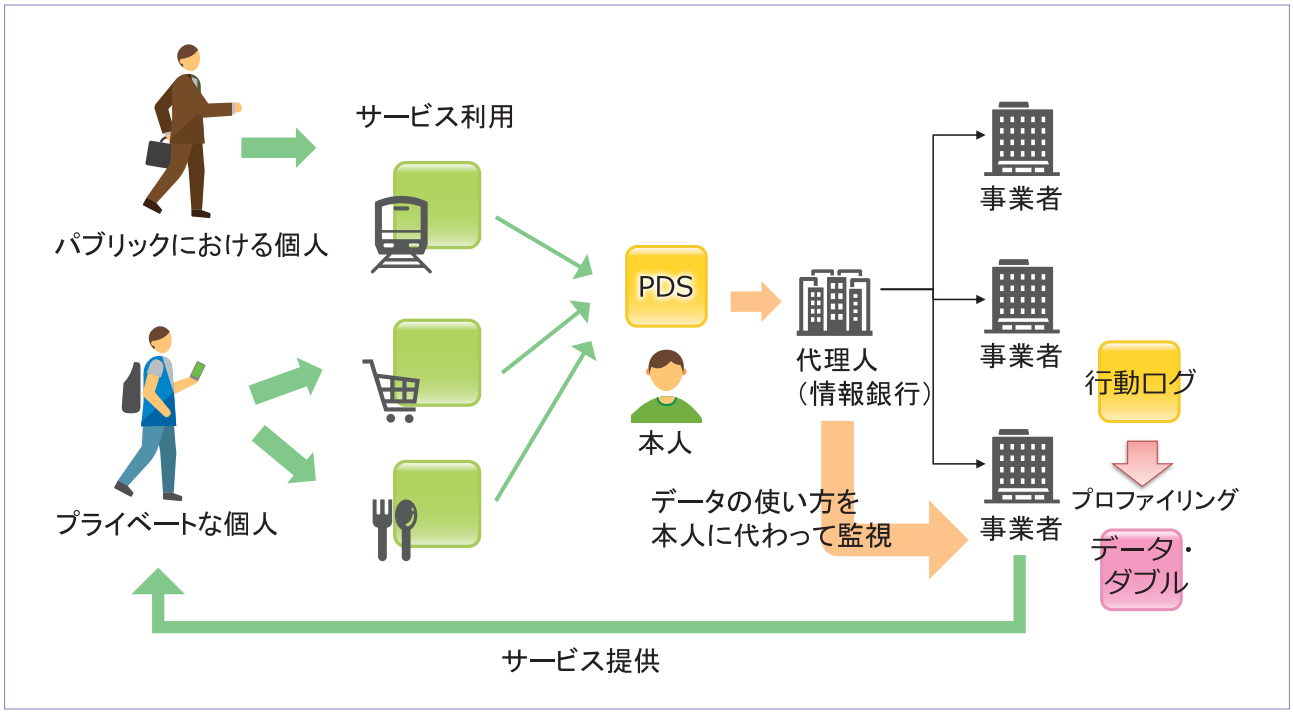
サービス提供に関係する事業者が膨大な数になり、個人からすると、自分に関するデータがどの事業者にどこまで利用されているのか把握できないという状況が生まれる。

こういったSociety 5.0における個人情報やプライバシーに係る問題の解決策として、サイバー空間上の代理人という考え方がある。サイバー空間上の代理人とは、オンライン上の各種手続き、サービスの利用（推薦）、セキュリティの確保、個人情報・プライバシー保護、事業者によるデータ利用への関与などを個人に代わって行う機能を提供するものである。このようなサイバー空間上の代理人としては、たとえば消費者からの信頼を得てパーソナルデータを取り扱う情報銀行等が考えられる。（図表１-７）

また、サイバー空間上の代理人には、本人による関与の機会を提供するという観点から、人物像の使い分けに関しても対応することがよいのではないか。MaaSを例にすると、MaaSアプリをビジネスで利用する際に、会社の規程に則った最短区間で安価なルートが提案され、プライベートでは、家族全員でゆったりとした移動が行えるような提案がなされるようなことが考えられる。これを、個人が主体的に選択できてもよいし、AIによる自動判定がなされてもよいが、その結果に不服がある場合には本人が関与できる仕組みを提供すべきではないか。（図表１-８）

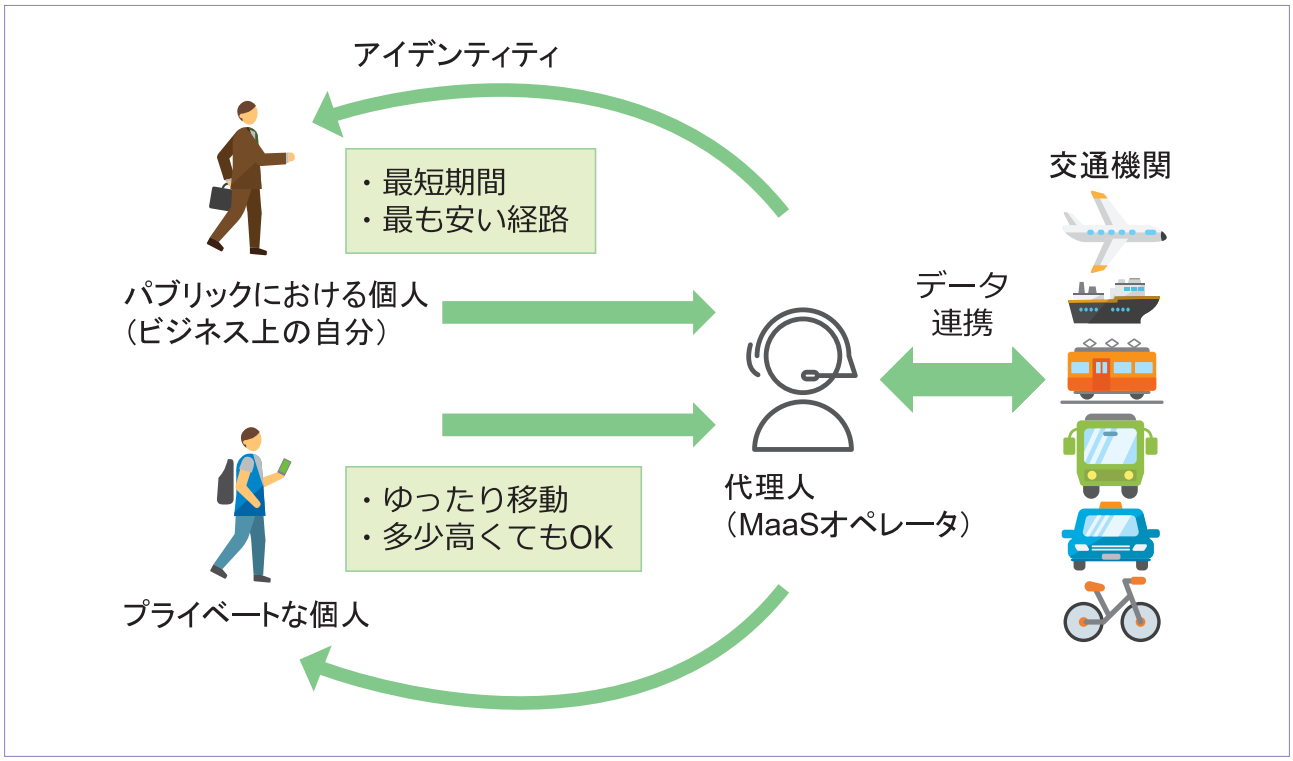
2019年10月には、「情報信託機能の認定に係る指針ver2.0」が総務省[8]・経済産業省[9]より公表されたが、この指針検討の中で「アイデンティティ（人物像）の使い分け」に関するようなテーマは含まれていない。

当協会電子情報利活用研究部は産官学との連携により「データ（情報）」の利活用と保護のための社会基盤整備に関する調査研究を行っており、情報銀行・PDS、ID連携トラストフレームワークに関する調査研究を通じて、Society 5.0が実現された社会において、個人情報・プライバシーが保護され、安心して生活できるデータ活用の基盤整備を推進している。



図表１-７．サイバー空間上の代理人（情報銀行）のイメージ

8　http://www.soumu.go.jp/menu_news/s-news/01tsushin01_02000290.html
9　https://www.meti.go.jp/press/2019/10/20191008003/20191008003.html



図表１-８．マルチな人物像を捉え適切なサービスを提供するイメージ

次章以降解説いただいている、Society5.0の実現を支えるデータ利活用の上で重視すべきプライバシー施策、AI解析上での留意点、パーソナルデータを使った新たな認証技術の具体例についても、関係各所と連携して検討を行っている。

デジタルツイン、アイデンティティ（人物像）の使い分けといった問題についても、今後、企業・有識者の方々と法制度の整備の側面と併せて、サイバー空間上の代理人、人物像の扱いについて検討し、提案していきたい。

（注）本章　脚注等掲載のURLは2019年12月現在のもの

Ⅱ 新たなプライバシー問題への対応に向けた企業のプライバシーガバナンスモデルの検討について

経済産業省　商務情報政策局　情報経済課　課長補佐　**関根 悠介**

1．Society5.0実現に向けたDXの推進とプライバシー問題の位置づけ

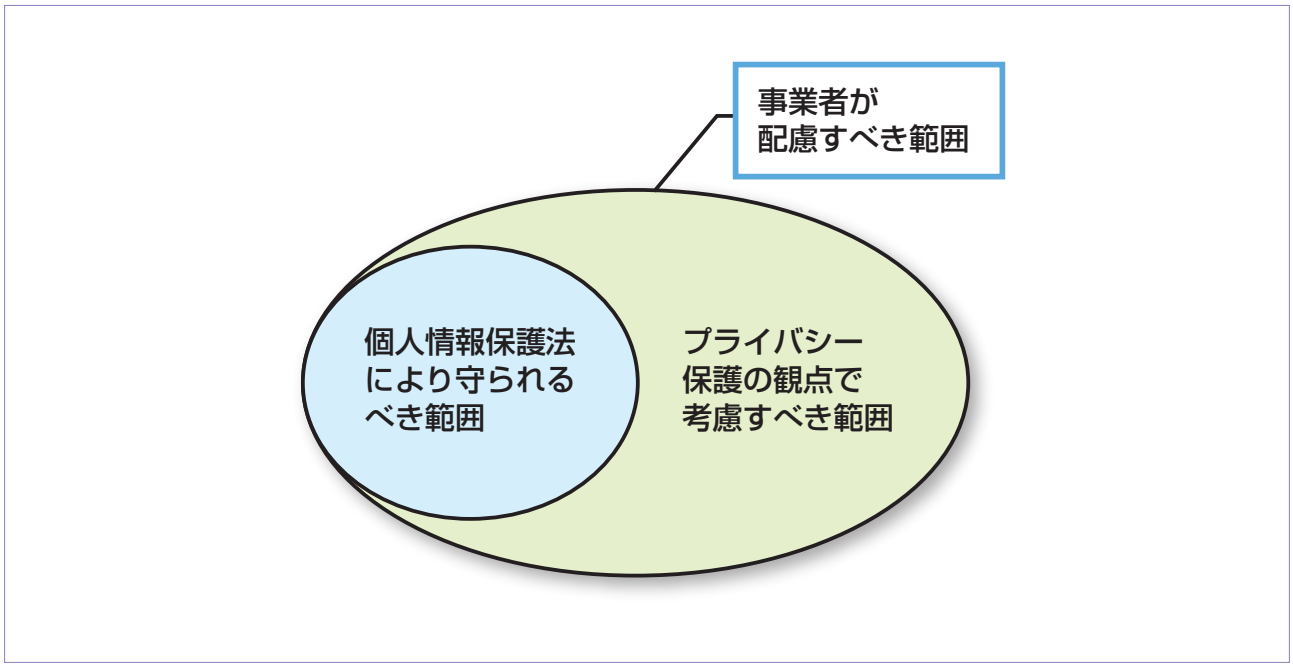
今日の社会は、デジタル技術の発展とサイバー空間の拡張により急速に構造転換を迎えている。高度に発達したセンサー・カメラ・ドローン等のデータ取得技術や、あらゆるモノをネットワークにつなげるIoT（Internet of Things）の推進によって、フィジカル空間（現実世界）の膨大なデータが、リアルタイムでサイバー空間に集積されつつある。また、近年の人工知能（AI）技術の急速な発展に代表されるデータの解析技術の進展により、蓄積されたビッグデータの解析結果がフィジカル空間にさまざまな形でフィードバックされるようになりつつある。こうしたいわばサイバー空間とフィジカル空間の融合が適切に進展することで、社会全体がより高度に発展していく可能性をとらえ、政府は、「サイバー空間とフィジカル空間を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する人間中心の社会」を、“Society5.0”と名付け、わが国が目指すべき社会の姿としている。また、このSociety5.0を実現するために、企業・経営と規制・制度の両面において、デジタル・トランスフォーメーション（DX）を一体的に進めることが重要であるとの考えの下、日本として「イノベーションと社会的信頼の双方を実現するモデル」を作るという観点から、デジタル・ガバナンス改革の検討も進められている。

こうした中でSociety5.0の実現の中核となるデータの高度な利活用は、これまでとは質・量ともに大きく異なることとなる。とりわけパーソナルデータの利活用は、個々人の嗜好やニーズにより的確にアプローチすることを可能とし、企業にとってビジネスチャンスの源泉となることに加え、個々人へのアプローチが、ひいては社会課題の解決にもつながりうることから、社会全体にとっても非常に重要である。

一方で、パーソナルデータの利活用の進展は、プライバシー問題のリスクを拡大する可能性が高いという点で、他のデータの利活用とは異なる課題を抱えていると考えられる。そもそもプライバシーという概念自体が、社会全体がそのときに抱いている価値観によって変化する性質のものであるということに加え、パーソナルデータの利活用の進展により拡大するプライバシー問題のリスクには、「私生活をみだりに他人に知られないこと」のような典型的なものにとどまらず、たとえば、データ解析の結果、機械的に不当な差別的取扱いを受ける、あるいは個人の政治的選択に対して介入される、というような現時点であまり顕在化されない新たな問題まで含まれ、一律に定義することが難しい。こうした点にプライバシー問題への対応の難しさがあると考えられる。他方で、従来とは質・量ともに異なる新たなプライバシー問題の発生を抑制すべく適切に対応しなければ、人々のプライバシー意識の高まりや変化と相まって、社会全体がデータの利活用に対する不信感を高めることになり、ひいてはSociety5.0の実現も覚束なくなることになる。そうならないためにも、新たなプライバシー問題への取組みは、Society5.0実現に欠かすことのできない重要なものといえるのである。

2．企業のプライバシーガバナンスモデル検討の背景

パーソナルデータの利活用を担う中心は企業である。したがって、新たなプライバシー問題への取組みについても企業が中心的な役割を担うことが期待される。これまで国内におけるプライバシー問題への対応は、個人情報保護法がその中心を担ってき



図表 2 - 1．カメラ画像の適用対象の概略図

出典：「カメラ画像利活用ガイドブックVer2.0」図表 2 適用対象の概略図より

た。企業がビジネスを行う上でプライバシー問題を考える際には、コンプライアンス＝法令遵守の観点から個人情報保護法を遵守しているかが問われ、多くの場合、その点を中心に検討することをもって事業が開始されていた。言い換えれば、企業のプライバシー問題への取組みや体制は、法令遵守を中心としたComply型といえるものであった。一方で、新たなプライバシー問題の発生や人々のプライバシー意識の高まりという状況変化の中で、必ずしも個人情報保護法の遵守状況に限らない形で、企業がプライバシー問題に関する批判を避けられず、いわゆる「炎上」する事例が散見されるようになっている。法令遵守以上の積極的な取組みについての説明がなされないと、十分であるとみなされない状況が強まっているのである。すなわち、企業は法令遵守を当然の前提としながら、自身のプライバシー問題への取組みについて積極的に説明するComply＆Explain型への組織的な転換が求められているといえよう。

経済産業省では、これまでもパーソナルデータの利活用を推進するため、企業がプライバシー問題への対応を進める上でサポートとなる取組みを行ってきた。特に、IoT推進コンソーシアムの下に設置し、総務省と共同で運営しているデータ流通促進ワーキンググループ[1]では、３年間にわたり個別の事業者からのお悩み相談という形で、個別のビジネスにおいて課題となるプライバシー問題への取組みについて有識者からの助言を行うとともに、蓄積された情報を事例集という形で公表し、企業にとって有益となる情報の提供に努めてきた。また、2017年以降、利活用の期待の高いカメラ画像について、その特徴を踏まえつつ利活用の促進を図るため、事業者が生活者のプライバシーを保護し、適切なコミュニケーションをとるにあたって配慮すべき事項を整理した「カメラ画像利活用ガイドブック」を公表・改訂[2]してきた。これらの取組みに共通するのは、個人情報保護法の遵守は当然の前提としつつ、遵守に必要な助言にとどまらない、企業がより高いレベルでプライバシー問題への対応を行うという観点からの助言・情報提供をしてきたことである。（図表 2 - 1 ）

1　IoT推進コンソーシアム　データ流通促進ワーキンググループ
http://www.iotac.jp/wg/data/

2　カメラ画像利活用ガイドブックver2.0
https://www.meti.go.jp/press/2017/03/20180330005/20180330005.html

一方で、これまでの取組みは個別の事業に対して個別具体的な取組みを示すものにとどまっていた。このため、Comply＆Explain型への企業の組織転換に向けたサポートとなる、より普遍的な取組みを検討すべく、今般、「企業のプライバシーガバナンスモデル検討会」をデータ流通促進ワーキンググループの下に設置し、議論を進めることとした。

3．企業のプライバシーガバナンスモデルの具体的な検討内容

検討にあたり昨今の批判を招いた事案等から企業が抱えている課題を考えると、法令遵守が中心に位置づけられる中で、「遵守」という言葉のとおり、ある意味で受動的に、法令を守るための個別の対応そのものが主眼となってしまい、個別の対応の背後にある本質的な目的、すなわちプライバシー問題の発生をどう抑止するかという点に対しての意識が希薄化してしまっているということが挙げられる。さらにプライバシー問題への対応自体が「コスト」として捉えられ、法令遵守ができる範囲においてできる限り対応を「合理化」しようとするケースも見られる。これが高じると「法令は守っていたのに炎上する」という事態が生じることとなる。この結果、炎上を経験した企業側は必要以上に保守的となってパーソナルデータの利活用に躊躇するという悪循環が生まれかねない。

これに対して、国内外を問わず、顧客や消費者の信頼を得ながらパーソナルデータを利用した新たなビジネスを拡大させている企業も少なくない。これらの企業においては、プライバシー保護を企業にとって単なる「コンプライアンス」とは見なさず、重要な経営戦略の一環としてとらえ、自社ビジネスのプライバシーリスクを適切に評価して対応する仕組み・体制を構築するよう、経営陣が積極的に取組みを推進するとともに、ステークホルダーや社会に対して発信している。

企業のプライバシーガバナンスモデルの具体的検討においては、まず、このように経営陣が積極的にプライバシー問題への取組みにコミットすることの重要性を明らかにし、その上で、社内全体でプライバシー問題に取り組むための体制をどのように構築するかという点を整理したいと考えている。

また、検討会においては、プライバシーバイデザインという考え方にも焦点をあてて検討を進めたいと考えている。プライバシーバイデザインとは、ビジネスモデルや組織の中でプライバシー問題が発生する都度、対処療法的に対応を考えるのではなく、あらかじめプライバシーを守る仕組みをビジネスモデルや技術、組織の構築の最初の段階で組み込むべ

原則	内容
事前的／予防的	プライバシー侵害が**発生する前**に、それを予想し**予防**すること。
初期設定としてのプライバシー	プライバシーを保護することを**当たり前の機能**として最初から組み込まれていること。
デザインに組み込む	プライバシー対策を、システムおよびビジネス・プラクティス、社会基盤にまで**組み込むことで最適化**される。
ゼロサムではなく、ポジティブサム	ポジティブサムの「WIN－WIN」のアプローチをとることで、**セキュリティとプライバシーを両立**させる。
徹底したセキュリティ （ライフサイクルを保護）	**情報のライフサイクル全体を通してプライバシー対策**を行う。
可視性／透明性	情報技術、組織や社会基盤の中でプライバシー対策がどのようになされているか**可視化**する。また、企業組織の理念、目標に対して独立した検証（第三者による監査など）を行い、**透明性**を高める。
ユーザの尊重	**個人の利益を尊重**し、適切な通知、権限委譲、およびユーザプライバシー対策について選択可能な状態で提供する。

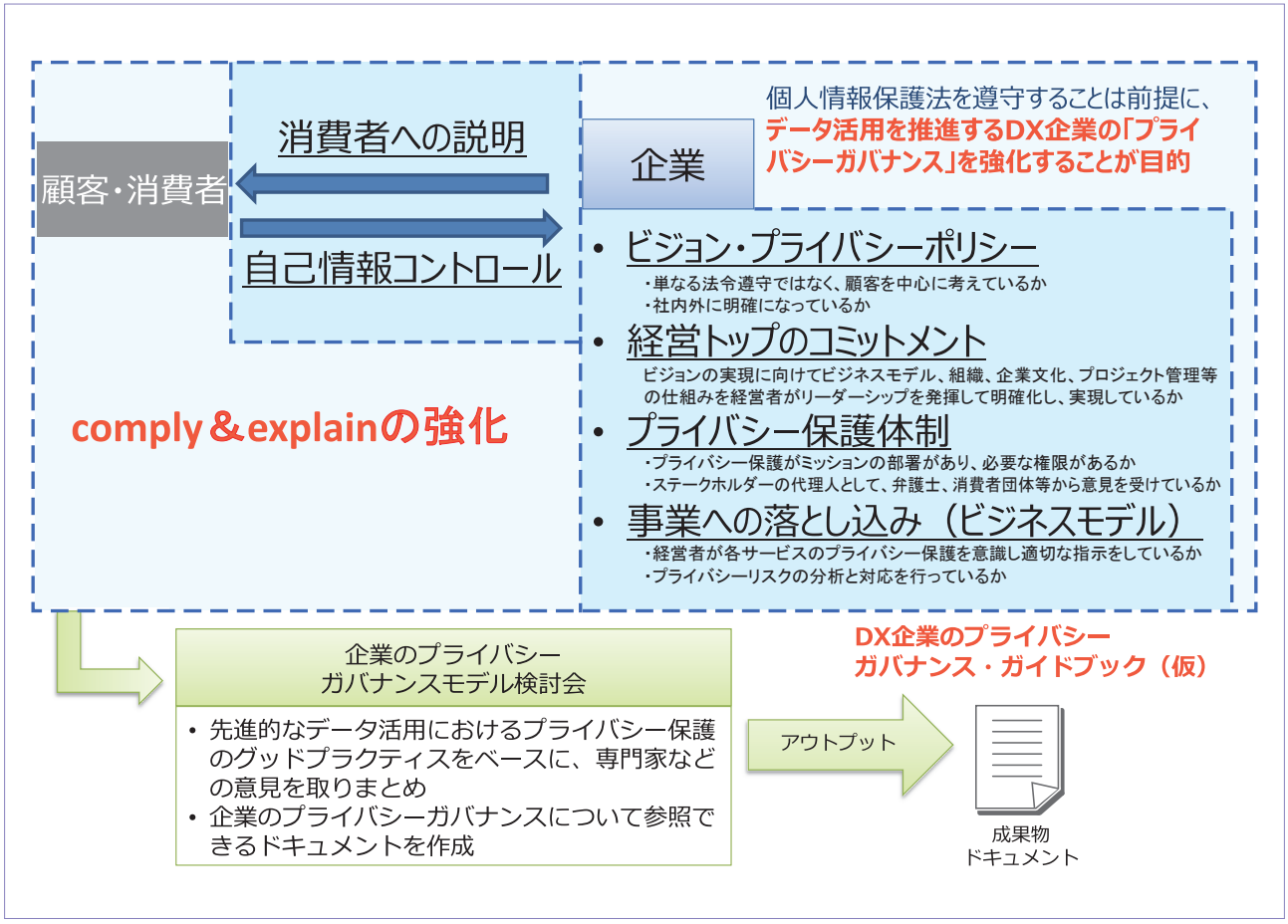
図表 2 - 2．プライバシーバイデザインの 7 つの基本原則

きであるという考え方である。プライバシーバイデザインの基本概念は、①プライバシーに対して関心を持ち、その問題を解決しなければならないということを認識する、②公正な情報取扱い（Fair Information Practices（FIPs））の原則を適用する、③情報技術とシステムの開発時に情報ライフサイクル全体を通したプライバシー問題を早期に発見し、軽減する、④プライバシーに係る指導者や、有識者から情報提供を求める、⑤プライバシー保護技術（PETs）を取り入れ、統合していく、という５つにまとめられている。また、あわせて前頁の表のとおり７つの基本原則が掲げられている。（図表２-２）

他方で、ビジネスや社会環境の変化は、当初想定していなかったプライバシーに関する問題を発生させる可能性がある。この場合、最初にプライバシーバイデザインを実施していたから十分であるということには必ずしもならない。このため、プライバシーバイデザインによる仕組みの構築と、それを不断に見直し改善していくプロセスとをあわせて検討していくことになる。

加えて、企業にとってExplainが求められると先に述べたが、これは単に自身の取組みを一方的に発信することのみを意味しているわけではない。そうした発信に加えて、消費者や社会と継続的に対話を続け、自身の取組みについて理解を得るだけでなく、消費者や社会の受け止めの変化などをタイムリーに自身の取組みに反映させていくということも含まれると考えている。こうした観点から、消費者等とのコミュニケーションのあり方についても検討が必要だと考えている。

今回の検討会においては、企業内での意思決定プロセスにおけるプライバシー問題の位置づけや、プライバシーバイデザインの取込み方、消費者とのコミュニケーションのあり方などを中心に、企業のグッドプラクティスのヒアリングなどを通じて把握した実際の企業の取組みを、より普遍的な形で整理し、企業として適切なプライバシーガバナンスを構



図表２-３．企業のプライバシーガバナンスモデル検討会の概観

築する上で参考となるガイドブックを作成したいと考えている。（図表2-3）

4．おわりに

プライバシーバイデザインのようにあらかじめ企業がプライバシー問題への対応を検討する上で、自身の事業が抱えるプライバシーリスクを適切に事前評価することが重要になるが、そのためのツールとしてプライバシー影響評価（Privacy Impact Assessment: PIA）という手法がある。現在JIPDECが中心となってISOのJIS化に向けた取組みが進められており、経済産業省も後押しをしているところである。

経済産業省としても、今回ご紹介した企業のプライバシーガバナンスモデルのガイドブックの作成や、PIAのJIS化などの民間における取組みの後押しのような、わが国の民間事業者が、より高度にプライバシー問題への取組みを推進するためのサポートになる取組みを継続的に進め、パーソナルデータのさらなる利活用に繋げていきたいと考えている。

（注）本章　脚注掲載のURLは2019年12月現在のもの

Ⅲ AI倫理指針の分析と個人データ利活用

国立研究開発法人理化学研究所・革新知能統合研究センター
グループディレクター　**中川 裕志**

1．公開されているAI倫理指針

2015年以降、国内、国外のいずれにおいても人工知能（以下、AIと略記する）の倫理に焦点が当たるようになり、多くの文書が公開された。すべてを列挙することはとてもできないが、参照されることが多いものをおおよその公表時期の古いものから順に挙げると以下の図表3-1のようになる。これらのAI倫理指針は2019年10月現在、Webで公開されているため容易に内容を確認することができる。

名宛人の意味

図表3-1の最右列に期待される読み手、すなわち名宛人を記載した[1]。名宛人は指針の性格を表す。当然、名宛人としてAIの開発者はほぼすべての指針で共通する。次に多い名宛人は政策立案者である。AI開発者は、本質的に先進技術の追求あるいは売れる商品の開発を狙うため、してよいこと、すべきことを示す倫理指針を必ずしも歓迎するわけではなく、倫理指針にマッチしない開発に進むこともありえる。したがって、倫理指針に実効性を持たせたければ、より強制力のある国の政策に反映させるべ

名称	略称	作成した組織	公開時期	名宛人
Asilomar AI Principles	Asiloma	Future Life Institute	2017	開発者、政策立案者
人工知能学会　倫理指針	JSAI	人工知能学会・倫理委員会	2017	開発者、AI自体
報告書2017－AIネットワーク化に関する国際的な議論の推進に向けて－	総務省AIネット	総務省・AIネットワーク社会推進会議	2017	開発者
Ethically Aligned Design version2: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems	IEEE EAD ver2	The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems	2017	開発者、政策立案者
Ethically Aligned Design（first edition）: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems	IEEE EAD 1e	The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems	2019	主に開発者
人間中心のAI社会原則	人間中心AI	AI戦略実行会議、内閣府	2019	開発者、利用者、政策立案者
Ethics Guidelines for Trustworthy AI	Trustworthy AI	The European Commission's High-Level Expert Group on Artificial Intelligence	2019	開発者、政策立案者
Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449	OECD	OECD	2019	政策立案者

図表3-1．AI倫理指針

1　必ずしも明記されていないこともあるので、筆者の主観的判断による部分もある。

きである。これが、政策立案者が多くの指針で名宛人とされる所以である。制約をかける方向の例としてはAIの軍事応用や自律AI兵器の抑制と禁止を訴えるAsilomaで明記されている。人間中心AIやTrustworthy AIには、AI研究開発の推進するAI開発ないし投資政策を促す文言が明示されている。また、AIの利用者を意識している倫理指針も多い。

特色があるのはJSAIである。JSAI、すなわち人工知能学会 倫理指針は明快に名宛人が人工知能学会会員としている。ただし、会員宛ての前半8項目の後の9項目に「人工知能が社会の構成員またはそれに準じるものとなるためには、上に定めた人工知能学会員と同等に倫理指針を遵守できなければならない。」と明記され、素直に読めばAI自体にも人間なみの倫理観を要求している。思うに、人間なみの倫理観を持つAIは、人間と同レベルの知的能力を持つ、いわゆる汎用AIであり、これは超知能の一歩手前のAIである。したがって、JSAIの第9項目は論理的に飛躍しているように思える。

2．AI脅威論

2000年代前半のカーツワイルのポストヒューマン[2]や2014年のボストロムの超知能[3]が脚光を浴びることにより、シンギュラリティによるAI脅威論が人口に膾炙した。その結果、人間に脅威になりうるAIの開発を無制限に許していてよいのか、という不安を持つ人が増えてきた。対処方法として、その能力が許せる範囲であるAIに開発を限定しようというアイデアに焦点が当たった。同時にAIとして期待すべき機能は何かを明示していくべきだというアイデアも現れてきた。この両者を合わせてAI倫理として整理したものがAI倫理指針である。言い換えれば、AI脅威論の蔓延がAI倫理への脚光となって跳ね返っていたともいえよう。図表3-1に記載された初期のAsiloma、総務省AIネット、IEEE EAD ver 2では、このテーマは強く意識されている。Asilomaでは、19～23の5項目において直接的に超知能に言及し、その危険性を直視するように諭している。特に19項目“未来のAIの可能性に上限があると決めてかかるべきではない”は当時の危機感を如実に表している。総務省AIネットではAIの制御可能性という形で触れている。IEEE EAD ver 2では3、4、5章でこのテーマを考察している。しかし、その後、上記のAI脅威論で述べられた人間を支配するような能力を持つAIの実現性が非常に薄いことが明らかになるにつれて、この話題はAI倫理指針では扱われなくなった。

3．軍事利用

AIの軍事利用に直接触れているのはAsilomaとIEEE EAD ver 2である。一つの理由はAIの軍事利用は好ましくないという主張はあまりにも当然である一方、これを実現するためのCCW[4]のような国際政治の場は各国の利害対立があまりに生々しい世界ということがある。AsilomaではLethal Autonomous Weapon System（LAWS）、すなわち自律型致死兵器システムを単純に禁止せよと主張している。IEEE EAD ver 2では、AI兵器の定義の再構築から始めている。大雑把にいえば、引き金を引く操作をAIの判断で行う兵器と定義される。しかし、積極的な攻撃なのか、攻撃された場合の防衛なのか、など複雑な戦場の状況では明確な定義が困難であろう。IEEEが工学、技術系の学会であるから、このような議論にあるのは当然である。また、直接的にAI兵器禁止を声高に記載しないのは、IEEEには多くの兵器製造に関連するメーカも入っているからではないかと思われる。最新のIEEE EAD 1eではこの問題に全く触れていない。他の指針でもほとんど触れられていない。なお、AIの軍事利用の倫理的側面については拙著[5]でまとめている。

2　R. カーツワイル：『ポスト・ヒューマン誕生』，NHK出版，2005
3　N. Bostrom: Super intelligence, Oxford University Press. 2014
4　特定通常兵器使用禁止制限条約
5　中川裕志：裏側から視るAI，近代科学社，2019/ 9 /24刊

4．透明性、説明可能性、アカウンタビリティ、トラスト

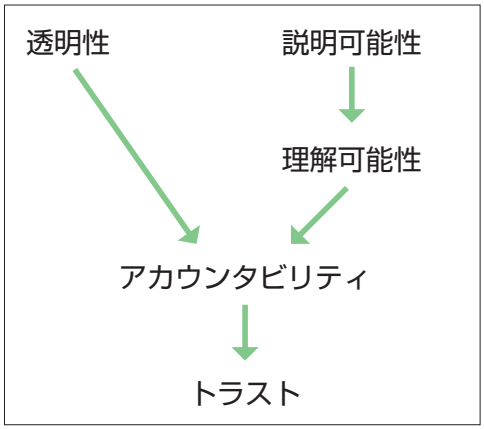
これらの項目は2018年以降に公表された倫理指針で取り上げられている。概念のわかりやすさから透明性がまず取り上げられ、その技術的側面として説明可能性が浮上してきた。特に日本において、これらは技術的論点と考えられていた。

説明可能性は、AIの動作内容を説明できることである。しかし、内部変数の値の変化などを表示されても開発者でもなければ理解はできない。したがって、説明可能性はもう少し丁寧に、AIシステムの一般人利用者にAIの内部動作が理解できることと定義しなければならない。一般人の利用者に理解可能な説明を生成することは困難なタスクである。AIの挙動を、AIが使っているアルゴリズムに沿って説明するような内部動作由来の説明は研究されたが捗々しい成果があがっていない。最近は、AIの動作を外部から見て理解できる簡単なシミュレータを、たとえば、決定リストや、各ノードが条件で、yes、noの各々の場合に移動する先のノードからなる決定木のように**理解可能性**のある形式[6]で表現し、入力から出力結果に至るルートを表示するような方法が研究されている。

3つ目の概念である**アカウンタビリティ**に至るとその概念が未だに正確に捉えられていない状況を散見する。アカウンタビリティは通常「説明責任」と和訳される。これを説明する責任があるという誤解が蔓延している。事故が起きた時のアカウンタビリティとは、事故が起きた理由を説明することに加えて、事故によって発生した損害を補償することまで含む。よって、**透明性**とは、AIシステムの動作を説明するだけではなく、補償に関係するステークホルダー、すなわちAIシステムの開発者、運用者、AIシステムの運営会社、その会社への出資者なども開示されなければならない。

このように考えてくると、アカウンタビリティは背後にある人的、組織的問題、技術的問題の両者が絡み合うため、一般のAIシステム利用者にとって理解が困難である。そのような状況で、一般利用者にも通用するアイデアとして**トラスト**[7]が浮上する。実際、トラストに言及するようになったのは、図表3-1のAI倫理指針では「人間中心AI」以降である。利用者がAIシステムをトラストするのはAIの動作理解の中身について理解を必ずしも要求しない。むしろ、同一のAI、あるいは同じ業者の提供するAIシステムが、過去に事故や不具合をおこしていないこと、あるいはAIシステムを提供している業者の過去の動作に落ち度がなかったこと、あるいは補償がきちんと行われたことなどによって、その業者の提供するAIシステムがトラストできるということになる。

以上の項目の間の関係を図表3-2に示す。



図表3-2．諸概念の関係

5．フェアネスと悪用、誤用

フェアネスあるいは公平性について陽に触れているのは、JSAI、人間中心AI、Trustworthy AI、OECDである。個人データの種々の属性、たとえば性別、人種、年齢などのうち、公平に扱うべき属性が決まれば、AIによる判断が、それらの属性に対して公平であるように制約をかける方法はすでによく

6　このようにAIシステムを近似するように作られた決定木をBorn Again Treesと呼ぶ。
7　trustはAとBの2者の間に成立する関係である。AやBが他の者からtrustされうる存在であることをtrustworthyと言う。

研究[8]されている。ただし、公平性はその確保のためにアファーマティブアクションのような方法を用いると、逆差別も起こしやすい[9]。

IEEE EADver 2 、 1 eでは悪用、誤用（misuse）をいかに防ぐかという観点から“Awareness of misuse”という標語で具体的な提案を行っている。AIの仕組みで防ぐだけではなく、悪用、誤用による被害を受けた者、発見した者からの内部通報制度を法制度化すること、通報者の保護、組織内で悪用・誤用をしないように教育すること、被害者に対する保険による補償の活用などを提言している。

6．独占禁止、国際協調

特定の企業や国によるAI技術やデータ資源の独占への警鐘を強く鳴らしているのは人間中心AIだけである[10]。一方、国際協調ないし開発組織間の協調はAsilomaと人間中心AI、Trustworthy AI、OECDで陽に言及されている。政治的ないし企業経営の観点からは難しい問題なので、他の倫理指針ではあえて触れなかったのであろうか。

7．プライバシー保護

すべての倫理指針で継続的に取り上げられているテーマとしてプライバシーの保護がある。このことから、プライバシーはAIシステムの主要かつ最も儲けになる対象データであることが予想される。他方、そのような予想が人々にとって不利益を生まないことを目指して、GDPR[11]に見られるようなプライバシー保護の世界的潮流が強いことが窺われる。

IEEE EAD ver 2 および 1 eでは個人データの管理に関してData Agencyというタイトルで提言をしている。また、間接的ではあるが、Trustworthy AIやOECDでも触れられている。この論点の展開を次節で試みる。

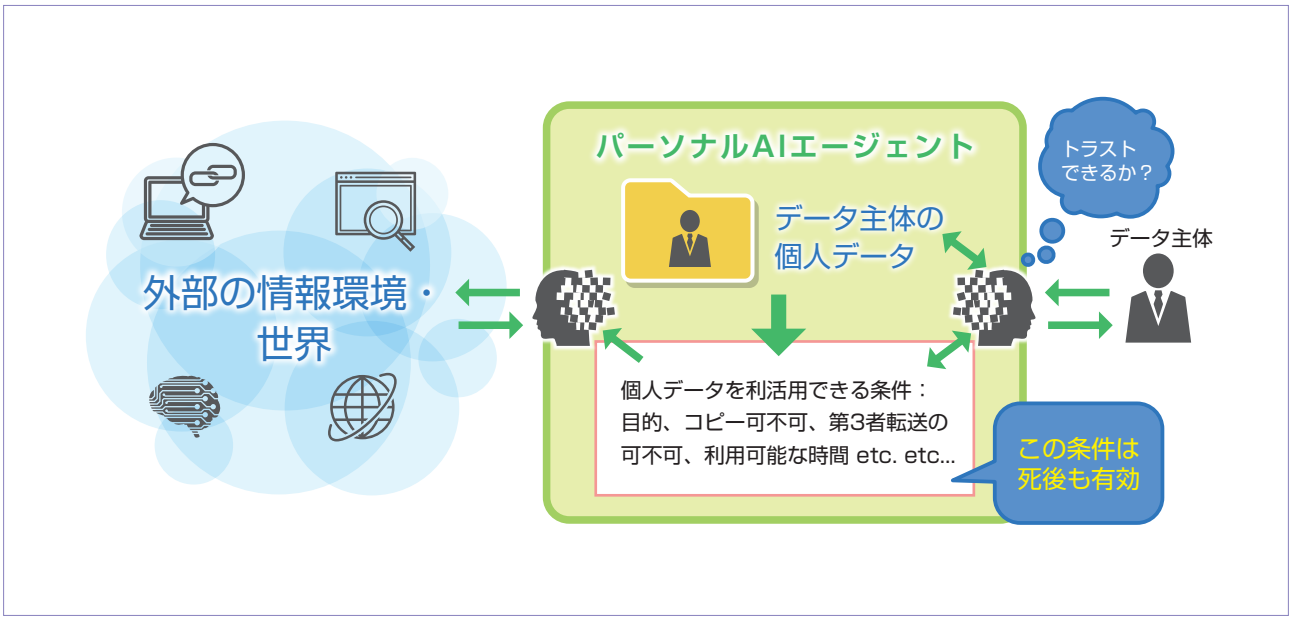
8．パーソナルAIエージェント

この節では、個人を代理するData Agency をAI技術によって実現するパーソナルAIエージェント（以下では、PAI Agentと略記する）について説明する[12]。

情報が溢れかえり、複雑化する一方の情報を扱う社会において、生身の人間が対峙できる時代は終わり、外界と個人を仲介してくれるAIによる個人の代理、すなわちPAI Agentが各個人にとって不可欠な存在になることが予想される。すでに起こっていることとして、家庭に入り込んできているAIスピーカがある。また個人情報を預けて運用を任せる情報銀行なども存在しており、これらを一般人が運用するには生身では難しく、PAI Agentの支援が必要になるのではないかと思われる。PAI Agentの概念を図表 3 - 3 に示す。

データ主体である個人の代理をするPAI Agent（図の中央）のデータ内容は、図の右側のデータ主体の個人データと、個人データを外部の事業者など（図の左側）が使う場合の利活用条件群からなる。明記しておくべきことは、個人データも利活用条件もPAI Agentに最初から与えられているわけではない[13]。最初からデータ主体が利活用条件を記述することはデータ主体にとって負担が大きいし、また

8　直接的に公平に扱う属性だけでなく、当然ながら、その属性に間接的に作用する属性も含めて公平化する。
9　拙著『裏側から視るAI』近代科学社 2019/ 9 刊の 5 章を参照していただけると幸いである。
10　人間中心AIの場合、日本の経済的位置、地政学的立ち位置を反映しているのかもしれない。
11　EUのGeneral Data Protection Regulation
12　ここでのPAI AgentはIEEE EAD ver2, 1eに書かれていることそのものではなく、そこに書かれた指針を実装する場合の私案、および補足である。
13　最初から利用条件をデータ主体が記述するシステムとして、PDE（Personal Data Ecosystem）が提案されていたが、あまり普及していないようである。筆者がみたところでは、利用条件の記述が難しく、IT技術の専門家でもなければとても書けそうにないと思われた。



図表 3 - 3．PAI Agentの概念と仕組み

種々の利活用ケースを数え上げることは現実的ではない。よって、外部事業者との利活用に関するやり取りにおいて、PAI Agentがその利活用の可否をデータ主体に伺いを立て、データ主体の可否判断の結果を使って利活用条件を徐々に拡充していくことが現実的であろう。このような処理はデータベースの解釈、更新を含む知的処理が必要であるため、PAI Agentのデータ主体向けインタフェースと外部事業者向けインタフェースにはAI技術が使われる。

図表 3 - 3 ではPAI Agentは独立したソフトウェアのように描かれている。たしかにこのような独立したソフトとして個人のスマホや個人対応するクラウドサーバ上で実現することもありえるだろう。一方で、情報銀行やSNS業者の個人個人に対応したサービスを行うAIインタフェースとして実現されることもあるだろう。PAI Agentの具体的な実装は今後の課題である。

今後の課題として次に考えられるのは、PAI Agentはデータ主体の個人データを扱うとするなら、どのような期間においてデータ主体の代理をするのであろうか、という問題である。人間は生まれる前、すなわち胎児のときから両親の氏名やDNAという個人情報を他者が知ろうと思えば知られてしまうし、成長して学校に通い、社会人として仕事をし、最後に退職して死にいたるまで、常に自分の外側にある膨大かつ複雑な情報の世界に係わり続けなければならない。また、死後もSNSメッセージやメールのような大量のデジタル遺産として個人データが残される。このような長期間にわたる代理をするとなれば、PAI Agentはどのような機能を持つべきかという問題があり、筆者を含めたグループ[14]で検討中である。

9．まとめ

最近、相次いで公開されたAI倫理指針のうち影響力の大きな指針を図表 3 - 1 で列挙し、それらの指針の内容について、その内容的変遷と変遷の理由を説明した。最後に倫理指針の重要な項目の一つであるプライバシー保護について、プライバシーの保護と利活用を支援する手段であるパーソナルAIエージェント（PAI Agent）の概念の導入のその仕組みの解略を紹介した。今後のデータ利活用の重要なツールとなるAIとデータ流通の関係についての展望をするうえで、読者の皆様のお役に立てれば、筆者としては望外の幸せである。

14　科学研究費基盤（B）『情報ネットワーク社会における「死」の再定義』代表者：折田明子

Ⅳ IoTを活用した新たなサービスとインフラのあり方 ～ライフスタイル認証技術から見た観点～

東京大学大学院　情報理工学系研究科附属　ソーシャルICT研究センター　**山口 利恵**

1．はじめに

近年、ビッグデータ、IoT時代といわれるとおり、さまざまな機器から得られる情報をさまざまな角度から解析を行った上で、解析結果を活用した便利なサービスが増えてきた。本稿の中では、特に最近目立ってきたセンサーやカメラから得た情報を活用し、ユーザに便利なサービスを行っている例を取り上げ、現状について考察する。これらのサービスの一部は近未来サービスと呼ばれることもある。

こういった便利なサービスは、ユーザが画期的に便利だと感じる一方で、サービス実現のためにさまざまな情報を解析し活用しなければならないことも多く、プライバシーの問題が大きいことが指摘されている。

現状、こういった問題に対しての唯一の解は、ユーザに適切に解説・説明し、「同意」を取得しなければならない。ユーザが「同意」をせずにサービスに参加することはできないようになっている。

しかし、「同意」をしなければサービスに参加できないために、ユーザ自身に真の選択肢がないことや、ユーザが本当に正しく理解をした上で、「同意」ボタンを押しているかどうかについて問題があることは多数の論文で指摘されている。特に、今回紹介するような最先端のサービスの実現のために必要とされている情報は、「名前や住所を利用します」、といったような単純な説明だけでは想像できないような別の問題を生じさせる危険性がある。そこで、これらの問題について指摘し、今後発展するであろうサービス実現のために、社会が踏むべき項目について議論する。

2．最近のデータを活用したサービス

（1）複数のサービス事例

最近始まってきた近未来のサービスについて紹介する。これらのサービスは、個人に関する情報をさまざまな角度から取得した上で、データを渡した人が自分のデータが利用されていることを感じられるサービスである。

事例 1 ：Amazon Go

2018年 1 月にはじまったアメリカのECサイト大手であるAmazonが行っているレジ無しのスーパーである[1]。

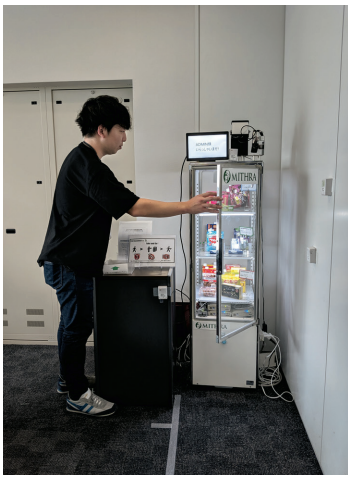
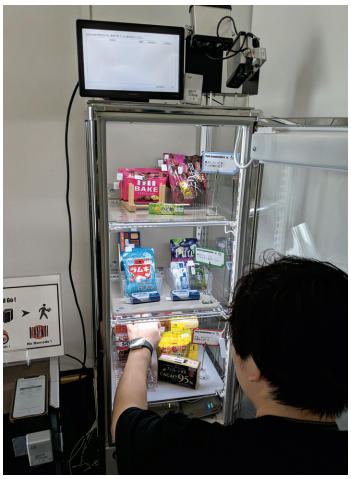
入り口にてスマートフォンアプリに表示されるQRコードをかざし入場（チェックイン）し、店舗内にある商品を手にとり、そのままお店を出ればよい。従来あったようなレジに買いたいものを提示するということがないし、お金やカードを店内で出すことはない。つまり、ユーザはチェックイン後に買いたいものを手に取るだけで、カード等も提示せずに決済が終了する。このサービスは、入り口にてQRコードの所持者を確認し、そのあと、店内に無数に存在しているカメラが人物を常に補足（トラッキング）している。この補足によって、入場者が何を取得したのかを把握し、取得したものに対する決済を要求する。

事例 2 ：JR東日本の無人決済店舗

2018年10月にJR東日本とJR東日本スタートアップが無人決済店舗の実験を行った[2]。

この無人店舗の実験は、顧客が店舗に入り好きな

1　“Amazon.com: : Amazon Go.” https://www.amazon.com/b?ie=UTF8&node=16008589011。アクセス日： 8 11月. 2019。
2　“AIを活用した無人決済店舗の実証実験第二弾を赤羽駅で実施.” https://www.jreast.co.jp/press/2018/20181001.pdf。アクセス日： 8 11月. 2019。

図表 4 - 1．三菱UFJニコス内で実施されたライフスタイル認証の実証実験模様

商品を手に取った後、お店を出るときにSuicaを利用してチェックアウトをする仕組みである。商品の取得については店内の棚に存在してあるセンサーによって何を取得したのかを判断し、最後にSuicaにて決済を行う。

事例 3 ：顔認証を利用したサービス

顔認証のようなバイオメトリクスの利用は、建物のセキュリティエリアの管理や国が管轄する入国管理[3]など、限定された空間での利用が多かった。しかし、近年は、利便性を重視したようなサービスにおいても利用されることが増えてきた。

その一例として、顔認証の事例を取り上げる。大阪にあるユニバーサルスタジオジャパンでは、年間パスポートの取得者の入場管理に顔認証を行っている[4]。このため年間パスポート取得者はユニバーサルスタジオジャパンに対して顔写真を登録し、毎回園を訪れるたびに顔認証によって顔を提示することによって入場している。

事例 4 ：ライフスタイル認証

筆者が行っている研究として、ライフスタイル認証という研究がある。この研究は、人の行動に関する情報をスマートフォンやIoTデバイスを用いて取得し、人それぞれのライフパターンの特徴を活用して認証する手法である[5]。

2019年 8 月には、認証手法を実サービスにつなげるための実証実験を行い、近年流行っているオフィス内置き菓子をもっと手軽に利用できるようにしたサービスの実現に取り組んだ。この実験では、ユーザがスマートフォンをかざしたり等せずとも、冷蔵庫型の商品コーナーの扉が自動的に開き、ユーザはその中にある商品を取得することで、自動的に決済まで進む（図表 4 - 1 参照）。この実験は、Amazon Goですでに行われているような無人店舗実験の簡易版に見えるが、大きな違いは、Amazon Goで行われている二次元バーコードによるチェックインやJR東日本の行っているSuicaによるチェックアウトが必要ない点が特に画期的である。

ライフスタイル認証では、ユーザの動向を逐一解析することによって、新しいサービスが実現できるという考えで行われている。ユーザが認証のために特に新たな動きを覚えなくてもよいようにするので、高齢者、障碍者、ITに詳しくない人でもサービスを受けられるようなことにも繋げたいと考えている。

3 “法務省：顔認証ゲートの更なる活用について（お知らせ）.” http://www.moj.go.jp/nyuukokukanri/kouhou/nyuukokukanri07_00168.html。アクセス日： 8 11月. 2019。

4 “年間パス｜USJ WEBチケットストア.” https://s.usj.co.jp/ticket/apass/。アクセス日： 8 11月. 2019。

5 “ライフスタイル認証（MITHRAプロジェクト）.” http://www.sict.i.u-tokyo.ac.jp/research/lifestyle.html。アクセス日： 8 11月. 2019。

（2）これらのサービスに関する考察

前節でとりあげたサービスについて、取得している情報の概略をとらえた上で、これらの情報がプライバシーの懸念が大きいことを指摘する。その一方で、このように利便性が特に高いサービスは、今後特に普及していくと考えられるので、その普及のあり方とユーザへの説明方法について、今後考えるべき項目を指摘する。

①取得されている情報の概観

Amazon GoやJR東日本の無人店舗の実験は、複数のカメラやセンサーを利用して人の動向や、店内すべてを記録しなければサービスを実行できない。あわせて、これらの解析を行うために、一部のデータ解析についてはオンライン上のデータサーバによって計算がなされているケースもあろうかと考えられる。また、顔認証については、とりあげたテーマパークに加え、アイドルのファンクラブ会員のコンサートにおけるチケット転売を抑止するためにも利用がされている[6]現状があり、オンライン上に顔データが存在していないにしても、会員すべての情報が何らかのデータとしてどこかに保存されている。

②プライバシーに関する懸念

このような状況から考えるに、今回とりあげたサービス以外にもさまざまな場で普及している現状から考えると、ユーザの動向情報や生体情報の一部がインターネット上の何らかのサーバに置かれている可能性もある。もちろん、特徴量に変換している可能性もあるが、変換の程度などについての数値的な評価尺度が決まっているわけではない。

個人に関する情報がすべて保存されているといった状況は好ましくないという指摘がある一方で、このようなサービスが有しているという事例から考えるに、ユーザの利便性を重視すると情報を取得せざるを得ない状況がある。つまり、これらの状況はプライバシーとして問題である一方、自動化されたサービスの活用は、ユーザの負担感が大きく減り利便性が上がっており、おそらくさまざまな場で普及していくであろう。

③全体最適から個のサービスへ

従来のデータ利用は、ビッグデータ解析をして全体の傾向分析を扱ったものが多かった。この全体傾向分析は、サービス全体の効率化や最適化を目指しているケースが多く、何らかの統計情報にあたるため、ユーザのプライバシーの懸念については、少なかったといえる。

一方で今後のサービスは顧客に対していかに適切なサービスをしていくかを考えなければならない。そのためには個々のデータをさまざまな角度から解析しユーザに還元していく必要がある。つまり、統計情報にならないようなデータを解析しなければならず、プライバシーの懸念も大きい。（図表 4 - 2 参照）

3．今後のための検討事項

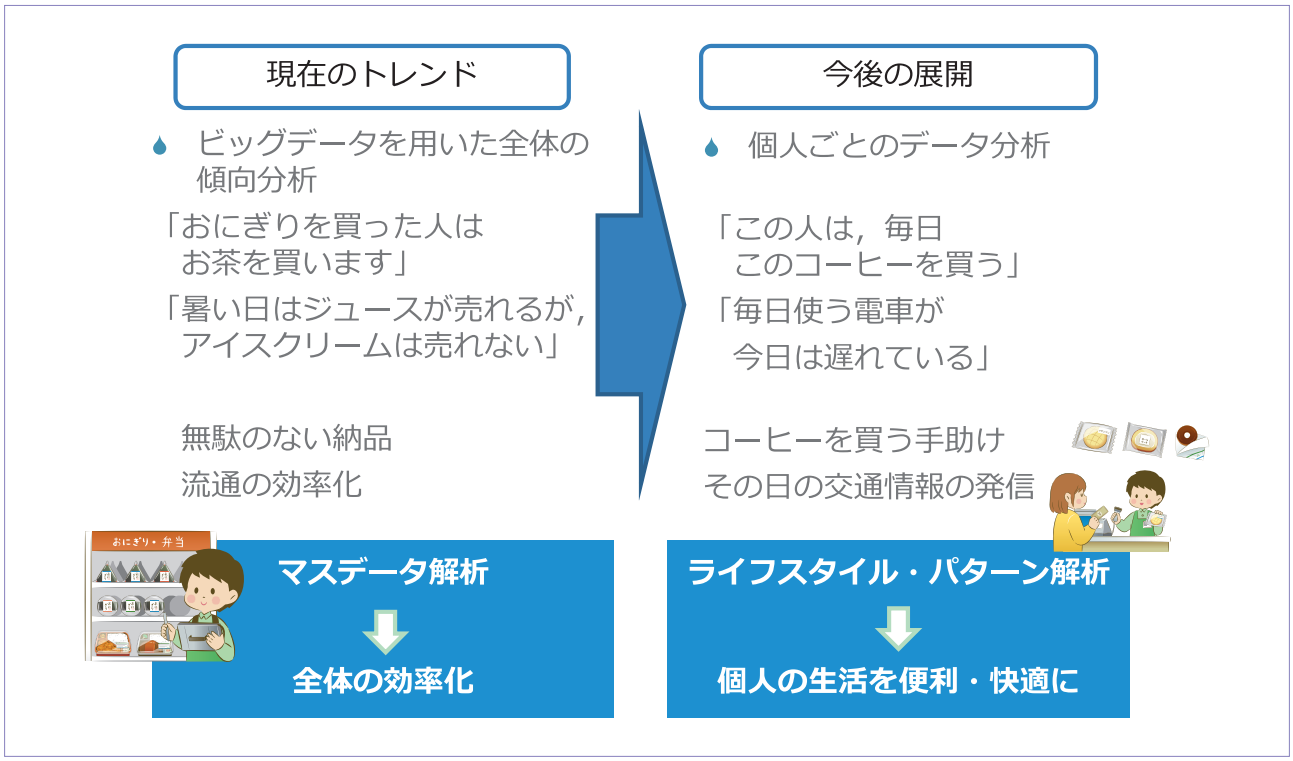
今後も上記に挙げたようなありとあらゆるデータを活用したサービスは、サービス向上を目指し発展し普及していくと思われる。このような状況の中で、ユーザの負担を減らして利便性の高いサービスを行いながらも、ユーザのプライバシーについて配慮するためにはどうしたらよいのかを検討する。

（1）情報管理者の複雑化

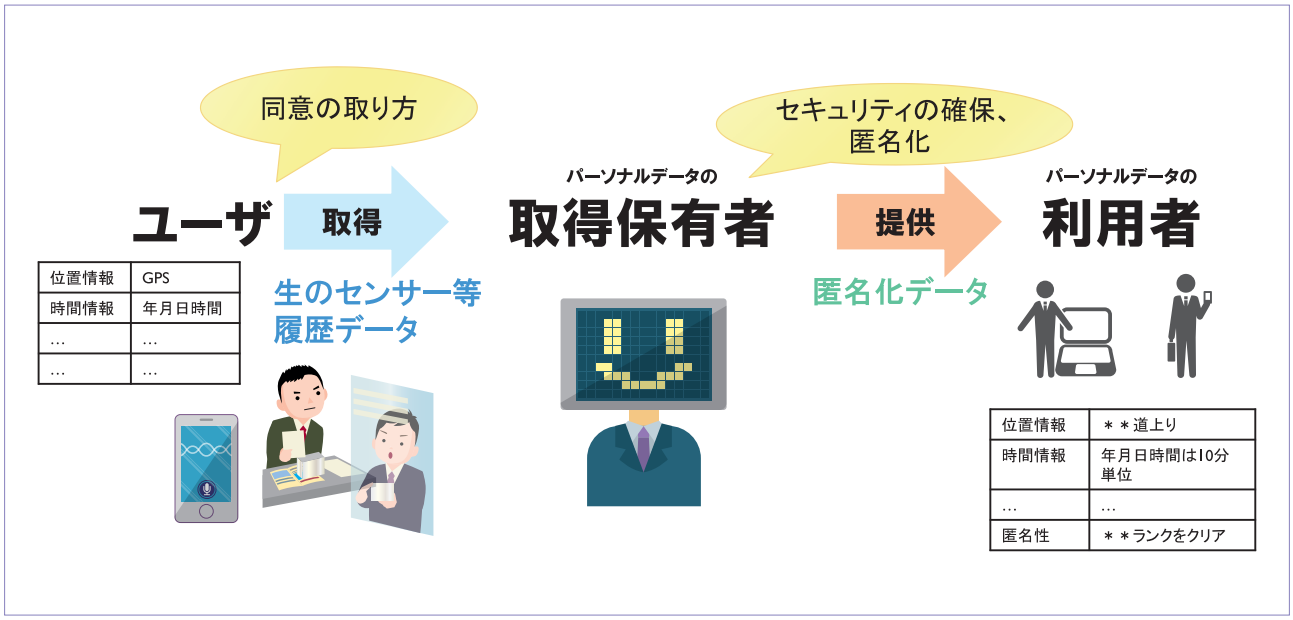
従来のサービスは、情報の取得者とサービス提供者が同一であることが多く、1 箇所の情報をどのように管理していけばよいのかを検討すればプライバシーの問題を解決できるような場面が多かった。このモデルの上では、情報が増える問題はあるにせよ、情報の管理者としては単純であるので、問題は比較的考えやすい。

また、よく見かけた場面では、情報の保有者が何らかの匿名化処理、つまり、プライバシー処理をした上で、サービス提供者に情報を提供してきた。（図表 4 - 3 参照）

6 “インフォメーション｜ももクロチケット.”https://momoclo-ticket.jp/mp/ae。アクセス日：8 11月. 2019。



図表 4 - 2．全体最適から個のサービスへ



図表 4 - 3．情報の管理者に関する匿名化処理をする場合のモデル図

たとえば、車の渋滞に関する情報の場合は、複数の車の動きに関する情報を取得し、ある信号から次の信号まで 5 分ぐらいかかるなどの情報にすることで、ユーザの生データを渡さざるともデータの利用者にとって有益な情報として渡すことができた。

しかし、すでに発生している事例としては、情報の取得者とサービス提供者が違うだけでなく、取得者も複数いたり、解析をする人が間に入るなど、複雑化してきている。特に、近年は人工知能的な研究が進んでおり、解析も従来に比べ容易になってきており、匿名化した情報でもユーザにたどり着くなど、新たな問題も生じてきている。

この結果、さまざまな取得者が取得した情報が複雑に混在し、管理が複雑になったり、解析が深くなったりすることで新たなプライバシーの問題が生

じてしまう。そのため、従来のような単純な検討ではなく、さまざまなパターンをシミュレーションしなければならない状況となる。

（2）同意の取り方

従来から、情報取得者は何らかの説明を行ってユーザへの同意をとって、それを踏まえてサービス提供が行われてきた。しかし、前節で述べたような情報管理者が複雑化することによって、ユーザから適切な同意がとれるかどうかは懸念が残る。現状行われているような同意の取り方では、ユーザが正しく理解をした上で、「同意」のクリックを押しているとは言いがたい。また、サービスが替わるごとにユーザへの同意を求める必要性があるのだが、あまり頻繁であればあるほど、ユーザに同意に対する嫌悪感だけが広がることになり、結局理解されない同意文書が多発することとなる。適切な「同意」の取り方について、検討不可欠である。

4．おわりに

現状の最適化社会に向けた取組みは、サービスの無駄がなくなり、さまざまな場での効率化が実現するなど、良いことも多数ある一方、検討が進めば進むほど、社会全体としては閉塞化し、だんだん歪みが生じてくる。しかし社会生活を行っていくためには、ストレスフリーであったり、心豊かであったり、生活にうるおいを与えるといったキーワードをもとにして、全体として余裕をもつための新たなサービスの実現が不可欠である。（図表 4 - 4 参照）

このような新たな観点のサービス実現のためには、情報の適切な管理とそれに対する適切な解析が必要であるが、一方で、現実に動いているサービスの現場において、アクセスコントロールを適切に実行しつつ、実現することはなかなか難しい。

今後は、ユーザ個々に有益な情報を還元できるサービスの実現が望まれる。

図表 4 - 4．安全快適社会を目指すためのキーワード

〈資料1〉国内外の主な個人情報保護関連の年表

国　内	年	海　外	
	1970	ドイツ	ヘッセン州において世界初の「データ保護法」採択
徳島県徳島市「電子計算機処理に係る個人情報の保護に関する条例」施行 コンピュータ処理された個人情報の適正な管理が目的（6/28）	1973		
	1974	アメリカ	「プライバシー法」制定
「電子計算機処理データ保護管理準則」策定	1976		
	1977	ドイツ	「データ処理における個人データの濫用防止に関する法律（連邦データ保護法）」制定（1月）（2009年に改正）
	1978	フランス	「データ処理・データファイル及び個人の自由に関する法律」制定
		カナダ	「カナダ人権法」制定
	1979	コミッショナー	「プライバシー・コミッショナー会議」開始
	1980	欧州評議会	閣僚委員会が「個人データの自動処理に係る個人の保護に関する条約（条約第108号）」採択（9/17）
		OECD	「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」採択（9/23）
	1981	欧州評議会	「個人データの自動処理に係る個人の保護に関する条約（条約第108号）」発布（1/28）
	1982	カナダ	「連邦プライバシー法」制定
	1983	ドイツ	ドイツの憲法にはデータに関連したプライバシーの権利が含まれていないが、連邦憲法裁判所が個人の「情報を自己決定する権利」を公式に認める
福岡県春日市にて「個人情報保護条例」可決（7/4）。10/1施行	1984	アメリカ	「ケーブル通信政策法」制定
		イギリス	「データ保護法」制定（1998年に改正）
	1985	欧州評議会	「個人データの自動処理に係る個人の保護に関する条約（条約第108号）」発効（10/1）
JIPDEC、民間事業者を対象とした「個人情報保護に関する調査研究」に着手	1986	アメリカ	「電子通信プライバシー法」制定
「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律案」閣議決定	1988	アメリカ	「コンピュータ・マッチング及びプライバシー保護法」制定
JIPDEC、「民間部門における個人情報保護のためのガイドライン」策定（5月）			
「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」公布（12/16）（「行政機関の保有する個人情報の保護に関する法律」で全部改正） 1989年10月1日に第三章と23条以外の規定が施行 1990年10月1日に全面施行			「ビデオプライバシー保護法」制定

国　内	年	海　外	
	1994	韓国	「公共機関における個人情報保護に関する法律」制定
		フランス	フランス憲法では明示的にはプライバシーの権利は保護されていないが、憲法裁判院がプライバシーの権利は憲法に内在的に含まれていると裁定
	1995	香港	「個人データ（プライバシー）法」制定
		台湾	「1995年コンピュータ処理に係る個人情報の保護に関する法律」制定
		EU	「個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する欧州会議及び理事会の指令」公示（10/24） （加盟国に３年以内の個人情報保護法制の整備を求める）
	1996	アメリカ	「電気通信法」制定
通商産業省、「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」公表（３/４）	1997		
JIPDEC、プライバシーマーク制度開始（４/１） （1997年の「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」に基づく）	1998	アメリカ	「児童オンラインプライバシー保護法」成立（10/21）
		EU	「EUデータ保護指令」施行（10/24）
			スウェーデンで、アメリカン航空に対してスウェーデン国内で収集した搭乗者の個人情報を米国内の予約センターに移転することを禁じる（11月）
		イギリス	「人権法」採択（11月）
「JIS Q 15001個人情報保護マネジメントシステムー要求事項」制定（３/20）	1999		
	2000	カナダ	「個人情報保護及び電子文書法」制定
		EU-アメリカ	EU・米国間における「セーフハーバー協定」締結（７月）
	2001	アメリカ	「米国愛国者法」制定（10/26）（2015年６月失効）
「個人情報保護法」公布・一部施行（５/30）	2003		
	2004	APEC	「APECプライバシーフレームワーク」採択（10/29）
「個人情報保護法」全面施行（４/１）	2005		
「JIS Q 15001：2006」改正（５月）	2006		
	2007	APEC	「越境プライバシールール」策定 「パスファインダープロジェクト」の試験的な取組み開始
	2012	EU	「EUデータ保護規則案」提出
		アメリカ	「消費者プライバシー権利章典」が掲載された行政白書にオバマ大統領が署名（２/23）
「行政手続における特定の個人を識別するための番号の利用等に関する法律」および関連法公布（５/31）	2013	OECD	「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」改正（７/11）

国　内	年	海　外	
特定個人情報保護委員会発足（1/1）	2014		
APEC越境プライバシールール（CBPR）システムに参加（4月）			
「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律」成立（9/3）	2015	アメリカ	・「米国自由法」成立（6/2） ・「サイバーセキュリティ情報共有法」にオバマ大統領が署名（12/18）
		EU-アメリカ	欧州で「セーフハーバー協定」無効判決（10月）
特定個人情報保護委員会が改組し、個人情報保護委員会発足（1/1）	2016	EU	欧州本会議「一般データ保護規則（GDPR）」を正式可決（4/14）
APEC-CBPRシステムの認証団体として、JIPDECがアカウンタビリティ・エージェント（AA）に認定（1月）			
個人情報保護委員会、アジア太平洋プライバシー機関フォーラム（APPA）の正式メンバーに就任（6月）			
「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律の施行に伴う関係政令の整備及び経過措置に関する政令」および「個人情報の保護に関する法律施行規則」制定（10月）		EU-アメリカ	EU・米国間における「プライバシーシールド」がEU諸国で承認（7/12）。8月から米商務省への参加申請受付開始
「改正個人情報保護法」全面施行（5/30）	2017	EU	欧州委員会、電気通信分野のプライバシー保護を目的とする「e-プライバシー規則案」公表（1月）
		中国	「中華人民共和国サイバーセキュリティ法（インターネット安全法）」施行（6/1）
「JIS Q 15001：2017」改正（12/20）		ドイツ	GDPR施行に向け「連邦データ保護法」全面改正（6/30）
情報銀行に求められる「情報信託機能の認定に係る指針ver.1.0」公表（6/26）	2018	EU	GDPR施行（5/25）
日-EU間の相互の円滑な個人データ移転を図る枠組み構築に係る最終合意確認、および個人データの越境移転に言及した共同声明発出（7/17）		フランス	「個人情報保護に関する法律」成立（5/14）
「個人情報の保護に関する法律に係るEU域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」策定（9月）		ベトナム	「サイバーセキュリティ法」公布。国内でのデータ保存と事務所設置を義務化。2019年1月1日施行へ（6/12）
		アメリカ	カリフォルニア州、消費者プライバシー法成立（6/28、2020/1施行予定）
		ベルギー	「個人データの処理に関する保護法」制定（7/30）
		イタリア	「改正個人データ保護法典」施行（9/19）
		EU	欧州委員会、日本の個人情報保護に対する十分性認定の採択手続きに着手（9月）
個人情報保護法第24条に基づき、日-EU間での相互の円滑なデータ移転を図る枠組み発効。（1/23）	2019	EU	GDPR第45条に基づき、日本の十分性認定を決定。日-EU間での相互の円滑なデータ移転を図る枠組み発効（1/23）

〈資料2〉情報化に関する動向（2019年4月～2019年9月）

国　内	海　外
2019年 4 月	
・日本政府、サイバーセキュリティ基本法の一部を改正し、サイバーセキュリティの脅威情報等の共有・分析、対策情報等の作出・共有等を迅速に行う「サイバーセキュリティ協議会」発足。 ・経済産業省（METI）、サイバーフィジカルセキュリティ対策フレームワーク（CPSF）策定。サプライチェーン全体のサイバーセキュリティ確保へ向けた取組み。 ・公正取引委員会調査、巨大IT企業の取引先・消費者を対象に行った実態調査の中間報告公表。不利益な規約変更等、IT企業側に有利な取引慣行の実態が明らかに。消費者の個人情報や利用データの収集、利用、管理への懸念は75％。 ・個人情報保護委員会（PPC）、2020年の「個人情報保護法」改正骨子案公表。個人が巨大IT企業に個人情報の利用停止を請求できる「利用停止権」新設。 ・日本サイバーセキュリティ・イノベーション委員会、セキュリティ事故発生時の損害額軽減のための評価指標（KPI）モデル策定。セキュリティ対策を 3 段階の成熟度合い別に設定し、目標管理可視化。	・米UpGuard指摘、Facebook上のアプリ経由で5.4億件以上のデータセットがAWS上で公開。 ・Amazon、ユーザと音声認識アシスタント間の会話を従業員が解析していることが明らかに。その後Google、Appleでも同様の事実が発覚。 ・欧州評議会、改正著作権指令成立。コンテンツ制作者への公正な報酬、ユーザ権利強化、巨大IT企業の責任保証盛込み。加盟国は 2 年以内に自国の法律適用義務。 ・英情報コミッショナーオフィス（ICO）、育児情報サービスのBounty社に1998年データ保護法違反で過去最大規模の40万ポンドの罰金。適切な通知なしに調査会社等とデータ共有。 ・欧州議会、巨大IT企業による電子商取引、アプリストア、SNS、価格比較ツールなどのビジネス慣行に関する規約の透明化を目指し、新規則承認。 ・欧州議会、過激コンテンツ削除要請に 1 時間以内に対応できないIT企業に対する最大売上高の 4 ％の罰金処分案を承認。 ・カナダプライバシー委員会、Cambridge Analytica（CA）事件での国民約60万人の情報不正共有に対し、Facebookを個人情報保護法違反で制裁金代わりに提訴。

国　内	海　外
2019年 5 月	
・ユニクロ・GUのオンラインストア、リスト型攻撃により約46万件に不正ログイン。 ・情報処理推進機構（IPA）発表、小学 4 年生が基本情報技術者試験合格者として最年少記録更新。 ・日本政府、2019年度のサイバー防衛に関し、中小企業を含むあらゆる企業に自律的なサイバー防衛対策を求める方針決定。 ・アンケートモニタサービスのアンとケイト、不正アクセスで77万件のアカウント流出の可能性。サーバ設定上のミスが原因。 ・日本政府、仮想通貨取引や交換事業者規制強化策として、改正賃金決済法、改正金融取引法成立。仮想通貨は暗号資産と改称。	・仮想通貨取引所大手Binance、サイバー攻撃で7,000ビットコイン（約44億円）流出。 ・シンガポール議会、ネット上の偽ニュース防止法成立。言語統制に繋がる可能性から国内外から反対の声多し。 ・米サンフランシスコ市、市職員の顔認識技術導入・利用禁止条例案可決。顔認証監視技術を禁止する米初の主要都市に。その後オークランド市等でも禁止の動き。 ・欧州連合、重要インフラへのサイバー攻撃者／機関の資産凍結やEUへの移動禁止等の制裁措置で合意。 ・OECD諸国とパートナー諸国、人権を尊重した初の国際的なAI政策ガイドライン採択。 ・米不動産保険大手First American、ウェブサイトのバグで約8.85億件の顧客データ露出。 ・中国政府、「データ安全管理規則」原案公表。自国内でネットサービスを運営する内外企業に対し政府へのデータ提供を義務化。重要データの国外移転時に監督部門の同意求める。 ・米ボルチモア市、米国家安全保障局製ソフトの悪用により数千台のコンピュータがハッキング被害。身代金約10万ドル分のビットコイン要求に市は支払い拒否。

国　内	海　外
2019年 6 月	
・慶應義塾大学他、一般の通信で発生しないダークネット通信を分析し、サイバー攻撃の予兆検知可能な分析技術開発成功。 ・三井住友銀行とフェリカポケットマーケティング、日本IT団体連盟が情報銀行サービス開始可能状態の運営計画に対し認定する「P認定」を国内初取得。 ・情報通信研究機構（NICT）、安全性評価コンテストで、多変数公開鍵暗号が世界記録達成。従来の解読方法よりも 5 倍の速さで計算可能に。 ・東京高裁、2014年のベネッセ顧客流出事件被害者 5 人の損害賠償訴訟で、 1 人2,000円の支払い命令。ベネッセ本社に初の賠償命令。	・米メイン州、プロバイダによる消費者のネット閲覧データの販売禁止法成立、 7 月 1 日発効。第三者への販売には同意が必須。 ・G20財務相声明、巨大IT企業へのデジタル課税に関する共通ルール推進で合意。 ・米国税関・国境警備局、ハッキング被害で旅行者の顔写真やナンバープレート写真等、最大10万人分の情報漏えい。 ・英国政府、量子コンピュータ商用化に約1.9億ドル投資。業界からの追加コミットメントで総額4.4億ドル超に。 ・Facebook、新暗号通貨「Libra」とデジタルウォレット「Calibra」の2020年提供を発表。その後、世界中の通貨政策面で問題視され、10月時点で運営見直しの可能性。 ・Facebook、ヘイトスピーチ容疑者情報の裁判所提出に同意したと仏デジタル担当相の言。合意は世界初。

国　内	海　外
2019年 7 月	
・総務省、脆弱なIoT機器を検知し注意喚起を行う「NOTICE」（19年 2 月開始）で147件に注意喚起。 ・NICT他、開発した量子鍵配送ネットワーク技術成果を盛り込んだ国際標準勧告が国際標準化機関ITU-Tで初承認。 ・セブン・ペイ、モバイル決済サービス「 7 pay」サービス開始数日後に不正アクセス被害。セキュリティの甘さから被害が収まらず、 9 月末でサービス自体を廃止。被害約800名、被害総額約3,861万円。METIは決済事業者に対し、不正利用防止のためのガイドラインの徹底とセキュリティレベル向上を求める。 ・マイデータ・インテリジェンス、商用サービス国内初の情報銀行サービス開始。購買履歴、家計収支、健康状態等を企業に自分の意志で提供し、対価を得る。 ・仮想通貨交換業者ビットポイントジャパン、不正アクセス被害で数十億円の資金流出。 ・NEC、EU首脳会議に顔認証システム提供。同会議初の生体認証導入。 ・最高裁判決、インターネット関連会社によるグーグル検索結果削除請求訴訟で、検索結果が真実ではないと認められない、として上告を棄却。 ・ビジネスチャットツールChatwork、第三者による不正ログイン675万件。うち1.1万件がログイン成功の可能性。	・ICO、2018年 9 月発生のBritish Airwaysの顧客50万人の情報流出事件はGDPR侵害と判断し、1.8億ポンドの制裁金。 ・仏上院、巨大IT企業に対する国内売上へのデジタル課税導入承認。2019年初めに遡って適用。米政府は自国企業に対する不当な扱いとして調査開始。 ・米連邦取引委員会（FTC）、FacebookのCA事件問題を巡り、約50億ドルで和解案承認。Facebookも支払い合意。 ・ロシア政府、違法情報を含む項目のフィルタリングを怠ったとして、Googleに70万ルーブルの罰金。 ・米信用情報機関大手Equifax、2017年発生の個人情報流出に関し、全米地域で最大 7 億ドル支払いで合意。 ・米司法省、GAFAへの独占禁止法違反行為調査着手。 ・ブルガリア国家歳入庁、ハッキングで国内成人500万人分の機密個人記録漏えい。 ・米証券取引委員会、Facebookに 1 億ドルの制裁金。ユーザデータのリスク開示の不十分さを指摘。 ・米金融大手Capital One Financial、不正アクセス被害で約1.06億件の個人情報漏えいの可能性。後日逮捕された容疑者は元Amazonの従業員。 ・欧州司法裁判所判定、Facebookの「いいね！」ボタンを組み込んだサイト運営企業はFacebookへの個人情報移転に関し、ユーザの事前同意を得る必要があると判断。

国　内	海　外
2019年 8 月	
・リクルートキャリア、内定辞退確率をAIで予測し、個別の予測データを30社以上の民間大手企業に提供。8,000人の学生からの同意を得ず。後日企業への販売サービス自体を廃止。後日調査で学生の閲覧履歴も取得発覚。ずさんな学生情報の取扱いに対し、PPCが初の是正勧告。厚生労働省も行政指導。 ・IPA調査、2019年の情報セキュリティ10大脅威、個人 1 位は「クレジット情報の不正利用」「フィッシングによる個人情報等の詐取」、組織 1 位は「標的型攻撃被害」。 ・Amazon、クラウドサービスAWSが冷却装置の故障で大規模障害。大多数のクラウド利用企業でサービス停止等の影響。 ・公正取引委員会、GAFA等巨大IT企業に対する独占禁止法での規制指針案公表。個人データの吸上げ行為が独禁法違反に当たると判断。 ・IT総合戦略本部、「我が国におけるデータ活用に関する意識調査」結果公開。個人情報の管理、企業への個人情報提供、情報銀行利用等に対する意識度合いを調査。	・米フィラデルフィア裁判所判決、Googleのクッキーを利用した個人情報収集に関する訴訟問題で、連邦地裁承認の和解案（クッキー使用停止および550万ドルの和解金）が不十分として、差戻しを決定。 ・国連安全保障理事会、北朝鮮が仮想通貨の不正マイニングやサイバー攻撃で、最大20億ドルの資金を違法取得したと報告書にとりまとめ。 ・韓国Suprema、セキュリティプラットフォームの生体認証データ約2,800万件が平文で公開状態に。問題発覚 1 週間後に対応措置。 ・米テキサス情報資源局、州内23機関がランサムウェア被害。身代金を要求されるも、連邦捜査局は支払いをしないよう勧告。全米市長会議は 7 月に身代金脅迫者への支払いに反対する決議案を採択。 ・米仏両政府、デジタル課税について妥協案合意。仏政府が条件付きで企業に税金の一部を払戻し。 ・独デュッセルドルフ地裁、Facebookの国内でのデータ収集を巡る連邦カルテル庁の制限に対し、仮差止め命令。

国　内	海　外
2019年 9 月	
・NTT、暗号化したままディープラーニングの学習処理を行う技術が世界で初めて実現したと発表。 ・富士通と三菱地所、丸の内地区の来街者のデータを利用した情報銀行の実証実験開始。副業マッチングサービス等展開。 ・日米政府、「日米デジタル貿易協定」合意。国によるAIアルゴリズム、ソフトウェアソースコードの開示請求原則禁止。 ・NICT調査、IPアドレス 1 件につき平均48万件の攻撃パケット受信。2018年以降、IoT機器への攻撃多し。 ・NTTドコモ、1995年にサービスを開始した「 i モード」の新規受付終了。FOMAとともに2026年 3 月でサービス終了へ。	・Facebook、オンライン上にユーザの電話番号等4.2億件が流出。同社は古いデータのため危険はない、と主張。 ・GoogleとYouTube、FTCとニューヨーク司法長官からの児童保護法違反申立てで1.7億ドルの和解金支払い。Googleによる和解金では過去最高額。 ・全米約50州・地域の司法当局、Google、Facebookを独占禁止法違反の疑いで調査実施。 ・Google、仏政府からの納税滞納指摘に対し、約10億ドルの和解金支払いで同意。 ・南米エクアドル政府、死者を含む全国民約2,000万人分の個人情報が海外流出。セキュリティが不十分なサーバでのデータ保管が原因。 ・米出前サービスDoorDash、顧客、配達員等、470万人分の個人情報流出を発表。 ・米司法省、民間企業によるDNA分析サービスの遺伝情報について法執行機関による捜査利用時の指針発表。利用できるデータの範囲制限や遺伝情報収集の際に家系図サービスのユーザから別途同意を取る、等盛込み。

IT-REPORT

JIPDEC IT-Report 2019 Winter

2019年12月16日発行（通巻第14号）

発行所　一般財団法人日本情報経済社会推進協会
〒106-0032 東京都港区六本木1-9-9 六本木ファーストビル12階
TEL：03-5860-7555　　FAX：03-5573-0561

制　作　株式会社ウィザップ