【産業競争力懇談会　2014年度　研究会　最終報告】

【オープンデータ利活用とプライバシー保護】

２０１５年３月５日

産業競争力懇談会 COCN

【エグゼクティブサマリ】

●本研究の目的

2014 年 6 月に改定された「世界最先端 IT 国家創造宣言」では、「公共データの民間開放（オープンデータ）を推進するとともに、ビッグデータを活用した新事業・新サービスの創出を促進する上で利用価値が高いと期待されているパーソナルデータの利用を促進するための環境整備等を図る」と謳われている。しかし、省庁等の公共機関が公開するオープンデータについては活用環境が整備されつつある一方で、期待されていたパーソナルデータの業種横断的な利活用による新事業の創出や社会課題の解決などは進んでいない。これは消費者側のプライバシーに対する懸念が主要な要因であり、様々な施策を通じてパーソナルデータの利活用に関する国民のコンセンサスを形成する必要がある。

本研究の目的は、公共機関のデータだけでなく、企業や個人が所有するパーソナルデータを組み合わせて得られる知見を個人や社会に還元し、ひいては経済の活性化や産業競争力強化につなげるため、パーソナルデータの利活用とプライバシー保護を両立するモデルの立案と提言を行うことにある。

●検討の視点と範囲

パーソナルデータの利活用に対して国民のコンセンサスを得るためには、データ保護に必要な法制度の整備だけでなく、ライフサイクルの様々な場面に応じてパーソナルデータを開示することが個人へのメリットにつながることを、具体ケースを例にして示すことが有効と考えられる。そこで本研究では国による調査結果を踏まえて、個人のメリットが分かりやすいと考えられる「防災」「医療・ヘルスケア」「オリンピック・パラリンピック」を具体ケースとして取り上げることとした。これらの具体ケースを通じて国民のコンセンサスの壁を打破することで市場の拡大につながることが期待できる。

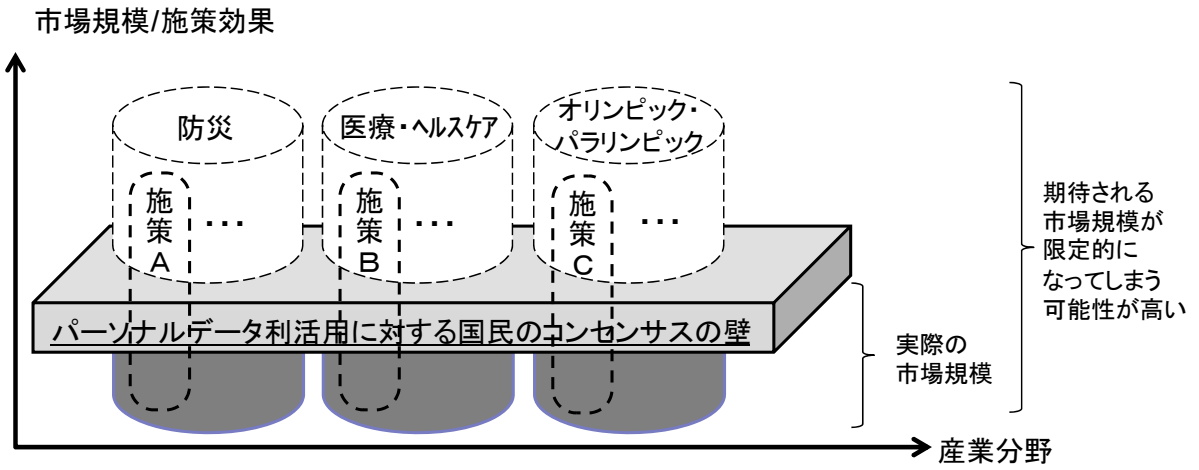


図　本研究のスコープ

国民のコンセンサスを形成する上で重要となるパーソナルデータの利活用パターンは、法令の適用による義務的な利活用（パターン①）、個人の意思・同意による利活用（パターン②）、本人同意を必要としない利活用（パターン③）に分けられる。本研究会では個人の同意に着目し、パターン②およびパターン③について提言としてまとめた。

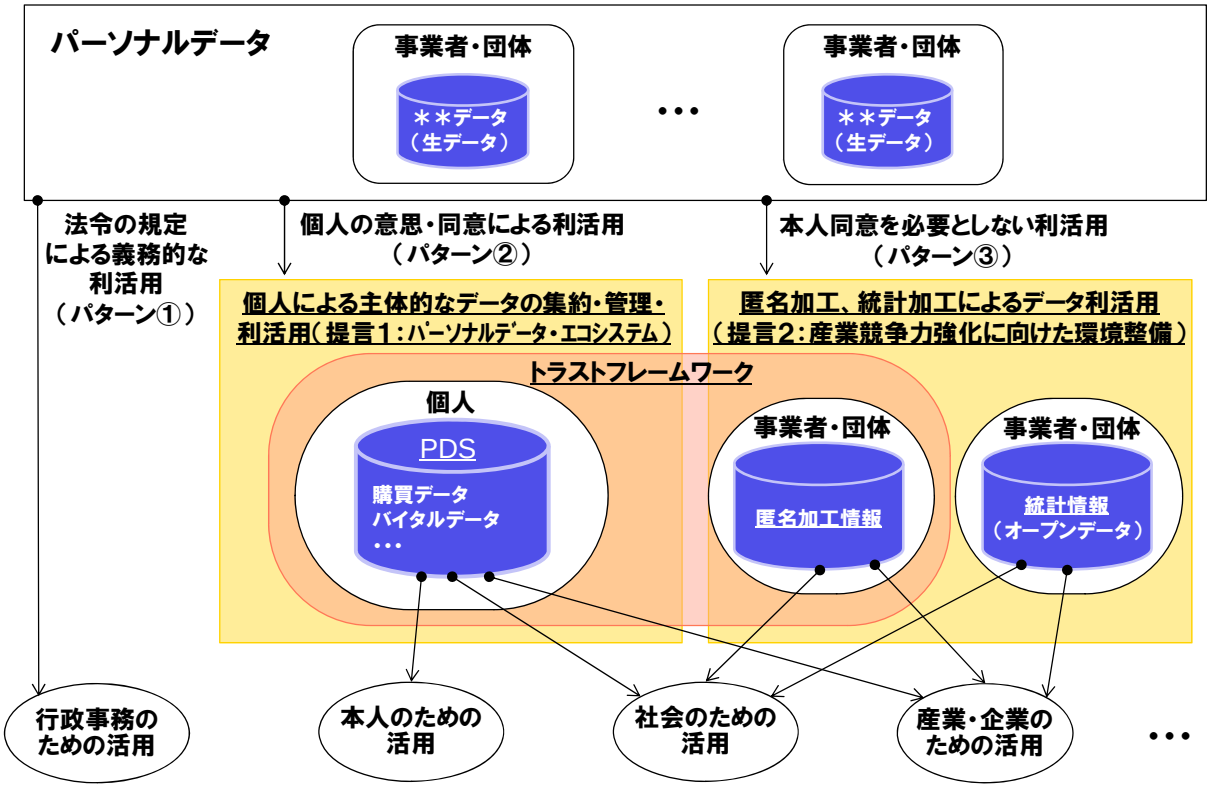


図　パーソナルデータ利活用パターンと提言の関係

まずパターン②に対応して、個人による主体的なデータの集約・管理・利活用を行う仕組みとして、パーソナルデータ・エコシステムの構築を提言する。パーソナルデータ・エコシステムとはパーソナルデータを個人が集め、管理し、様々な組織や企業に利用させることで個人が直接的に利益を得るシステムで、国内外に先進事例がある。本研究では国内外の事例や具体ケースでの検証などから日本型モデルに必要な機能を明らかにした。基本的にはパーソナルデータストア（PDS）と呼ばれるパーソナルデータを安全に格納するとともに効率的な利活用を図る仕組みを中心としている。

さらにパターン③に対応して、個人情報保護法等の制度改正で導入される見込みの匿名加工や統計加工によるデータ利活用を促進するための環境整備について提言する。個人の特定性を低減した形に加工した匿名加工情報の活用を促進することで、民間企業での新たな価値創造や社会的課題（防災、医療・ヘルスケアを始め、交通・物流、都市計画、エネルギーコントロール等）の解決などが期待できる。これらを円滑にすすめるためにも国民のコンセンサスは必要不可欠のものである。

●産業競争力強化のための提言と施策

［提言１］日本版パーソナルデータ・エコシステムの構築

諸外国と比して、日本では国民のプライバシーに対する不安感が高い傾向にある。パーソナルデータ利活用促進のために個人情報保護法の改正が進められているが、法制度の整備だけで個人の不安感や不利益感が解消されるものではない。そこで、法令の遵守に留まらず、個人のプライバシーを守りながら個人に対して新たな価値やメリットを提示する仕組みとして日本版パーソナルデータ・エコシステムを官民連携して構築する。

（施策１）個人によるデータコントロール環境整備の推進

個人が自分のデータを自分で管理できるPDS等の仕組みを推進するため、企業等によるマシンリーダブルな形式でのパーソナルデータ開示と、データ形式の標準化を進める。企業等が足並みを揃えた取組みを行うように、国がPDS推進のための積極的な旗振りを行う。

（施策２）トラストフレームワークの整備

パーソナルデータを授受する個人や企業などが互いに相手を信頼できるものとみなすことができる仕組みとしてのトラストフレームワークをグローバル視点で整備する。

（施策３）パーソナルデータ・エコシステムを前提とした新産業創出支援

個人によるパーソナルデータの提供・開示に対して金銭的対価・利便性向上・社会的意義等のインセンティブを与えるようなサービス事業者の育成を支援する。

［提言２］産業競争力強化に向けた環境整備

ビッグデータの利活用加速のため、オープン化した行政情報だけでなく企業や個人の持つパーソナルデータの利活用を促進する。プライバシー保護に配慮した形でパーソナルデータの利活用を進めるためには国民のコンセンサスが必要不可欠である。そこでコンセンサスの壁を構成する国民の不安や不満を解消するため、パーソナルデータを利活用するプロセスに関する環境整備を官民共同で加速する。

（施策１）匿名加工に対する安心感醸成に向けた国民への発信

匿名加工に対する運用規定の整備や具体例を通したメリットの体験など、国民に対する不断の情報発信を行う。

（施策２）オプトアウト規定の見直しを踏まえた利活用ガイドライン整備

個人の求めに応じた利活用の円滑な停止のため、ITの導入を念頭においた事業分野ごとのパーソナルデータ利活用のガイドラインを整備する。

（施策３）個人が利活用できるパーソナルデータの政策的な充実と管理強化

諸外国での取り組みを踏まえて政府主導で個人が利活用できるパーソナルデータを政策的に充実するとともにセキュリティ対策についても強化する。

（施策４）国民が自ら実践できるプライバシー保護対策の認知度向上

自ら実践できる対策の認知度を向上し、安全な情報化社会を構築する。

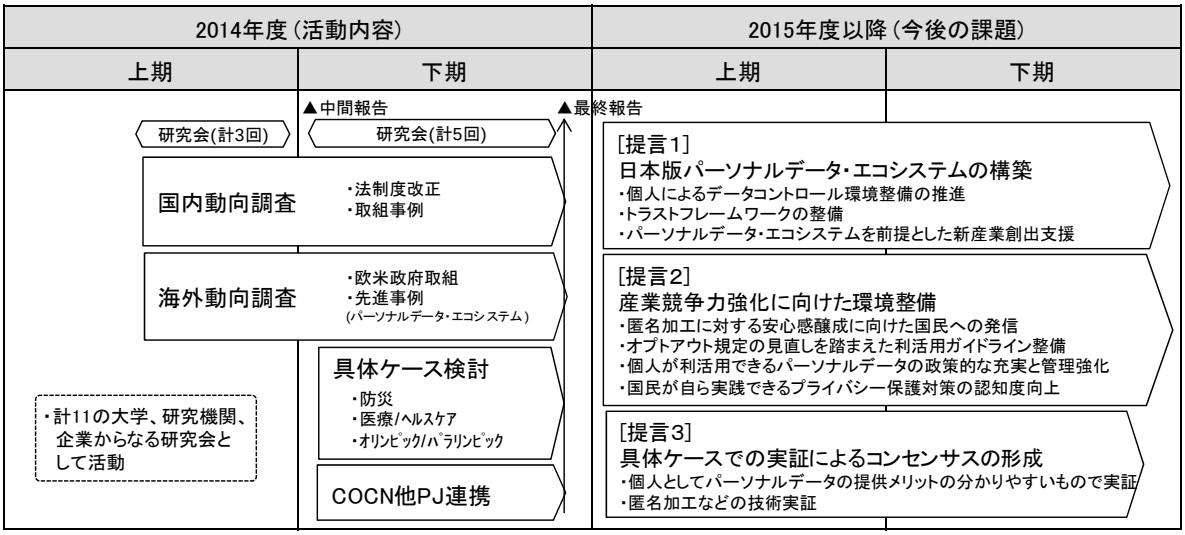
［提言３］具体ケースでの実証によるコンセンサスの形成

個人にとってパーソナルデータの提供メリットがわかりやすいもの（例えば「防災」「医療・ヘルスケア」「オリンピック・パラリンピック」）を具体ケースとして取り上げ、実証実験を通じて国民がメリットを体感できるようにする。同時に匿名加工などの技術実証を行う。

●今後の課題と展開

IoT の時代においては、カメラ、センサー、カードリーダー、カーナビ、駅自動改札、自販機など様々な場面で本人の同意なくパーソナルデータが収集・利用される可能性がある。こうした膨大なパーソナルデータに対してどのように個人のコントロールが及ぶようにするか、またどのようにして匿名加工を実施し、オプトアウトを保証するかは、具体ケースで個別に検証していかなければならない。

パーソナルデータの利活用については、具体例を通した国民のコンセンサス形成が不可欠で、そのためにはパーソナルデータを提供するメリットを個人にわかりやすく伝えるとともに、データ利活用やプライバシーに関する個人のリテラシーを向上させることが必須である。本研究ではこの点を念頭において報告としてまとめた。今後は提言や施策に挙げた内容を官民連携して加速していく。



【目　次】

【はじめに】

●本研究会の提案の背景・理由

オープンデータ利活用では、行政機関等から公開された統計データなどを、公共事業、医療、交通情報など個人の生活に向けた新たな価値創造に活用する取り組みが始まっている。欧米でもオープンデータを活用したアプリケーションサービスが多数実用化されており世界規模で今後大きな影響力を持つ事象と想定される。

地方公共団体でのオープンデータ利活用の試みも様々な形で始まっているが、現時点では地元密着型の住民向けサービスが中心である。サービスの拡充は地方活性化等に向けて非常に重要であるが、増え続ける膨大なデータからの恩恵を産業競争力強化に向ける試みとしては、別のアプローチもあわせて行われるべきと考えている。その観点から本研究会は、オープンデータの利用価値創出・活用促進に対し、データのプライバシー保護規制、技術的課題、想定リスクなどへの対応策を検討することを目的として発足した。

海外では基本的な考え方を整備し、その精神に則る形で活用が進んでいる。また各国間でのやり取りのルール等を調整する機関が存在する。グローバル競争激化の中で、海外諸国との間での諸問題を解決しながら日本が競争力強化を図っていくためには未だ様々な課題が存在するが、オープンデータ活用を推進するための、政府、自治体、民間企業との連携が重要である。本研究会は産官学共同で、その課題解決に向けた方向性を提言した。

特にデータ公開に関する国民の理解と活用効果の認識の整理が必要である。ＣＯＣＮ研究会として、欧米諸国の先進事例も視野に入れ官民一体となった方針として整理し、日本の産業界の活性化につなげる。

●本報告により実現を目指す産業競争力強化上の目標・効果

本研究では、単に公共機関の公開するデータだけではなく、パーソナルデータも含めたデータを対象として、個人活動から生まれる様々なデータについても、個人の権利を守りつつ、個々人の許諾の元で、公共的な利益が得られる場合に「オープンな」データとパーソナルデータを組み合わせて得られる知見を導くこと及び利活用するために必要な仕組み・制度等を対象範囲に含めた。ビジネス規模と照らし、オープンデータの中でも対象範囲が広く、オープンデータの電子化規模や利活用が産業界を活性化し、競争力強化につながるもの、もしくは日本の社会インフラを強化するもの（医療/災害対応等）を本研究対象とした。

ＣＯＣＮとして産業競争力強化に向け、他研究/プロジェクトの進捗を踏まえて共通課題を特定し、提言・施策としてまとめた。今後、さまざまなデータ利活用が加速し、日本の産業競争力向上に資するものと期待する。

産業競争力懇談会
会長（代表幹事）
西田　厚聰

【研究会メンバー】

〇リーダー

安田　誠　　（株式会社日立製作所　情報・通信システム社
Senior Technology Evangelist）

〇サブリーダー

中村　章人　　（独立行政法人産業技術総合研究所　情報技術研究部門　主任研究員）
若目田　光生　（日本電気株式会社ビジネスイノベーション統括ユニット　主席主幹）
加藤　晋弘　　（株式会社日立製作所　情報・通信システム社　経営戦略室　企画本部
担当本部長）

〇研究会メンバー　（組織名、氏名　五十音順）

・沖コンサルティングソリューションズ株式会社
後藤　裕久　　（エグゼクティブマネージャー）
長谷川　晴朗　（シニアマネージングコンサルタント）

・沖電気工業株式会社
須崎　昌彦　　（研究開発センタ　センシング技術研究開発部　部長）
竹内　晃一　　（研究開発センタ　センシング技術研究開発部　チームマネージャ）
伊加田　恵志　（研究開発センタ　センシング技術研究開発部）

・株式会社国際社会経済研究所
東　富彦　　（主幹研究員）
小泉　雄介　　（情報社会研究部　主任研究員）

・独立行政法人　産業技術総合研究所
渡辺　創　　（セキュアシステム研究部門　セキュアサービス研究グループ
研究グループ長）

・清水建設株式会社
大門　将人　　（情報システム部　情報管理グループ　グループ長）

・株式会社東芝　クラウド&ソリューション社
山中　泰介　　（ビッグデータ・クラウドテクノロジーセンター開発第一担当　参事）

・日本電気株式会社

徳島　大介　　(SI・サービス市場開発本部システム概念開発グループ マネージャー)

佐古　和恵　　(クラウドシステム研究所　技術主幹)

森　拓也　　(クラウドシステム研究所　主任研究員)

武田　安司　　(政策渉外部　シニアマネージャー)

重田　篤史　　(ビッグデータ戦略本部　主任)

・株式会社日立製作所　情報・通信システム社

小松原　瑛里子　(経営戦略室　企画本部　経営企画ユニット　担当部長)

中田　順二　　(経営戦略室　企画本部　経営企画ユニット　主任技師)

・株式会社富士通研究所

鵜飼　孝典　　(インテリジェントテクノロジ研究部)

・三菱電機株式会社

松田　規　　(情報セキュリティ技術部　開発第 2 グループマネージャー)

・早稲田大学

澤谷　由里子　(研究戦略センター　教授)

松島　裕一　　(研究戦略センター　教授)

〇事務局

・株式会社日立製作所　情報・通信システム社

加藤　晋弘　　(経営戦略室　企画本部　担当本部長)

小松原　瑛里子　(経営戦略室　企画本部　経営企画ユニット　担当部長)

阿知波　紀子　(経営戦略室　企画本部　経営企画ユニット)

〇ＣＯＣＮ

住川　雅晴　　(実行委員長)

富田　達夫　　(研究会担当実行委員)

寺田　透　　(企画小委員)

中塚　隆雄　　(事務局長)

【本　文】

第１章　国内/海外におけるパーソナルデータ利活用と保護の現状

オープンデータの範囲は本来非常に広範であるが、一方で官庁等の公共機関が公開するデータのみを指す場合も多い。中央省庁が公開するオープンデータについては、2014 年 10 月 1 日から内閣官房が提供するデータカタログサイト「DATA.GO.JP」が稼動を開始し、活用の拡大が期待されている[1)]（図１－１）（図１－２）。

「DATA.GO.JP」では、各行政機関が保有する、予算、決算、調達情報や各種統計情報、防災・減災情報など 10,000 件以上のさまざまなデータを一つのサイトから一括して検索できるため、より効率的なオープンデータの収集・活用が可能となる。

図１－１　DATA.GO.JP の Web サイト画面[1)]

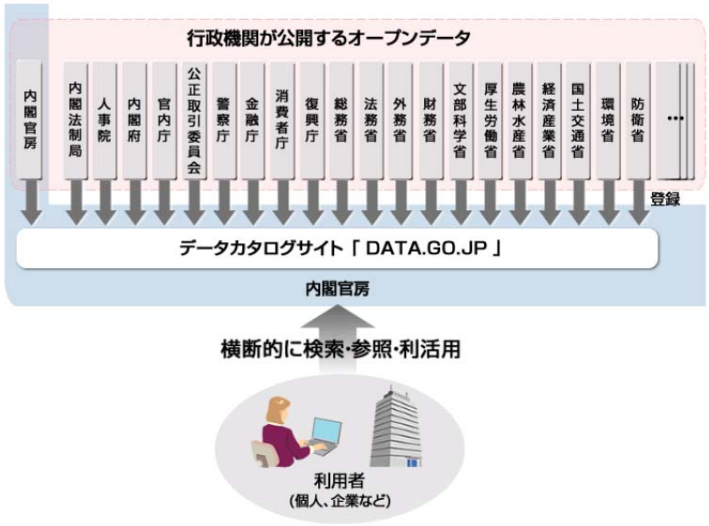


図１－２　DATA.GO.JP の概念図[1)]

このように中央省庁の公開するオープンデータについては活用環境が整備されつつある一方で、企業や個人が所有するパーソナルデータの利活用はなかなか進まない。ある民間での意識調査[2)]

によると、パーソナルデータ（当該調査の中では「生活者情報」と定義）の利活用については「期待より不安が大きい」との結果が得られた（図１－３）。性別では男性より女性のほうが、年代別では若年層よりも中高年のほうが不安を感じる傾向にある。

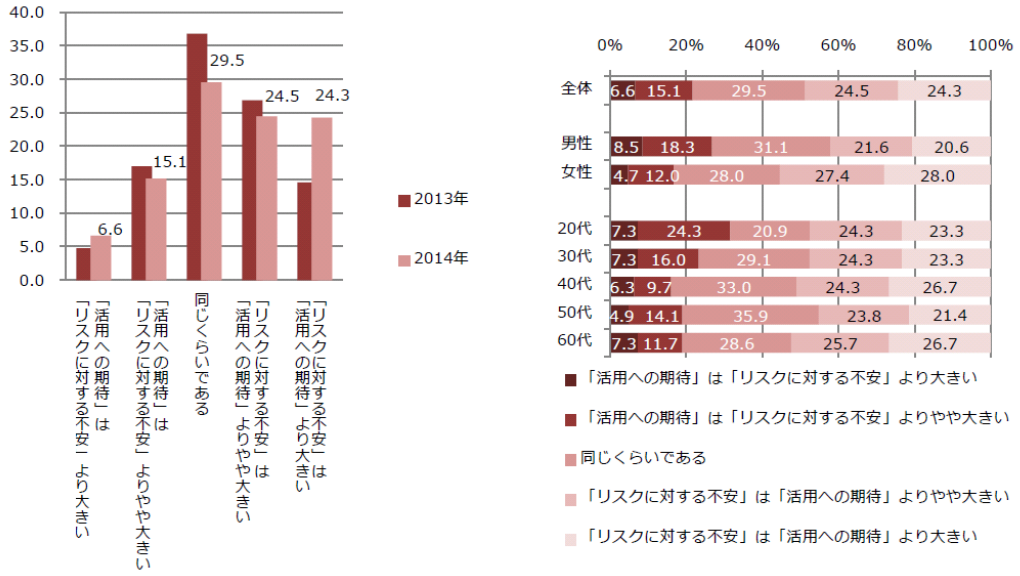


図１－３　企業や公共機関による生活者情報の活用に関する意識調査結果 [2)]

また、不安を覚える要因は上位から「目的外利用の恐れ」「利活用への拒否権の欠如」「説明・公表不足」となっている（図１－４）。すなわち個人のプライバシー侵害リスクに対する高い懸念が表れていると考えられる。

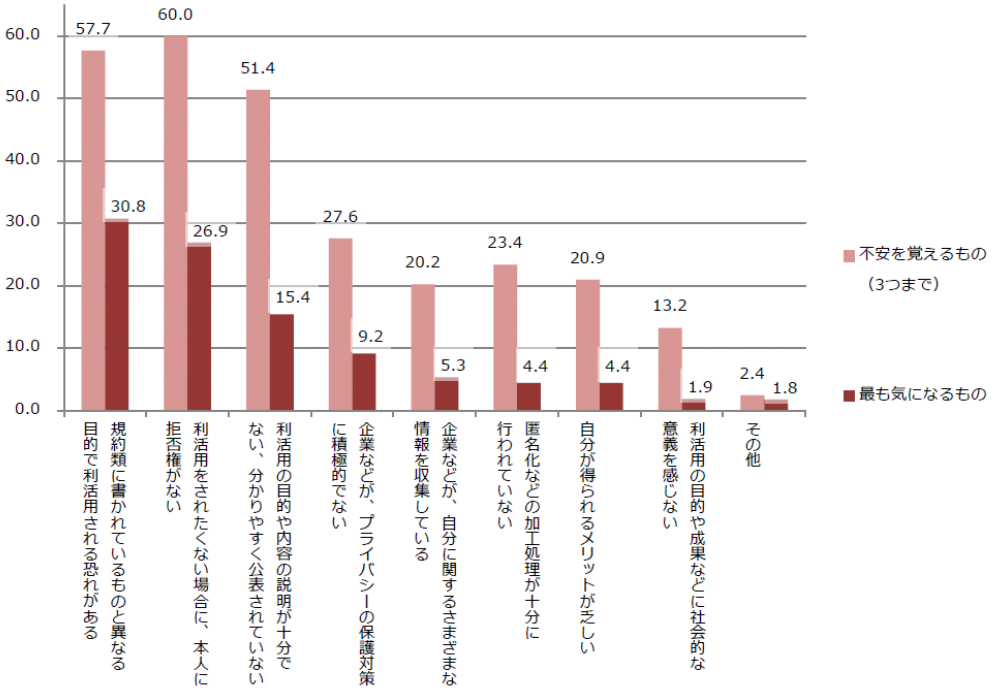


図１－４　生活者情報の利活用に関して不安を覚える要因 [2)]

また、世界 15 カ国の消費者を対象としたプライバシーに関する意識調査[3]によると、日本特有の傾向として次の点が明らかとなっている。

①今後のプライバシーに対する高い不安（15 カ国中第 1 位）

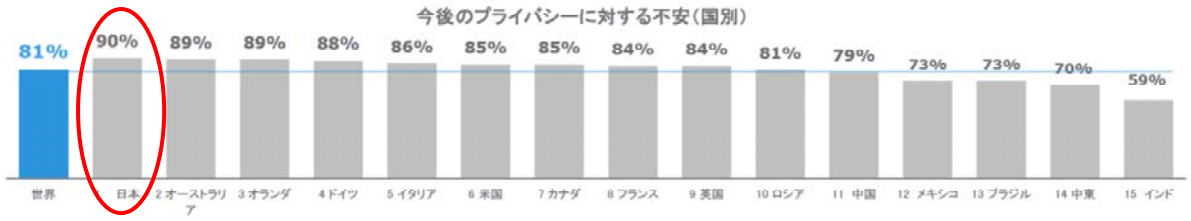


図１－５　今後のプライバシーに対する不安（国別）[3]

②自国行政機関への低い評価（15 カ国中 15 位）

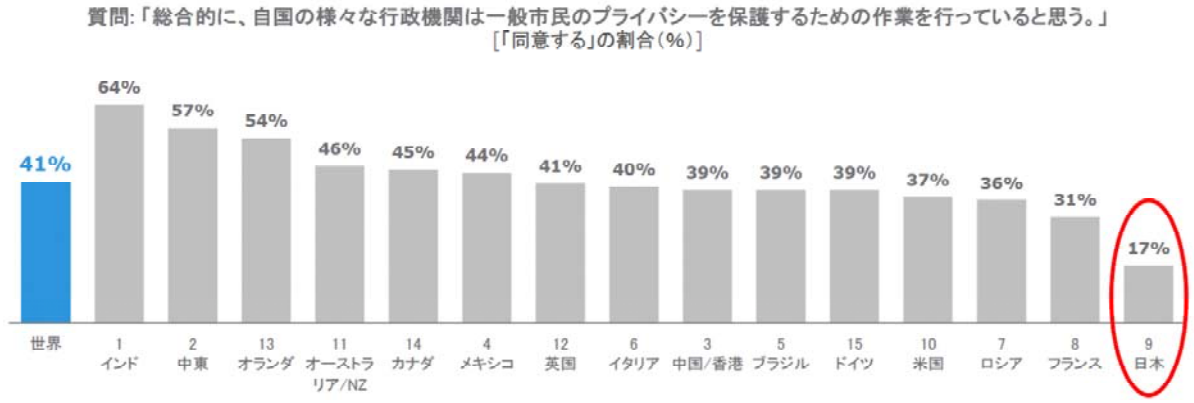


図１－６　自国行政機関のプライバシー保護に関する評価[3]

③自ら実施可能なプライバシー保護対策の低い実施率（下記 3 項目につき 15 カ国中 15 位）

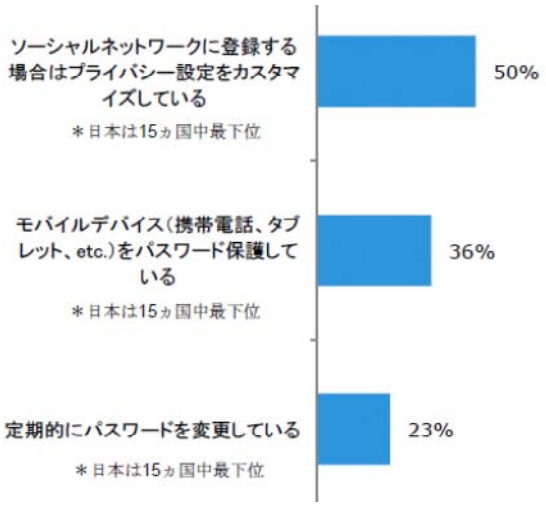


図１－７　プライバシー保護対策の実施率[3]

これらアンケートの結果を総合すると、日本ではパーソナルデータの利活用に対する不安感が

高い一方で行政機関への評価は低い。しかし、自ら積極的にプライバシー保護対策を実施しているわけではない、というかなり特徴的なプライバシー意識が存在すると言える。

こうした背景の下、本研究では、公共機関のデータだけでなく、企業や個人の持つパーソナルデータも組み合わせて得られる知見を個人や社会に還元し、ひいては経済の活性化や産業競争力強化につなげるため、パーソナルデータの利活用とプライバシーの保護を両立するモデルの立案と提言を行う。はじめに本章ではパーソナルデータの利活用に関する国内外の状況を概観する。

１．１　国内の状況

１．１．１　パーソナルデータの利活用に関する制度改正大綱および パーソナルデータの利活用に関する制度改正に係る法律案の骨子(案)

（１）経緯

2013 年 9 月､内閣官房高度情報通信ネットワーク社会推進戦略本部(IT 総合戦略本部)の下に｢パーソナルデータに関する検討会」が設置された。同年 12 月､｢パーソナルデータの利活用に関する制度見直し方針」を本部決定、2014 年 6 月､｢パーソナルデータの利活用に関する制度改正大綱」が本部決定された。同年 6 月から 7 月にかけてパブリックコメントの募集がなされ、同年 12 月に「パーソナルデータの利活用に関する制度改正に係る法律案の骨子(案)」として公開された[4)]。2015 年 1 月以降に国会へ法案提出される予定である。

（２）特徴

今後法案の提出や国会審議のプロセスにおいて内容の変更は想定されるが、2014 年 12 月時点では以下の項目が法律案の骨子(案)として提示されている。特に下線の項目について、図を引用して内容を紹介する。

１．個人情報の定義の拡充
２．適切な規律の下で個人情報等の有用性を確保するための規定の整備
<u>（１）匿名加工情報(仮称)に関する規定の整備</u>　→　（ア）
（２）利用目的の制限の緩和
（３）情報の利用方法から見た規制対象の縮小
３．個人情報の保護を強化するための規定の整備
（１）要配慮個人情報(仮称)に関する規定の整備
（２）第三者提供に係る確認及び記録の作成の義務付け
（３）不正な利益を図る目的による個人情報データベース提供罪の新設
<u>（４）本人同意を得ない第三者提供への関与(オプトアウト規定の見直し)</u>　→　（イ）
（５）小規模事業者への対応
（６）個人情報取扱事業者による努力義務への個人データの消去の追加

（７）開示等の請求権明確化

４．個人情報保護委員会の新設及びその権限に関する規定の整備

（１）個人情報保護委員会の主な権限

（２）個人情報保護指針の作成への関与

５．個人情報保護の取扱いのグローバル化に対応するための規定の整備

（１）国境を越えた個人情報の取扱いに対する適用範囲に関する規定の整備

（２）外国執行当局への情報提供に関する規定の整備

（３）個人データの外国にある第三者への提供の制限

（ア）匿名加工情報（仮称）に関する規定の整備

個人情報から特定の個人を識別することができる記述等を削除したものを匿名加工情報と呼ぶ。第三者に提供するために匿名加工情報を作成するときは、個人情報保護委員会に届け出た上で、個人情報保護委員会規則で定める基準に従い、個人情報から特定の個人を識別することができる記述等の削除（他の記述等に置き換えることを含む）をするなど、当該個人情報を復元することができないように加工をしなければならない。

匿名加工情報を第三者に提供する場合はその旨を公表すること、取得した匿名加工情報から本人を識別するために他の情報を照合することを禁止すること、などを定める（図１－８）。

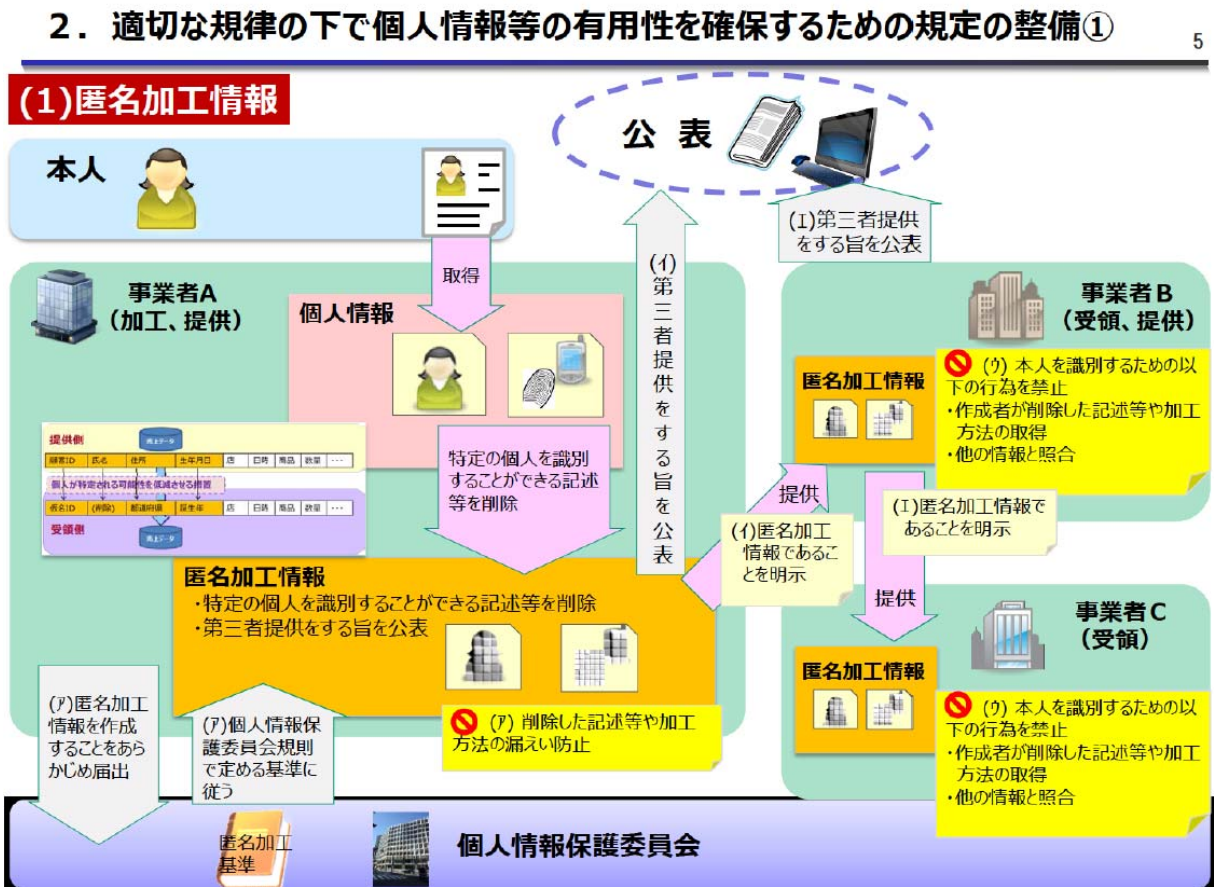


図１－８　匿名加工情報に関する規定の整備 [4)]

（イ）本人同意を得ない第三者提供への関与（オプトアウト規定の見直し）

個人情報取扱事業者は、本人同意を得ない個人データの第三者提供をしようとする場合には、次の事項を、個人情報保護委員会規則で定めるところにより、あらかじめ本人に通知し、又は本人が容易に知り得る状態に置くとともに、個人情報保護委員会に届け出なければならない。

①第三者への提供を利用目的とすること
②第三者に提供される個人データの項目
③第三者への提供の方法
④本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること及び本人の求めを受け付けること

この場合において、個人情報保護委員会は、その内容を公表しなければならず、本人への通知方法や本人が容易に知り得る状態が不適切な場合には勧告・命令を出す（図１－９）。

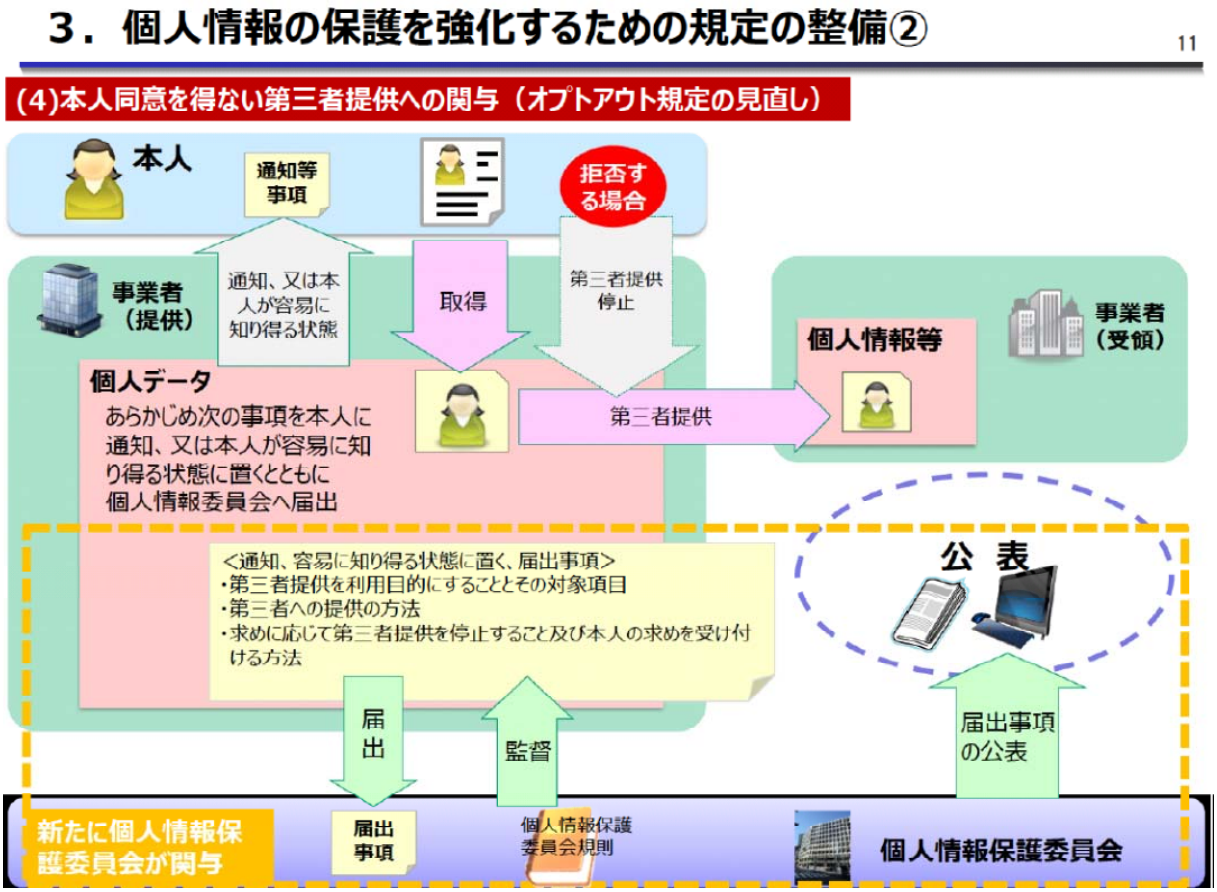


図１－９　本人同意を得ない第三者提供への関与 [4)]

ここで個人情報保護委員会は、行政手続き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監督機関である特定個人情報保護委員会を改組して内閣府の外局たる機関として設置する。

骨子(案)の中で頻出する「匿名化」「特定」「識別」については、骨子(案)の作成に先立ちパーソナルデータに関する検討会 技術検討ワーキンググループ報告書(2013/12/10 報告、2013/12/26 更新)の中で次のように定義説明されている。まず「匿名化」については、

－ 「匿名化」は個人情報から特定の個人の識別性をなくす方法として注目を集めており、本 WG はその匿名化に関して広範な議論を行っている。しかしながら、「匿名化」という用語は、無名化、仮名化、属性削除、一般化といったものから、同じレコードが複数存在し一意に個人(A さん)であることをも識別できないような状態(k-匿名性)にすることまで含む幅広い概念であり、単に「匿名化」と表現した場合に人によって受け取るイメージが異なってしまうと考えられる。このように安易に「匿名化」という用語を用いることにより議論があいまいになることを極力避けるため、本 WG では「特定」と「識別」に分けて議論している。 －
(報告書 p10 より)

として「特定」と「識別」に分けている。これらの関係については、いわゆる「匿名化」技術により加工・作成される情報のカテゴリーとして整理している(表１－１)。

表１－１　いわゆる「匿名化」技術により加工・作成される情報のカテゴリー

No	用語	用語の説明
1	識別特定情報	個人が(識別されかつ)特定される状態の情報(すなわち「個人情報)」(それが誰か一人の情報であることがわかり、さらに、その一人が誰であるかがわかる情報)
2	識別非特定情報	一人ひとりは識別されるが、個人が特定されない状態の情報(それが誰か一人の情報であることがわかるが、その一人が誰であるかまではわからない情報)
3	非識別非特定情報	一人ひとりが識別されない(かつ個人が特定されない)状態の情報(それが誰の情報であるかがわからず、さらに、それが誰か一人の情報であることが分からない情報)

同報告書では匿名化に関わる技術について、「いかなる個人情報に対しても、識別非特定情報や非識別非特定情報となるように加工できる汎用的な方法は存在しない」とし、汎用的な方法は存在しないものの「ケースバイケース、つまり個人情報の種類・特性や利用の目的等に応じて技術・対象を適切に選ぶことにより、識別非特定情報や非識別非特定情報に加工することは不可能ではない」としている。法制度の整備とともにユースケースなどを想定した詳細検討を今後の課題としている。

１．１．２　ID 連携トラストフレームワーク

（１）経緯

2013 年 6 月に策定、2014 年 6 月に改定された「世界最先端 IT 国家創造宣言」における「3. 規制改革と環境整備」において、「本人確認手続き規定の類型化を図り、契約締結や役務の利用に係る利用者の利便性向上とプライバシー保護、本人確認の正確性の担保との両立を図るオンライン利用を前提とした本人確認手続等の見直しについて検討する」とされている[5)]。

現在、本人確認を必要とする IT サービスが多数登場しており、同じユーザ ID・パスワードの使い回しなどのセキュリティ上の懸念や、IT サービスごとに様々な本人確認を行わなければならない、などの課題が指摘されており、この解決のため異なる組織間で ID 連携、データ連携を行うための信頼基盤を構築する必要がある。

こうした認識の下、経済産業省では 2013 年度から ID 連携トラストフレームワークの実証事業を開始し、有効性や実用性の実証、ユースケースの発掘、認定基準の整理等を行っている[6)]。

（２）特徴

ここで ID(アイデンティティ)とは個人に関する属性情報の集まりで、一般には利用者が利用するサービスに対応して個別に管理されている（図１－１０）。図の中でユーザ ID 発行の際に氏名などの他の属性情報は利用者から登録されるものである。利用者側が登録する属性情報の確からしさの確認方法、ユーザ ID とともに発行するパスワードの管理方法を含む認証方法などが利用するサービスに応じて多様化している。たとえば、無課金の SNS などはオンラインでの二者間の属性情報のやりとりだけで完結するが、現金決済を伴う場合は第三者を含む本人確認方法や認証方法が採用される。このため「（１）経緯」で記述した諸問題が発生する。

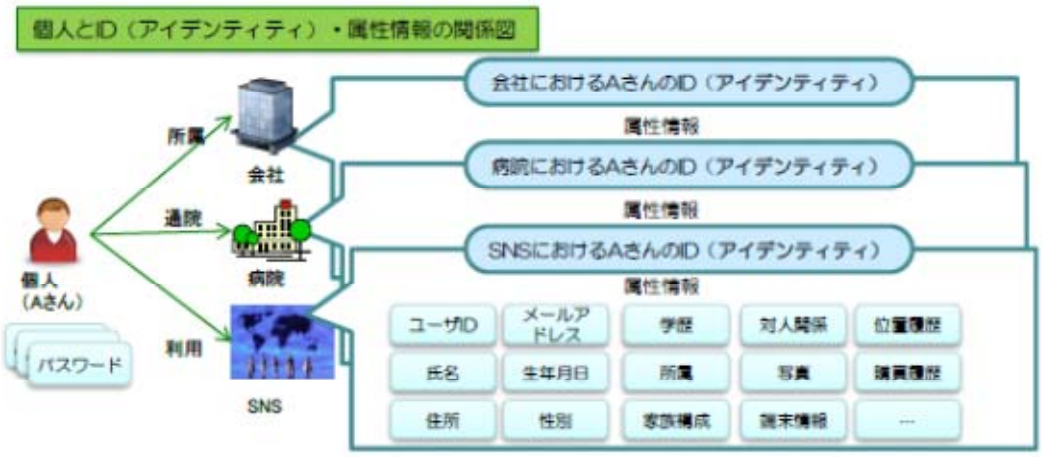


図１－１０　個人と ID(アイデンティティ)・属性情報の関係[6)]

これに対して、ある事業者が管理している ID を他の事業者のサービスでも使えるようにする仕組みが ID 連携であり、ID 連携を実現するフレームワークが ID 連携トラストフレームワークである（図１－１１）。ID 連携トラストフレームワークを構成するプレーヤーを以下に示す。

・利用者
サービスを受ける主体。自分自身を証明する情報を、IdP に渡す必要がある
・IdP(アイデンティティ・プロバイダ)
利用者を認証する主体。保証レベルによって、ID の確からしさの確認を行う
・RP(リライング・パーティ)
IdP から必要な属性情報のみを受け取り、利用者にサービスを提供する
・AP(アトリビュート・プロバイダ)
利用者に関する属性情報を IdP や RP に提供する
・ポリシーメーカー　(政府や業界)
トラストフレームワークにおける要求事項やルールを策定する。また、TFP の認定基準を策定する
・TFP(トラストフレームワーク・プロバイダ)　(第三者機関)
ポリシーメーカーが策定したルールに基づき保証レベルを定義し、保証レベル毎に IdP/RP/AP が満たすべき技術、運用面での監査要件を作成する。また、監査を行うアセッサーを認定し、アセッサーの監査結果に基づき IdP/RP/AP を認定する。
・アセッサー
TFP が作成した監査要件に基づき、IdP/RP/AP の監査を実施する

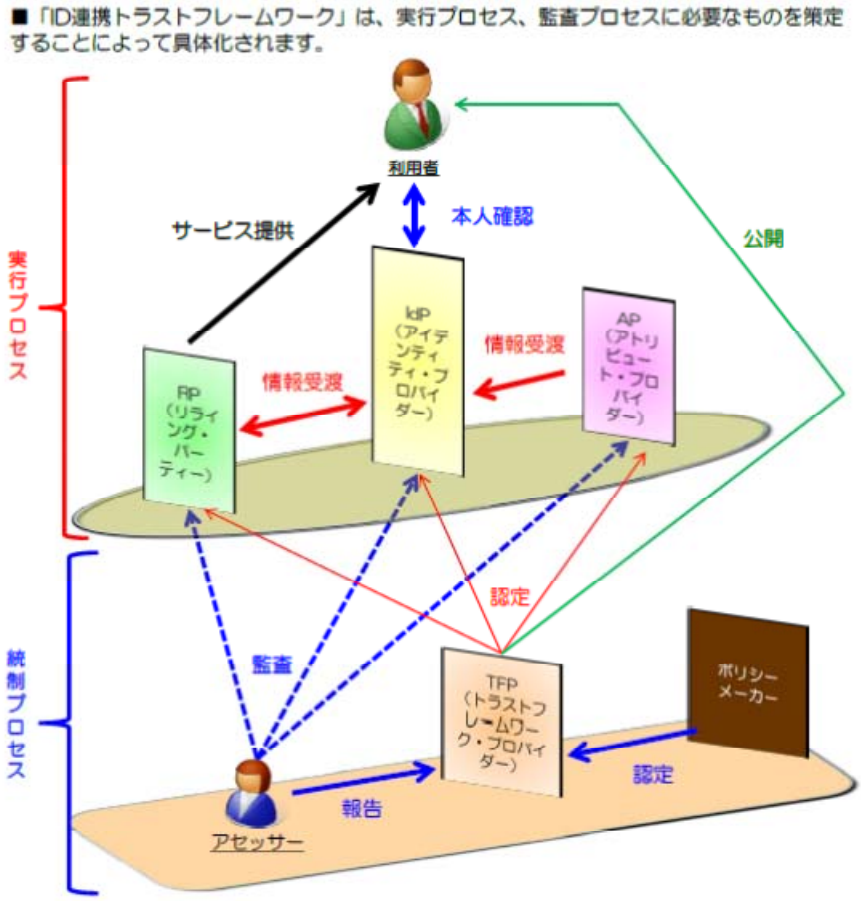


図１－１１　ID 連携トラストフレームワークの具体化に必要なもの [6)]

１．１．３　インフォメーションバンクコンソーシアム

（１）経緯

2013 年 9 月、東京大学空間情報科学研究センター(柴崎亮介教授)と慶應義塾大学大学院メディアデザイン研究科(砂原秀樹教授)が合同でインフォメーションバンクコンソーシアムを設立した。個人からパーソナル情報を預かり、活用し、個人に利益を還元する情報銀行実現のために必要な事項を検討し、その整備を推進する。2013 年 9 月に第一回シンポジウム、2015 年 1 月に第二回シンポジウムを実施した。

インフォメーションバンクコンソーシアム Web サイト　http://www.information-bank.net/

（２）特徴

情報銀行の考え方は、まず利用者が情報銀行に情報を預け、ビジネス利用等での条件を提示する。情報銀行は情報を匿名化した上で企業等に貸し出し、対価として利用料を徴収する。利用者は企業からパーソナライズされたサービスの提供やポイントの付与を受ける、というものである（図１－１２）[7]。

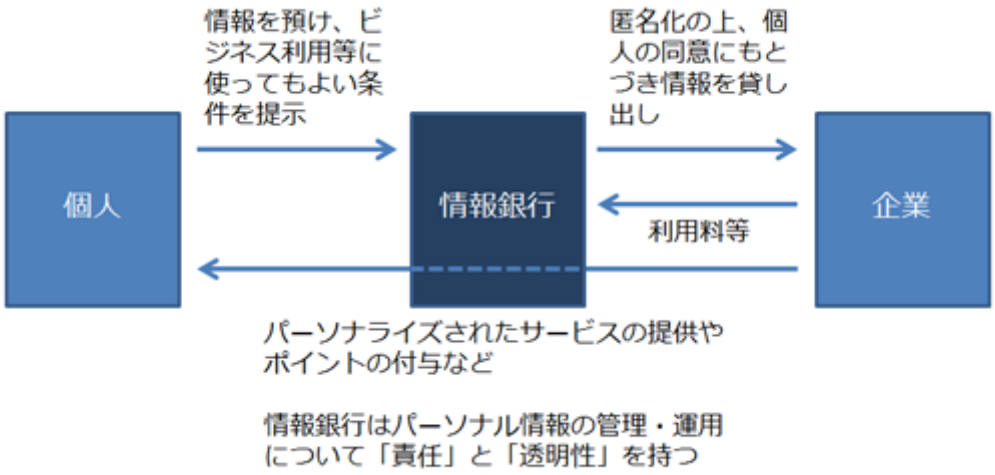


図１－１２　情報銀行とパーソナル情報の流れ [7]

インフォメーションバンクコンソーシアムは次の 3 つの WG を設けて活動している [8]。

・技術 WG
- 認証・暗号化・匿名化など、セキュリティや ID 管理技術を整理・組み合わせ、拡充する
- パーソナル情報の効率的な収集・交換技術を整理・拡充(標準化など)する

・データ応用 WG
- 実証実験に参加し、情報を信託する「預金者」、および実験参加企業を募り、「総合」パーソナル情報からの新たな価値創出の方法・ノウハウを開発、効果を例示する

・サービス開発、「預金」視覚化ツールなどのハッカソンなども

・社会受容性 WG

- 実際に情報銀行を法人として立ち上げ、情報を信託する利用者・企業、信託された情報を利用する企業等との契約をはじめとする運用体制・ルールに関する検討を具体的に行い、ひな形を示す
  - ・ATM の設置、預金通帳の発行などによるアウトリーチも
  - ・スマートシティなどの実証実験ともリンク ： 「スマートシティパスポート」
- また、情報銀行に対する監査・評価などの方法についてひな形を示す
- 以上を総合して「パーソナル情報の信託銀行」の成功例を積み上げ、社会的受容性・信頼感を確立する

１．１．４　集めないビッグデータコンソーシアム

（１）経緯

2014 年 10 月､東京大学大学院情報理工学系研究科ソーシャル ICT 研究センター(橋田浩一教授)は、個人ごとの分散管理により個人データを安全かつ効率的に流通させ、効果的に活用するための分散パーソナルデータストア(PDS)の普及を目的として､集めないビッグデータコンソーシアムを設立した[9)]。これに先立つ同年 7 月、分散 PDS の一種である Personal Life Repository(PLR)を利用した介護記録アプリケーションを開発し、山梨県の老人ホームで試験運用している[10)]。

（２）特徴

PLR は、個人のデータを本人が保管し、家族や友人や事業者と安全に共有して活用するためのスマートフォン用のアプリとして開発されている。個人が本人のデータを暗号化して Google Drive や Dropbox 等のパブリッククラウド等に格納する(図１－１３)。

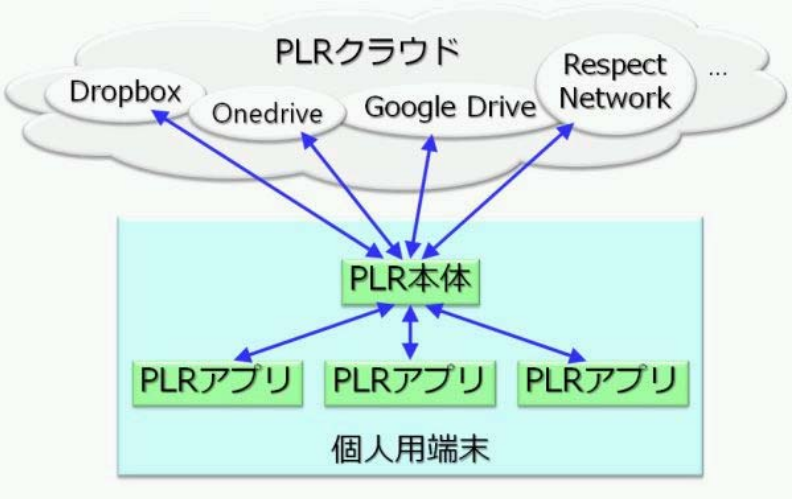


図１－１３　PLR の構成[11)]

PDS には事業者が多数の個人データを管理する集中型の PDS と、各個人のデータを本人が管理する分散型の PDS があるが、無償のパブリッククラウドストレージを利用することなどにより、集中型 PDS よりも分散型 PDS のほうがはるかに安価かつ安全で利便性も高い、としている[11]。

１．１．５　Privacy Policy Manager

（１）経緯

Privacy Policy Manager(PPM)は利用者のポリシーに基づいたパーソナル情報の流通を実現するための仕組みで、株式会社 KDDI 研究所が研究開発を進めている。2012 年度および 2013 年度の NEDO「都市情報利活用基盤構築プロジェクト」にて基本機能のプロトタイプが開発された[12]。開発したプロトタイプシステムを用いて、一般の被験者を対象としたアンケートにより受容性評価を実施した。2014 年 3 月、経済産業省が主催するパーソナルデータの利活用に関する事前相談評価試行において、ベストプラクティスの一つに選定された[13]。

（２）特徴

利用者がパーソナルデータを事業者に提供するサービスでは、サービスごとに規約(約款)が提示され、利用者は都度合意する。これはサービスが追加されるたびに行う必要があり、利用者にとっては煩わしいだけではなく、規約がほとんど読まれない、提供したパーソナルデータがどのように利用されているのか不安になる、などの課題がある。

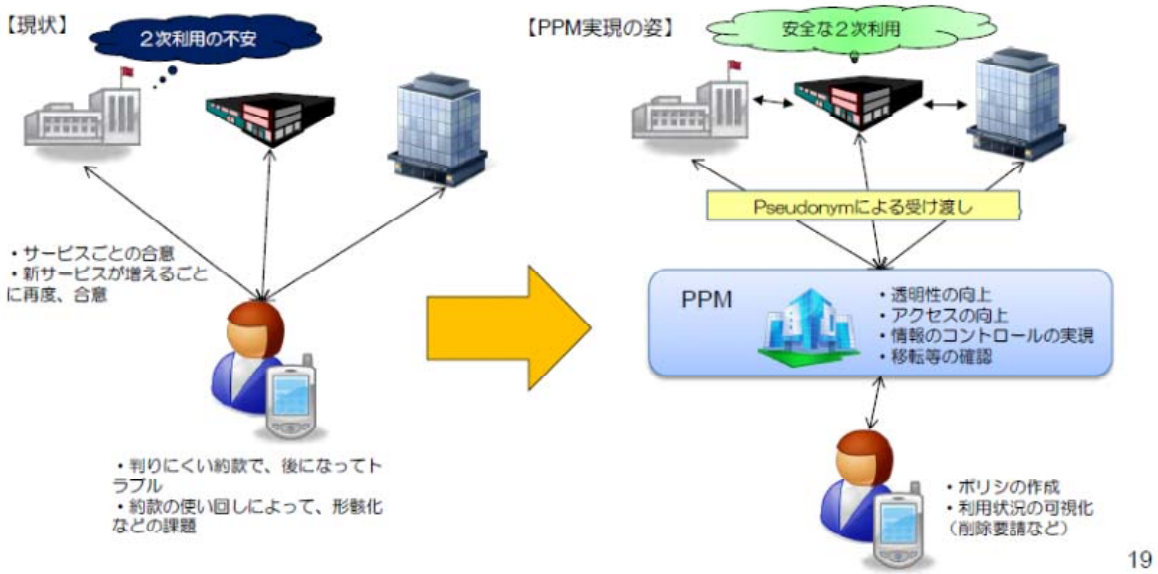


図１－１４　PPM の概要[14]

これに対して PPM では以下の機能により利用者好みに設定をカスタマイズし、利用者が安心してデータを提供できるようにする[14]。

①設定に応じてサービス利用前に提示される規約の表示をカスタマイズ(図１－１５)

（例） [詳細表示]サービス規約を使用する情報項目ごとに並べて個々に使用目的を表示
[簡易表示]情報項目と使用目的をそれぞれまとめて表示

②出したパーソナル情報に応じたサービスの提供

（例） 「性別」「位置情報」などの情報提供を許可するとお勧めの商品が変わる、周辺の店舗情報が地図で表示される、など

③設定に応じて事業者に提出する情報をコントロール

（例） PPM で位置情報の提供を拒否していた場合は、位置情報利用サービス提供事業者からの情報提供要求に対して PPM が拒否する

④事業者に提出した情報のログを後で確認

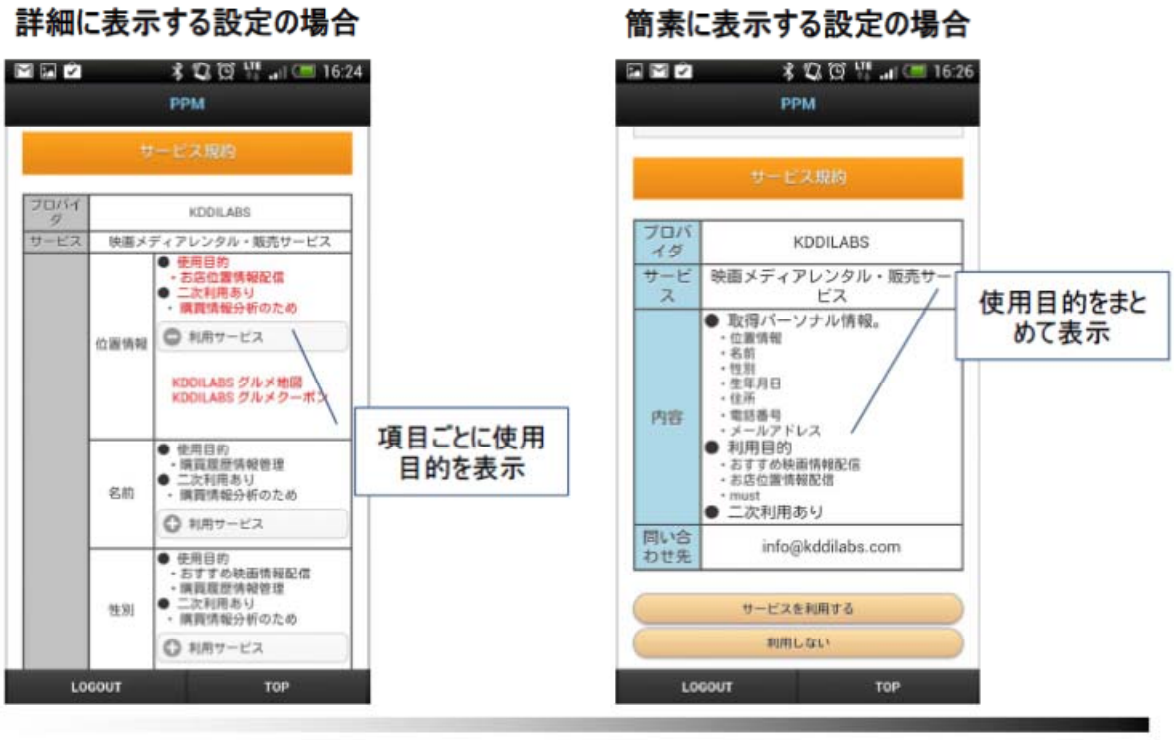


図１－１５　設定に応じて規約の表示をカスタマイズする例 [14)]

１．２　海外の状況

国内の状況はパーソナルデータの利活用に絞ってリストアップしたが、本来パーソナルデータの利活用とプライバシー保護は表裏一体である。海外の状況についてはプライバシー保護に関する代表的な取り組みについて紹介し、続いてパーソナルデータに関する事例に言及する。

１．２．１　Privacy by Design

（１）経緯

1995 年、カナダ・オンタリオ州のプライバシー・コミッショナーである Ann Cavoukian 博士が提唱したプライバシー保護の原則である。2010 年 10 月、イスラエルで開催された第 32 回データ保護・プライバシー・コミッショナー国際会議で「基本的なプライバシー保護の不可欠な要素」であることが決議され、各国のプライバシー保護の考え方に広く採用されている。日本では、2012 年 8 月に総務省が公表したスマートフォンプライバシーイニシアティブに盛り込まれている[15)]。

Privay by Design Web サイト　http://www.privacybydesign.ca/

（２）特徴

7 つの基本原則からなる。Privacy by Design の Web サイト上にて 37 種類の言語版で入手できる(2015 年 1 月時点)。以下に英文原則、日本語訳、説明(抜粋)を列記する。

The 7 Foundational Principles of Privacy by Design

1. Proactive not Reactive; Preventative not Remedial

(1. 事後的ではなく事前的; 救済的でなく予防的)

受け身で対応するというよりむしろ先見的に対応することが特徴である。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である。

2. Privacy as the Default Setting

(2. 初期設定としてのプライバシー)

所定の IT システムまたはビジネス・プラクティスにおいて、個人データが自動的に保護されることを確保することによって、最大級のプライバシー保護を提供することを目指す。

3. Privacy Embedded into Design

(3. デザインに組み込まれるプライバシー)

Privacy by Design は、IT システムおよびビジネス・プラクティスのデザインおよび構造に組み込まれ、事後的に付加的に追加するものではない。

4. Full Functionality – Positive-Sum, not Zero-Sum

(4. 全機能的 – ゼロサムではなくポジティブサム)

プライバシーとセキュリティの両方とも持つことが可能であることを実証し、プライバシー対セキュリティのような誤った二分法を回避する。

5. End-to-End Security – Full Lifecycle Protection

(5. 最初から最後までのセキュリティ - すべてのライフサイクルを保護)

強力なセキュリティ対策を最初から最後まで施すことにより、すべてのデータを安全に保持し、プロセスの終了時には確実に破棄しなければならない。

6. Visibility and Transparency - Keep it Open

(6. 可視性と透明性 - 公開の維持)

どのようなビジネス・プラクティスまたは技術が関係しようとも、独立した検証を受けることを条件に、関係者に対して機能することを保証する。

7. Respect for User Privacy - Keep it User-Centric

(7. 利用者のプライバシーの尊重 - 利用者中心主義を維持する)

設計者および管理者に対し、強力なプライバシー標準、適切な通知、権限付与の簡単なオプションを提供することにより、個人の利益を最大限に維持することを求める。

１．２．２　消費者プライバシー権利章典(米)

（１）経緯

2012 年 2 月、米国ホワイトハウスは大統領名で、政策大綱「ネットワーク化された社会における消費者データプライバシー」を発表 [16]。この中で消費者プライバシー権利章典(Consumer Privacy Bill of Right)の草案を公開した。

（２）特徴

消費者プライバシー権利章典は次の 7 項目からなる(下記和訳は参考文献 17)参照)。

1. 個人によるコントロール

   消費者は、事業者が収集する自身の個人データをコントロールする権利を持つ

2. 透明性

   消費者は、事業者によるプライバシーとセキュリティの順守に関して、分かりやすい手順で情報を得る権利を持つ

3. 背景情報の尊重

   消費者は、消費者が提供した背景情報に沿って、事業者が個人のデータを収集、利用、開示することを期待する権利を持つ

4. セキュリティ

   消費者は、個人のデータが安全かつ責任を持って扱われる権利を持つ

5. アクセスと正確性

   消費者はセンシティブなデータや、不正確なデータが消費者にリスクを与えるようなケースにおいて、適切な方法で利便性の高いフォーマットのパーソナルデータにアクセス、修正できる権利を持つ

6. 適切な範囲の収集

   消費者は、事業者が収集、保存できる個人のデータを適切な範囲に限定する権利を持つ

7. 説明責任

消費者は、事業者によって個人のデータが、消費者プライバシー権利章典に従って適切に扱われる権利を持つ

１．２．３　データ保護規則案（EU）

（１）経緯

2012 年 1 月、欧州委員会はデータ保護規則(General Data Protection Regulation)(案)を公表した[18)]。これは 1995 年に作成したデータ保護指令の見直し案である。その後、2013 年の欧州議会の修正案で規制が強化された(罰金等)。

（２）特徴

個人の権利の強化として、忘却される権利(個人に係るデータが不必要になった場合、データの消去を求められる)、同意を撤回する権利、データポータビリティの権利(個人に係るデータを事業者から事業者へと移行できる権利)等を新たに規定した。規則に違反した場合は、1 億ユーロまたは国際的売上の 5%を上限に罰金が課せられる。

１．２．４　プライバシーガイドライン(OECD)

（１）経緯

2013 年 7 月、OECD はプライバシーガイドラインを改定した[19)]。これは 1980 年に作成・採択したガイドラインを 33 年ぶりに改定したものである。日本では 1988 年に行政機関個人保護法を制定、2003 年に個人情報保護法が制定されるなど、OECD プライバシーガイドラインは日本の個人情報保護法制の基礎をなしている[20)]。

（２）特徴

1980 年ガイドラインでは次の 8 原則を定めている。

①収集制限の原則（Collection Limitation Principle）
②データの質の原則（Data Quality Principle）
③目的特定化の原則（Purpose Specification Principle）
④使用制限の原則（Use Limitation Principle）
⑤安全保護措置の原則（Security Safeguard Principle）
⑥公開の原則（Openness Principle）
⑦個人参加の原則（Individual Participation Principle）
⑧責任の原則（Accountability Principle）

これに対してさらにデータ管理者の責任として

a)プライバシーマネジメントプログラムの構築
b)プライバシーマネジメントプログラムが適切に実施されていることの証明
c)重大なセキュリティ侵害があった場合、必要に応じてプライバシー執行機関に通知

などを追加している。また、国際的な相互運用についても記述している。

１．２．５　midata(英)

（１）経緯

2011年4月、英国Department for Business Innovarion & Skills(BIS)が発表したPolicy Paper[21]の中で、消費者が企業によって保持されている自身のパーソナルデータにアクセス・利用できるようにする「mydata」プログラムを紹介した(後にmidataと改称)。2013年7月にはこれを発展させ、midata innovation lab(miL)を発足した。
(注：miL Webサイト(http://www.midatalab.org.uk/)については2015年2月時点では参照できなくなっている)

（２）特徴

企業が保有しているパーソナルデータを消費者が参照するだけでなくダウンロードして第三者に活用を委ねることができれば、例えば携帯電話の最適な料金プランを見つけることも容易になる。ユーティリティなどにも同様のメリットがある（図１－１６）。これが消費者のよりよい選択や取引につながり、経済成長を促すことになる。

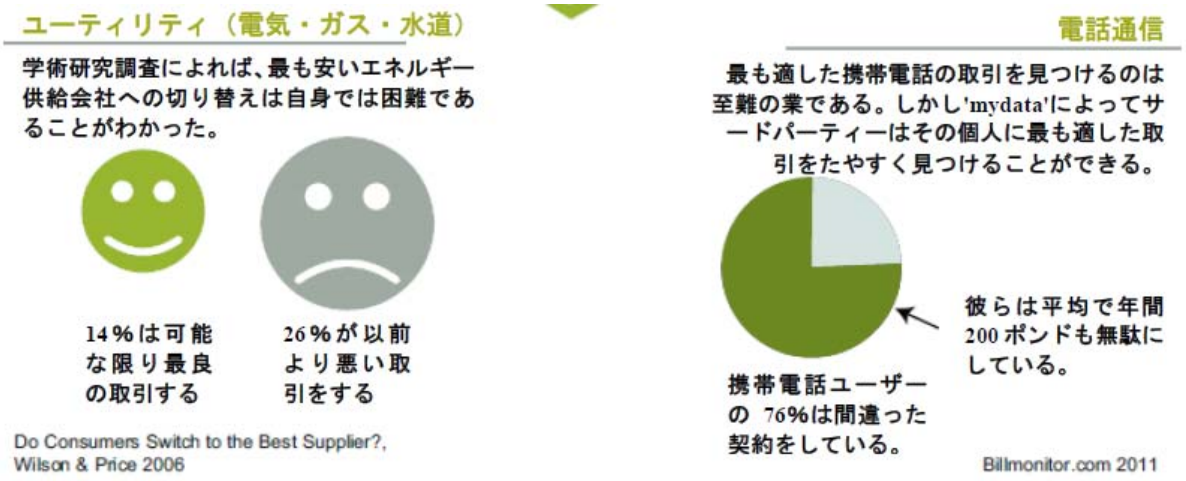


図１－１６　パーソナルデータの利用メリット(例)[22]
(参考文献22)に含まれる参考文献21)の仮日本語訳から一部抜粋)

midata は、企業や組織が持つ消費者のパーソナルデータを消費者がダウンロード、管理、活用するために英国 BIS 主導で消費者団体と先進企業が協力してすすめるプログラムの名称である。2011 年 3 月に始まり、2013 年 7 月には 25 以上の英国の組織や企業が参加して消費者保護のプロトタイプを開発する miL を発足した。

miL には 1,000 人の消費者ボランティアがあり、彼らのパーソナルデータは安全なパーソナルデータストア(PDS)に保管される。参加組織はこのデータにアクセスして様々なサービスの開発を行う。消費者は評価をフィードバックする。

アプリケーションの例としては次のものがあげられている

・MI Energy（単純なインタフェースでエネルギープラン最適化）
・MI Finance（債務返済計画の最適化）
・MI Relative Calm（高齢者の見守り; 寝起き、室温、消費など生活全般）
・MI Health（健康増進）
・MI Move（引越し時に必要となる複数の組織への連絡支援）

また具体例として、自動車走行距離に応じた保険のプレミア、現在位置に対応したジョギング目標作成など多数の事例が掲載されている。

１．２．６　MyData Initiatives（米）

（１）経緯

米国大統領府は 2012 年から Presidential Innovation Fellows（PIF：大統領府技術革新フェロー)プログラムを実施している[23)]。2013 年 1 月、Round2 として 9 分野を特定、その中で MyData Initiatives を募集・実施している[24)]。

（２）特徴

PIF の目的は民間や大学等から優秀なイノベータをフェローとして招聘し、政府の課題を迅速に解決することにある。オープンデータ関連では 2012 年のテーマとして、Open Data Initiative (政府機関が保有するデータの積極的な公開)、Blue Button for America（医療記録情報への簡便なアクセスを提供)があった。

2013 年は Open Data Initiative は継続、Blue Button for America についてはさらにエネルギーや教育などに対象分野を拡充して、MyData Initiatives とした。
(注 ： PIF の Web サイト上では MyData Initiatives について直接参照はできなくなっている)

１．２．７　Respect Network(米)

（１）経緯

2011 年、Respect Network 社は世界初のパーソナルクラウドネットワークを構築する目的で設立された。2013 年 6 月、米国で開催された Identity Relationship Management Summit にて、それまでの 50 のパートナーに加えて新たに 20 のパートナーを加え、世界初のグローバルプライベートクラウドネットワークのサービスを開始することを発表した[25)]。また、Respect Network 社は共著の論文発表等で Privacy by Design とも密接に連携している。

Respect Network 社 Web サイト　https://www.respectnetwork.com/

（２）特徴

[Respect Network の想定するビジネスモデル（図１－１７)]

1. アプリやビジネスサイトの広告を見たユーザーが Respect Connect ボタンを押す
2. ボタンを押した場所から Respect Network のパーソナルクラウドに接続される

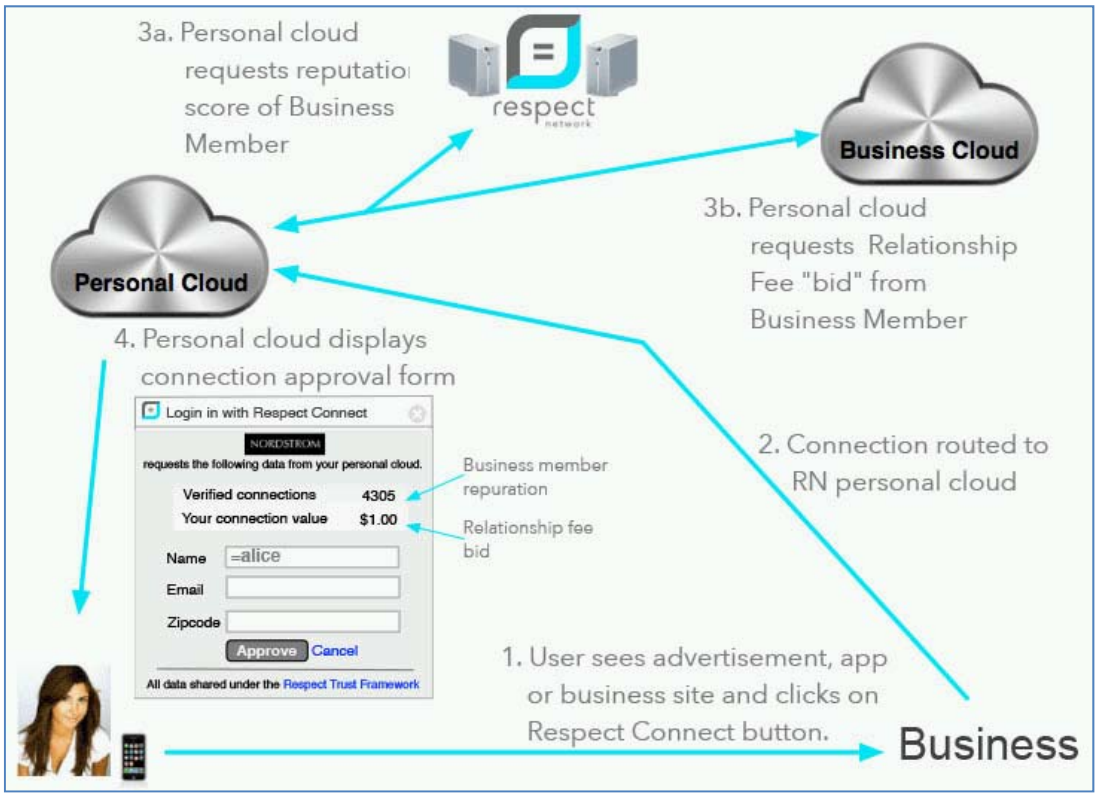
3a. パーソナルクラウドは Respect Network 社に対して対応するビジネスメンバーの評判スコアを問い合わせる

3b. パーソナルクラウドはビジネスメンバーに対して関係性手数料"bid"を問い合わせる

4. パーソナルクラウドは問い合わせで得られた情報を含む接続承認フォームを表示する
5. ユーザーが接続を承認する
6. パーソナルクラウドとビジネスクラウドの間で XDI 接続が生成される
7. ビジネスメンバーはパーソナルデータに対して適切なアクセスを得る
8. ビジネスメンバーは Respect Network 社に対して関係性手数料を月次で支払う
9. ユーザーは関係性手数料の 1/3 を受け取る

パーソナルデータを活用する企業からの手数料を徴収する点では「１．１．３　インフォメーションバンクコンソーシアム」も同様であるが、Respect Network 社はパーソナルクラウドやビジネスクラウドの提供はパートナー企業に委ね、自身は以下のサービスからなる Respect Network Infrastructure service を提供する。

- Connect Service
- Reputation Service
- Member Graph Service
- Discovery Service
- Billing Service
- Signaling Service（計画中）
- Dictionary Service（計画中）



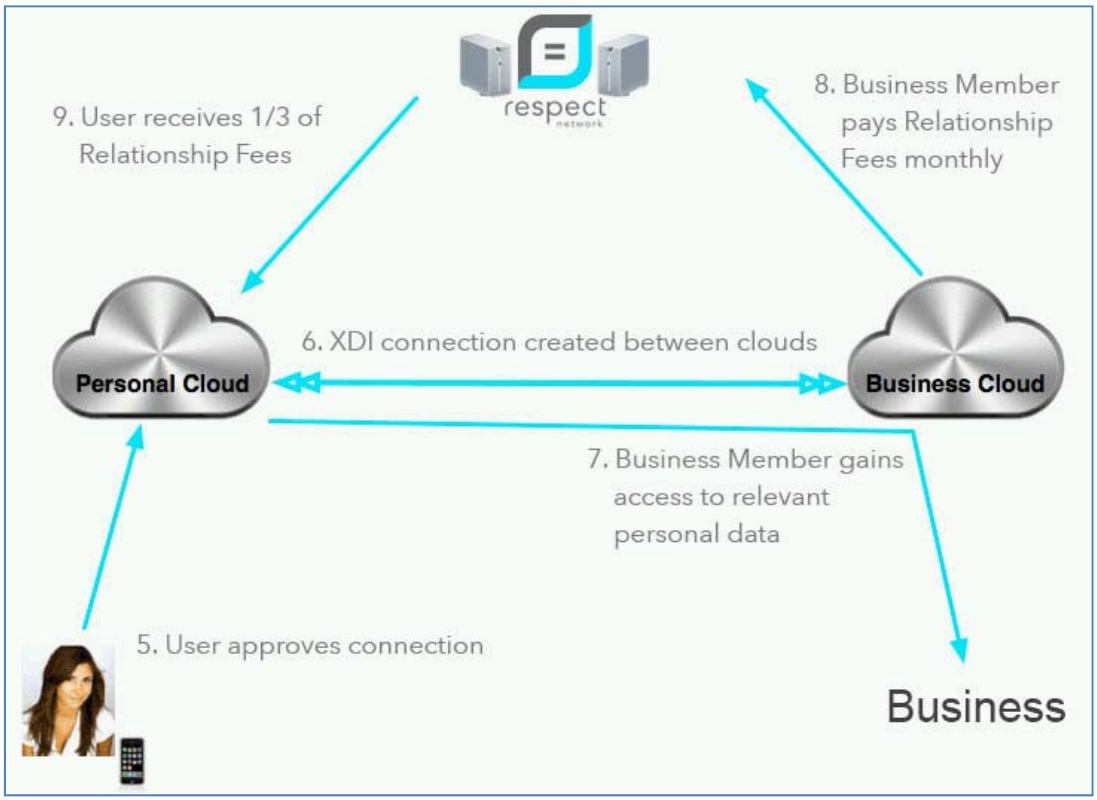


図１－１７　Respect Network の想定するビジネスモデル(同社 Web サイトより)

2013 年 12 月、Respect Network 社の Reed CEO は Privacy by Design の Cavoukian 博士と連名で発表した論文[26]の中で、プライバシーとビッグデータの「win-win」のシナリオを実現するものとしてビッグプライバシーを提唱した。ビッグプライバシーの定義はビッグデータの定義に対応するものとして、次のように紹介されている(日本語訳は参考文献 27)より)。

－ ビッグプライバシーはプライバシー・バイ・デザインを大規模適用したものである。すなわち、プライバシー・バイ・デザインの 7 原則を、個別の組織、アプリケーション、コンテキストにだけでなく、ネットワーク、バリュー・チェーン、生態系全体、特にビッグデータの作成・利用をするものに、適用したものである。

ビッグプライバシーのゴールは、パーソナルデータの組織的保護と、それらがどのようにして集められ利用されるかと言うことに関する過激なまでの個人によるコントロールである。この過激なコントロールは、「情報自決権」－ ドイツ憲法に銘記されている、自らの情報の運命を決定する個人の能力に関連する権利 － の体現である。

これは、ビッグデータを処理するネットワーク、バリューチェーン、生態系がプライバシー・バイ・デザインを系全体に適用し、同意した個人が自らのパーソナル情報を使って便益の一部を刈り取ることを可能にすることに通じ、全人口に対してプライバシーが尊重されることを保証し可能にしなければならないことを意味する。 －

同論文では、ビッグプライバシーのアーキテクチャーの紹介、これが OASIS XDI[28]と Respect Network によってどのように実装されているかが紹介されている。

１．３　本研究の狙い

（１）国内、海外の状況

本章では国内、海外の状況について概観した。パーソナルデータの利活用とプライバシー保護にフォーカスした形となったが、総じて以下の動向と理解する。

まず国内については、個人情報保護法の改正案が国会提出される予定である（１．１．１）。これまではプライバシーの保護に重点が置かれていたが、オープンデータ/ビッグデータ利活用の観点からパーソナルデータの利活用に道を開くことを念頭に置いている。「匿名加工」「本人同意を得ない第三者提供」「利用目的制限の緩和」などが骨子として含まれているが、今後予定される国会審議を注意深く見守る必要がある。産業競争力強化の観点からは、諸外国の取り組みとの調和・整合性にも留意して頂くことを期待する。

関連する取り組み（１．１．２～１．１．５）については府省主導のもの、大学や民間主体のものなど様々あるが、基本的には諸外国で先行している取り組みを踏まえて技術開発やビジネスモデルの構築に取り組もうとしているものである。前記法制度の改正と同期して、技術開発等についても国内のレベルアップが期待される。

海外については、プライバシーについての基本原則やガイドライン、規則案等を列挙した（１．２．１～１．２．４）。共通しているのは個人によるパーソナルデータの管理・権限強化であるが、これを後付けの機能ではなく全体の設計段階から組み込むことを提唱しているのがプライバシー・バイ・デザインである。続いて取り上げた先進事例はパーソナルデータの利活用を直接的に個人へのメリットとして還元するもので、英米における政府主導のもの（１．２．５～１．２．６）と民間の代表例（１．２．７）を列挙した。その他外国における民間でのパーソナルデータの利活用事例については参考文献 29)の他、多数の報告書が公開されている。

（２）本研究の狙い

ビッグプライバシー（１．２．７）としても言及されているように、ビックデータとプライバシーは「win-win」の関係を構築するのがあるべき姿である。パーソナルデータの利活用についてもパーソナルデータを提供する利用者に直接的なメリットが還元できるべきであり、これを目指す様々なアプローチがとられている。

一方、パーソナルデータの利活用については利用者の意図しない利活用がなされ、その結果社会問題化する事例も少なくない。本章の冒頭でも紹介したように、パーソナルデータの利活用には期待より不安が大きく、その理由は目的外利用や説明不足となっている。すなわち、パーソナルデータの利活用については一般に国民のコンセンサスが形成されているとは言いがたい。

国民のコンセンサスを形成するためには法制度の整備や技術開発に加えて、わかりやすい事例に基づいた理解が必要である。自らのパーソナルデータを提供することでどのようなメリットが

得られるのか、その過程の中でプライバシーはどのように守られるのか、これらを具体的な事例の中で理解することでデータ活用に対する国民のコンセンサスの壁を取り払うことができる。コンセンサスの壁の存在により、実際の市場規模が一定レベル以下に留まっているのに対して、壁を取り払うことでさらなる市場の拡大が期待できる(図１－１８)。

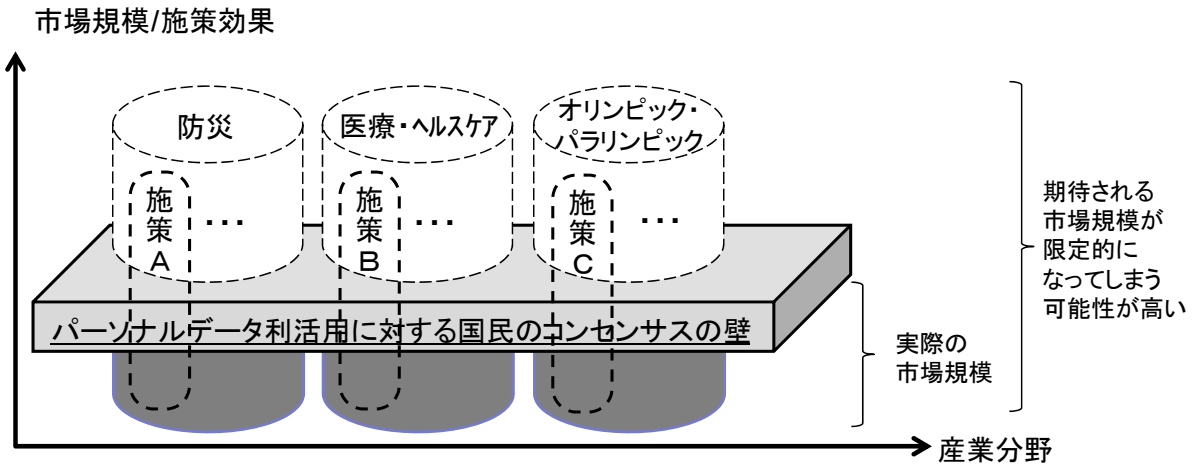


図１－１８　本研究のスコープ　(本研究会中間報告(2014 年 11 月 5 日)より※一部語句修正)

以降の章では、まず国内外の状況を踏まえて、パーソナルデータの利活用と保護を両立させるモデルの提案を行う。さらに、具体的なケースでどのようなメリットや課題があるのかを検討する。具体的なケースとしては利用者にとってパーソナルデータの提供に直接的なメリットが得られると想定される分野として「防災」「医療・ヘルスケア」「オリンピック・パラリンピック」を設定する。そしてパーソナルデータの利活用に対する課題解決に向けた提言を行う。

なお、ケースの具体化にあたり、オリンピック・パラリンピック開催における重要なセキュリティインフラとなる監視カメラについては、1)データの提供に本人の同意がとれない、2)不特定多数の個人情報を記録する、3)匿名加工の技法が確立していない、などの課題がある。また、医療・ヘルスケア分野では、本人が遺伝情報を提供してしまうことにより、4)親族の個人情報を推測できる情報までも提供してしまう、などの課題も存在する。これら個別に深い議論を要する問題については本研究会の検討対象外としている。

[参考文献、Web サイト]

1) 日立製作所, "日立の「オープンデータソリューションを活用した内閣官房のデータカタログサイト「DATA.GO.JP」が稼動開始」", (2014/9)
http://www.hitachi.co.jp/New/cnews/month/2014/09/0930a.html

2) 日立製作所, "第二回　ビッグデータで取り扱う生活者情報に関する意識調査」を日立と博報堂が実施", (2014/8)
http://www.hitachi.co.jp/New/cnews/month/2014/08/0804.html

3) EMC, "EMC Privacy Index", (2014/2), http://japan.emc.com/campaign/privacy-index/index.htm

4) IT 総合戦略本部, "パーソナルデータに関する検討会　決定等",
http://www.kantei.go.jp/jp/singi/it2/pd/

5) IT 総合戦略本部, "決定等",
http://www.kantei.go.jp/jp/singi/it2/decision.html

6) 経済産業省, "ID 連携トラストフレームワーク",
http://www.meti.go.jp/policy/it_policy/id_renkei/index.html

7) 日経 BizGate, "パーソナル情報の安心利用へ、「情報銀行」の可能性", (2013/10)
http://bizgate.nikkei.co.jp/article/71475516.html

8) atmarkIT, "「情報銀行コンソーシアム」設立へ　-ビッグデータから、ディープデータ時代に-", (2013/10)
http://www.atmarkit.co.jp/ait/articles/1310/02/news133.html

9) 東京大学大学院情報理工学系研究科ソーシャル ICT 研究センター",「集めないビッグデータコンソーシアム」キックオフシンポジウム", (2014/10)
http://www.sict.i.u-tokyo.ac.jp/news/dbd20141015/

10) 東京大学記者会見, "東京大学大学院情報理工学系研究科付属ソーシャル ICT 研究センターが次世代ヘルスケアサービスの運用開始 - ヘルスケアにおけるビッグデータの個人分散管理による B2C サービスの向上-", (2014/7)
http://www.u-tokyo.ac.jp/public/public01_260710_02_j.html

11)WirelessWire News, "自律分散協調の思想　個人データの分散管理", (2014/5)
http://wirelesswire.jp/k_hasida/

12)NEDO 都市情報利活用基盤構築プロジェクト, "都市空間情報の利活用に向けた取り組みについて", (2013/11)
http://g-contents.jp/2013/data/2_kddi_.pdf

13)KDDI 研究所, "KDDI 研究所が研究開発を進める PPM(Privacy Policy Manager)が、経済産業省主催のパーソナルデータの利活用に関する事前相談評価試行において、ベストプラクティスに選ばれました", (2014/3)
http://www.kddilabs.jp/news/20140327.html

14)KDDI 総研(高崎春夫), "プライバシー保護と利活用のバランスを目指すプライバシーポリシーマネージャ(PPM)の開発", (2014/4)
http://www.jaist.ac.jp/project/NLP_Portal/doc/jeita/JEITA_symposium_2014_takasaki.pdf

15)総務省, "「スマートフォン プライバシー イニシアティブ -利用者情報の適正な取扱いとリ

テラシー向上による新時代イノベーション-」の公表", (2012/8)
http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html
16) THE WHITE HOUSE, "CONSUMER DATA PRIVACY IN A NETWORKED WORLD", (2012/2)
http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
17) 日本経済新聞, "米国「プライバシー権利章典」の衝撃", (2012/5)
http://www.nikkei.com/article/DGXNASFK22010_S2A520C1000000/
18) EUROPEAN COMMISION, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protecion of individuals with regard to the processing of personal data on the free movement of such data (General Data Protection Regulation)", (2012/1)
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
19) OECD, "Recommendation of the Council concerning Guidlines Governing the Protection of Privacy and Transborder Flows of Personal Data", (2013/7)
http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf
20) JIPDEC, "OECD プライバシーガイドライン 2013",
http://www.jipdec.or.jp/publications/oecd/2013/index.html
21) Department for Business, Innovation & Skills(UK), "Helping consumers make better choices and better deals", (2011/4)
https://www.gov.uk/government/publications/better-choices-better-deals-behavioural-insights-team-paper
22) JIPDEC, "個人情報の安心安全な管理に向けた社会制度・基盤の研究会報告書", (2012/3)
http://www.jipdec.or.jp/project/anshinkan/doc/2011/01.pdf
23) the WHITE HOUSE, "Presidential Innovation Fellows",
http://www.whitehouse.gov/innovationfellows/
24) IPA, "「米国オープンデータの動向調査」報告書の公開", (2013/9)
https://www.ipa.go.jp/about/research/20130830.html
25) Respect Network, "Respect Network Announces 20 New Founding Partners in Advance of Global Launch", (2014/6)
https://www.respectnetwork.com/wp-content/uploads/press-releases/IRM_SUMMIT_media_release_4-June-2014.pdf
26) Cavoukian, Reed, "Big Privacy: Bridging Big Data and the Personal Data Ecosystem Through Privacy by Design", (2013/12)
http://www.privacybydesign.ca/content/uploads/2013/12/pbd-big_privacy.pdf
27) アン・カブキアン、ドラモンド・リード, "ビッグプライバシー : プライバシー・バイ・デザインの適用によるビッグデータとパーソナル・データ・エコシステムの架け橋", (2013/12)
http://www.privacybydesign.ca/content/uploads/2013/12/Big-Privacy-JP-0519.pdf
28) OASIS, "OASIS XRI Data Interchange (XDI) TC",
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xdi
29) 経済産業省, "パーソナルデータに関する海外動向", (2012/11)
http://www.meti.go.jp/committee/kenkyukai/shoujo/it_yugo_forum_data_wg2/pdf/001_04_00.pdf

第２章　パーソナルデータの利活用と保護を両立させる仕組みのモデル

２．１　日本における課題の整理と対策の方向性

我が国では企業や個人が保有するパーソナルデータの利活用がなかなか進んでいない。前章で整理した国内外におけるパーソナルデータの現状に踏まえると、日本社会がパーソナルデータの利活用を進める上で課題となっている事項は、以下のように整理することができる。

課題（１）：パーソナルデータ利活用のための制度的環境・インフラ的環境が整っていない

- ・パーソナルデータの利活用ルールが明確でない
- ・パーソナルデータ利活用・流通のための共通的なインフラが整っていない

課題（２）：パーソナルデータ利活用に対して個人の不安感・不満感がある（図１－３、図１－４）

不安感

- ・「規約類に書かれているものと異なる目的で利活用される恐れがある」（目的外利用への不安）
- ・「利活用の目的や内容の説明が十分でない、分かりやすく公表されていない」（分かりやすい説明の欠如）
- ・「企業などが、プライバシーの保護対策に積極的でない」（保護対策不足）

不満感

- ・「利活用をされたくない場合に本人に拒否権がない」（自己情報コントロール権[1]の不在）

納得感の欠如

- ・「自分が得られるメリットが乏しい」（インセンティブの欠如）
- ・「利活用の目的や成果などに社会的な意義を感じない」（社会的意義の欠如）

これらの課題を解決するためには、個人の安心・信頼を確保しながらデータを利活用し、個人にも利益が還元されるようにするための仕組み、言わば個人・企業・社会にとって「三方良し」となるような仕組みとして、「日本版パーソナルデータ・エコシステム」の構築が急務である。

「日本版パーソナルデータ・エコシステム」の実現に向けて取るべき対策には以下のものが挙げられる。まず上記の課題（１）に対しては、主に国による「法令・ガイドライン等の整備」「パーソナルデータストア(PDS)推進のための政策」「トラストフレームワークの整備」「第三者機関による適正な監督」といった対策を通じた、パーソナルデータ利活用のための環境整備が求められる。

---

[1] 伝統的なプライバシー概念が他人に私的領域を干渉されないという消極的・受動的なものであるのに対し、1970 年代のコンピュータ・ネットワーク時代の到来とともに生じたのが、個人は政府や企業に対して自己に関する情報の訂正や利用停止を請求できるという積極的権利としての「自己情報コントロール権」の考え方である。

〇国による対策（例）

・法令・ガイドライン等の整備（１．１．１）
・PDS 推進のための政策（１．２．５、１．２．６）
・データ流通基盤としてのトラストフレームワークの整備（１．１．２、１．２．７）
・第三者機関による監督

次に課題（２）については、主に企業・組織による「個人の権利利益の保証」「企業の責任の遂行」「第三者機関による監督」といった対策を通じた、パーソナルデータ利活用に対する国民からのコンセンサス獲得が求められるだろう。

〇企業・組織による対策（例）

・ 個人の権利利益の保証
  - 個人への自己情報コントロール手段の提供（１．１．３、１．１．４）
    開示・訂正権、同意、オプトアウト　等
  - データポータビリティ
    一事業者によるデータ囲い込みを排し、個人による PDS 選択を容易化
  - 個人へのインセンティブ提供：
    金銭的対価、利便性向上、社会的意義 等
・ 企業の責任の遂行
  - 個人への分かりやすい説明の提供（１．１．５）
  - PIA／プライバシー・バイ・デザイン（１．２．１）
    (PIA ： Privacy Impact Assesment ； 特定個人情報保護評価)
  - 安全管理措置の強化、第三者認証の取得
  - 匿名加工情報（仮称）の利用（図１－８）
・ 第三者機関による監督
  - 事前相談、MSHP を通じた自主規制ルール策定 等
    (MSHP ： Multi StakeHolder Process ； 複数関係者のオープンなプロセス)

日本における現時点での個人情報保護法改正動向に鑑みると、これらの対策項目のうち、未だ十分な検討が行われておらず、今後の重点的な取組みが求められるのは、下線（図２－１中では太枠）を引いたような「自己情報コントロール手段の提供」や「(匿名加工情報等）データ流通の促進」に関連した項目である。

次節では、これらの対策項目を実装・実現することを通じて、データ利活用と保護を両立させるような、パーソナルデータ利活用のための日本型モデル（日本版パーソナルデータ・エコシステム）の在り方について検討する。

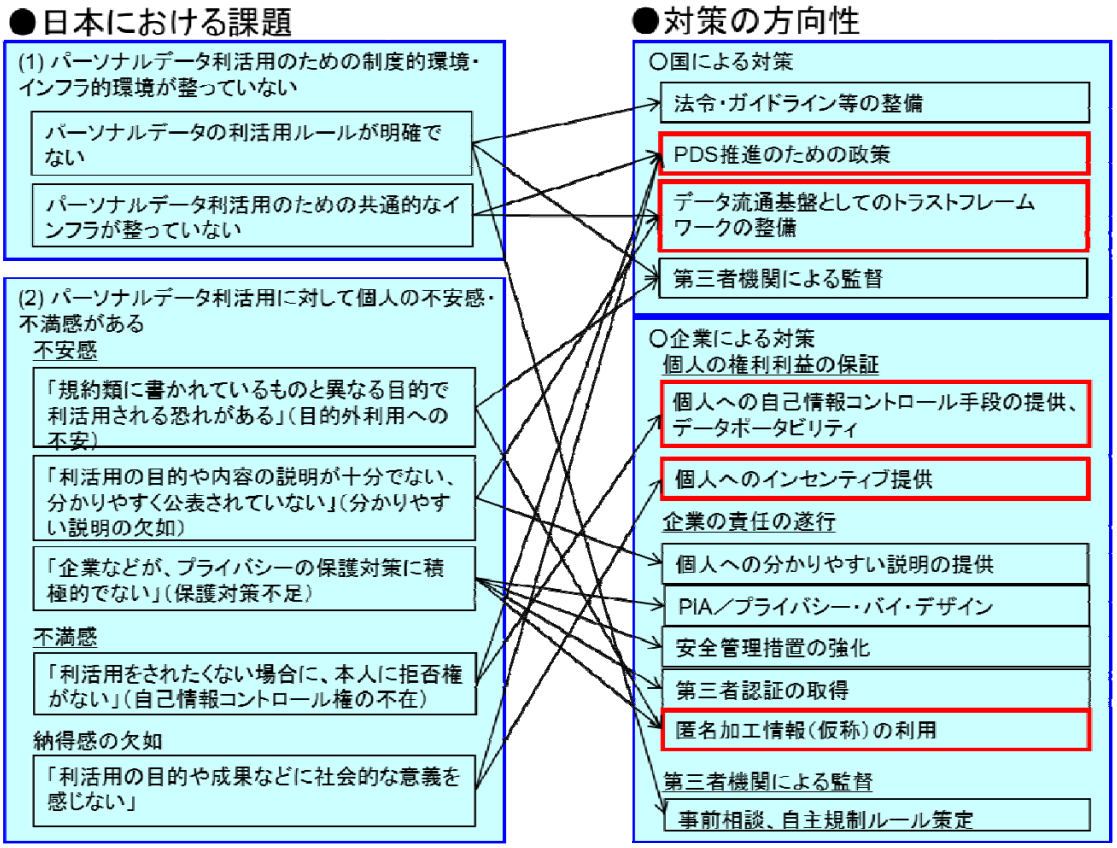


図２－１　日本におけるパーソナルデータ利活用の課題と対策の方向性

２．２　データ利活用と保護を両立させる日本型モデルの提示

日本型モデルを検討するに当たり、検討の軸として、パーソナルデータが利活用される条件・場面について階層化（パターン分け）を行い、それぞれの利活用パターンについて検討を行うこととする。

我が国でパーソナルデータが利活用される場面は、大きくは以下の 3 つに階層化（パターン分け）することができる[2]。

① 法令の規定による義務的な利活用／情報連携

- 行政手続き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(以下「番号法」と略す)、個人情報保護法等の規定に基づく
- 主に行政機関にとってメリット（行政事務の効率化）

[2] 個人情報の「利活用」には、一企業内部での二次利用（利用目的拡大）の側面と、異なる企業・組織で取得した情報の連携の側面とがあるが、本報告書では後者の側面を重点的に検討する。すなわち、異なる企業・組織で取得した情報の連携を円滑に行うことによって、個人や企業、行政機関、社会にベネフィットがもたらされるという立場から検討する。前者の側面については個人情報保護法改正法における利用目的変更手続きの明確化等で対処できるので本報告書では敢えて取り上げない。

② 本人の意思・同意に基づく利活用／情報連携（日本版パーソナルデータ・エコシステム）

- 官民連携（ワンストップサービス等）や民民連携（ex. 英国 midata）を実現
- PDS を用いる
- 主に個人にとってメリット（個人の権利利益の保証）

③ 本人同意に基づかない利活用／情報連携（匿名加工情報流通基盤）

- 改正個人情報保護法における匿名加工情報（個人特定性低減データ）を活用する
- 主に企業・社会にとってメリット（新サービス創出、社会的価値）

以下、各パターンごとにデータ利活用を促進するために何を行えばよいか、検討を行う。

２．２．１　法令の規定による義務的な利活用／情報連携（①）

（ａ）番号法等の規定により情報提供ネットワークシステム等を通じて義務的に行われる情報連携

（ｂ）個人情報保護法等の例外規定において「人の生命、身体又は財産の保護のために必要がある場合」等に該当する情報連携

の２つに大別される。（ａ）のイメージ図を図２－２に示す。

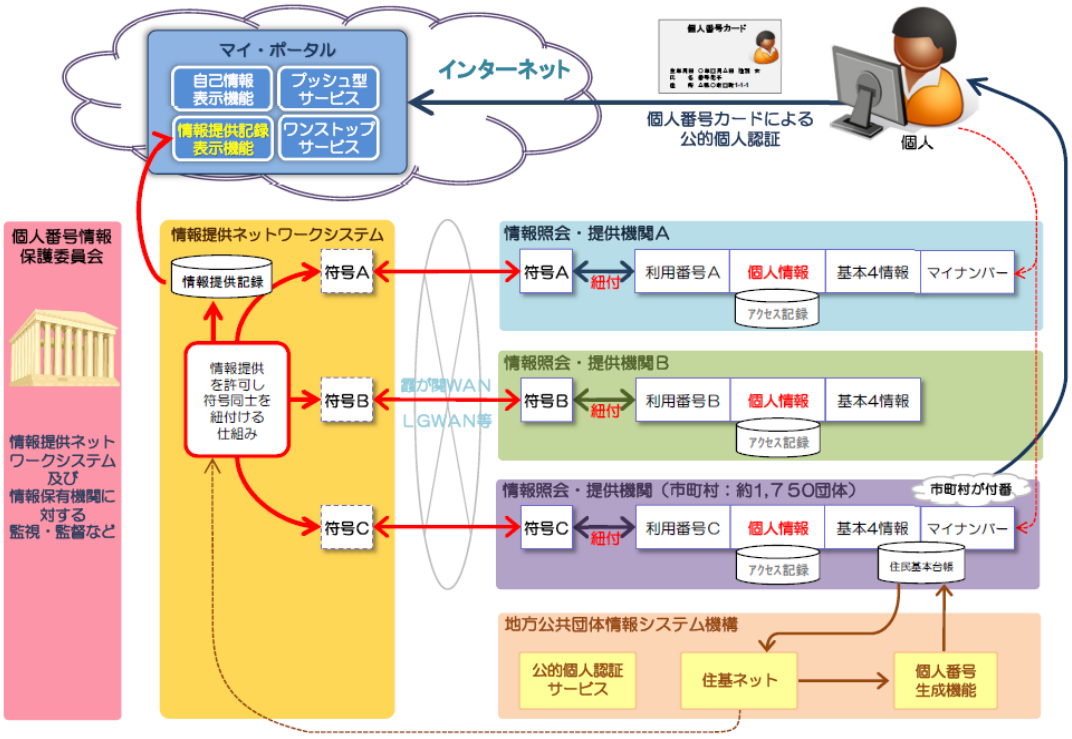


図２－２　番号制度における情報連携の概念図（出典：内閣官房資料）

（ａ）の番号法等の規定により義務的に行われる情報連携については、自己情報コントロール

権の保証（開示・訂正権）や、組織における安全管理措置、第三者機関による監督等が重要な対策となるが、番号法でその対策内容は規定されているので、本報告書では深堀りはしない。

（ｂ）の個人情報保護法等の例外規定における情報連携については、「人の生命、身体又は財産の保護のために必要がある場合」等の利活用であるため、事前の本人同意は必要ないが、組織がデータ主体である個人に対して、どのような場合に本人同意なく第三者提供を行うのかを分かりやすく明示することにより、適切な説明責任を果たすことが重要である。また、その前提として、どのような場合が「人の生命、身体又は財産の保護のために必要がある場合」等に該当するのかについては、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」や「金融分野における個人情報保護に関するガイドライン」において幾つかの事例が示されているが、緊急時等における情報利活用を阻害しないためにも、より多くの具体的事例を網羅的に把握したガイドラインを国が作成することが望まれる。

２．２．２　本人の意思・同意に基づく利活用／情報連携（②）

本報告書における検討の中心となるのが、このパターン②および③の利活用／情報連携である。

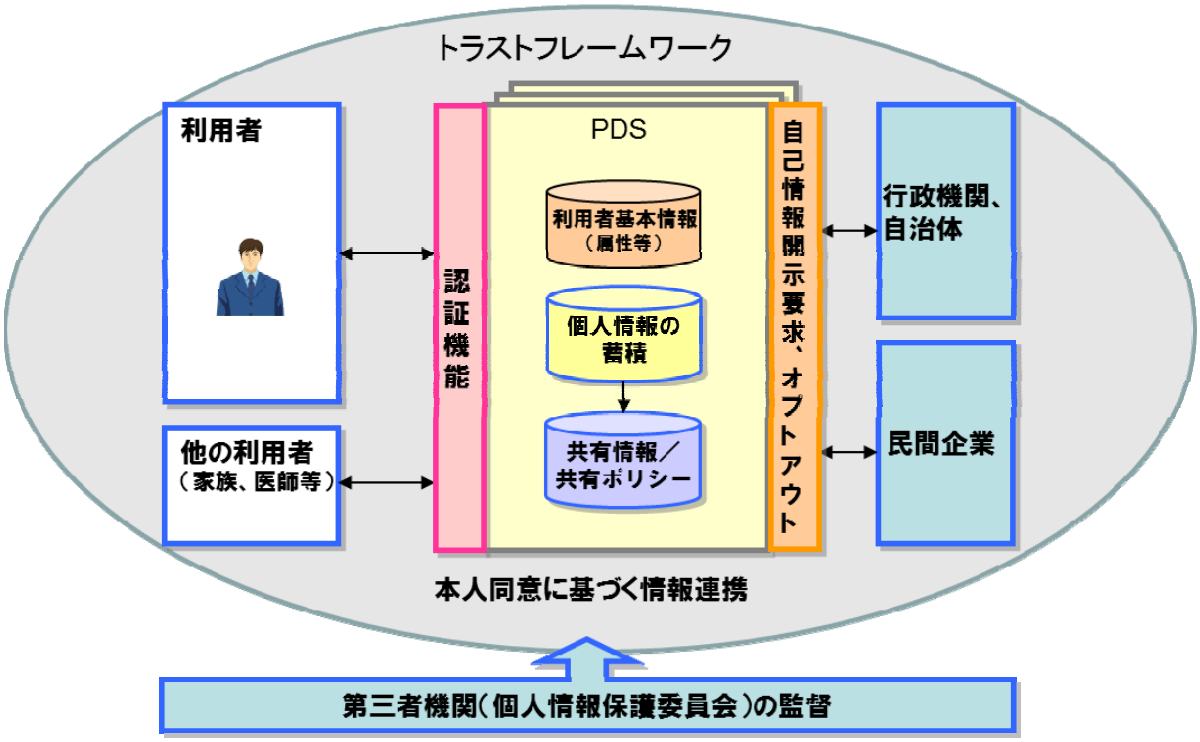


図２－３　本人の意思・同意に基づく利活用／情報連携（パーソナルデータ・エコシステム）

本人の意思・同意に基づくパーソナルデータの利活用／情報連携を行うためのシステムを仮に「日本版パーソナルデータ・エコシステム」と呼ぶ。前節で整理した対策の方向性より、日本版パーソナルデータ・エコシステムには、少なくとも以下のような機能要素が必要となろう。

（１）認証機能

（２）自己情報開示要求機能
（３）情報蓄積機能
（４）情報共有・活用機能
（５）オプトアウト機能
（６）データポータビリティ
（７）代理権限設定機能
（８）トラストフレームワーク

（１）認証機能

パーソナルデータストア PDS で蓄積・共有するデータは、医療健康データ（病名、常服薬、遺伝情報等）・所得証明書・金融口座利用明細などのセンシティブな個人データから、位置情報・通信履歴・購買履歴・マイレージ利用実績書・個人撮影の写真・日々のバイタルデータなど必ずしもセンシティブとは言えない個人データまで多岐に渡る。

このような PDS へのアクセスにあたっては、本人あるいは本人が許可した利用者であることを確認するためにアクセスする人を認証する機能が必要となる。また、PDS にデータを転送、あるいは PDS からデータを取得する際に、誰の PDS であるかの保証も必要となる。

これらの各手続きが、どの程度レベルの認証手段や保証手段を必要とするかを規定したガイドラインの策定や、システムの提供する認証手段の適正さを保証するためのトラストフレームワークの整備が重要となる。

たとえば、本人の利便性を優先して、現在の民間事業者が利用する ID＋パスワード程度の簡易な認証手段を選択したり、公的個人認証サービスのような高いセキュリティの認証手段を必須にする場合も出てくるであろう。その際は、官民で足並みを揃えて、PDS で閲覧等に供する個人データのセンシティブ度に応じた複層的な認証手段を用意する必要がある。

（２）自己情報開示要求機能

個人の意思によるデータ利活用を促進するためには、第一に、個人が企業・組織から自分のパーソナルデータをリアルタイムかつマシンリーダブルな形式で取得できる手段（「返却」してもらう手段）が必要である。

これにより、個人は企業・組織が保有する個人データを PDS 上で「自分のコントロール下に」蓄積することができ、自分で管理する個人データを他の企業（データ分析企業等）に開示して自分に合ったサービスのアドバイスを受けるといった利活用が可能となる。

本機能を実現するためには、個人データを保有する企業・組織がデータ（利用履歴等）を本人に「返却」する際に、当該データをスムーズに PDS に格納できるように、データ形式の標準化が鍵となる。個人に標準化データを「返却」する企業に対しては、JIS 等の標準化マークを付与するといった第三者認証の導入も考えられる。また、企業・組織におけるデータ形式標準化とデータ「返却」が進むまでは、Web スクレイピング技術[3]の活用も有効と考えられる。

また、企業・組織が足並みを揃えた取組みを行うように、国には PDS 推進のための積極的な旗振りが求められる。

[3] Web サイトから情報を抽出するコンピュータソフトウェア技術。

（３）情報蓄積機能

個人が企業・組織から「返却」してもらった自分の個人データを、自分が選択した PDS に蓄積し、本人の意思によって、医療・教育・就職・引越し・旅行・災害などの様々な生活場面で利活用できるようにすることが必要である。

PDS については、一事業者によるデータ囲い込みとそれによる個人の不利益を回避するために、同じ標準に基づいて複数事業者がサービス提供し、個人の側で自由に PDS を選択できることを保証する必要がある。そのためには、後述のデータポータビリティの考え方が重要である。

また、国は一事業者による囲い込みとならないよう、データ形式の標準化等を進めることにより、PDS サービス事業者間の競争を促進するべきである。

なお、IoT(Internet of Thing : モノのインターネット)の時代には、商品の送付先情報や購買履歴等の個人が明示的な意志で提供したデータよりも、ウェアラブル機器や各種センサー（GPS、カメラ、カードリーダー、車載器等）から自動的に取得され蓄積されていく動的データの方が膨大なものとなり、個人はもとより、企業・社会にとっても利用価値の高いデータとなる。その反面、個人の認識やコントロールの届かない範囲でのデータ利活用が拡大する恐れがある。このような観点からも、ウェアラブル機器等から取得されるデータを PDS で管理して「見える化」し、さらに個人に利益を還元するような取組みが重要となる。

（４）情報共有・活用機能

PDS が実際に「使われる」サービスとなるためには、個人に対して PDS 利用のインセンティブを与えることが必須の要素である。そのためには、PDS に蓄積した個人データを、他の利用者（家族、医師等）と共有したり、企業・組織（自治体等）に提供して様々なサービス（アドバイス・レコメンド、災害時の避難指示等）で活用できるような機能が必要である。

自分の個人データを他の利用者や企業・組織と共有・提供するにあたっては、「誰に（かかりつけ医、居住する自治体等)」「どのような利用目的で」「どのデータ」を開示するか、また「どのタイミングで（本人の個別許諾時、診察時、災害発生時等)」開示するかを「共有ポリシー」で予め設定できるようにする。

また、個人データ開示先の企業・組織におけるプライバシーポリシーは、個人が分かりやすく明確に理解できるものでないといけない。さらに、個人の利便性を高め、時間を節約するためには、個人の共有ポリシーと企業・組織のプライバシーポリシーを自動的にマッチングさせるといった機能も必要とされるかもしれない。このようなことを実現するためには、企業・組織におけるプライバシーポリシーの標準化と、マシンリーダブルな形での定義が必要となるだろう。

（５）オプトアウト機能

個人による自己情報コントロール手段の一つとして、一度許諾したデータ利用方法（共有、提供等）について、本人の意思でいつでも撤回できるような機能が必要である。

また、このように同意を後で撤回するためには、自分が同意した企業・組織の利用規約やプライバシーポリシーのコピーを「コンセントレシート」として PDS に保存しておき、その同意内容を確認することによって、一度許諾したデータ利用方法を撤回できるようにすることも考えられ

る。

（６）データポータビリティ

個人の選択の自由を保障する観点からは、個人が或る PDS に蓄積した自分のデータを、当該 PDS 事業者に妨害されることなく、他の PDS に円滑に移行できるようにすることが必要である。これにより、一事業者によるデータ囲い込みと、それによる個人の不利益（例えば、料金が高く、利便性が低い PDS サービスを使い続けないといけない等の不利益）を回避することが可能となる。そのためには、前述のように、PDS に蓄積するデータの標準化を推進することが重要である。

（７）代理権限設定機能

児童・高齢者・障害者等の情報弱者にとっては、本人の意思に基づく同意が難しかったり、PDS にアクセスする情報機器の操作に不慣れであるなど、家族等の代理人による権限の代理設定が必要となる場合が想定される。このような場合、PDS に代理権限を登録する機能が必要となる。

（８）トラストフレームワーク

個人データを扱う組織や企業、またデータ主体である個人を含め、どのようなルールでデータを扱うかに関して協定がなければ、個人データを安心・安全に提供することができない。利用者がいくら「共有ポリシー」を設定しても、個人データを提供する先の企業・組織が当該ポリシーに沿った取扱いをしてくれなければ、利用者は安心して PDS を利用することができない。個人データを渡す相手を「信頼できる」とみなすための仕組みをトラストフレームワークと呼ぶ。

PDS に蓄積された個人データが流通する先は、トラストフレームワーク内で、このような協定に賛同し、ルール通りに運営している組織や企業の間に限られる。なおルールには、一般的な利用規約から、技術的な共有ポリシーの表現方法やレベルの定義などが含まれる。

トラストフレームワークとして実施が進められているものに、ID 連携トラストフレームワークがある（１．１．２を参照のこと）。これは、企業・組織間で ID を連携する際に、ポリシーやルールを明確にし、信頼できる第三者機関によって、信頼できる組織を認定し、ID を連携して活用する仕組みである。

図２－４　ID 連携トラストフレームワークの概念図（出典：経済産業省資料）

２．２．３　本人同意に基づかない利活用／情報連携（③）

個人情報保護法改正の骨子案および大綱で示された「匿名加工情報（仮称）」（個人特定性低減データ）を用いたデータ利活用を促進することにより、民間企業による新たな価値創造のみならず、社会保障、健康医療、防災対策、交通・物流、都市計画、エネルギーコントロールといった社会的課題の解決にも役立てることが期待できる。

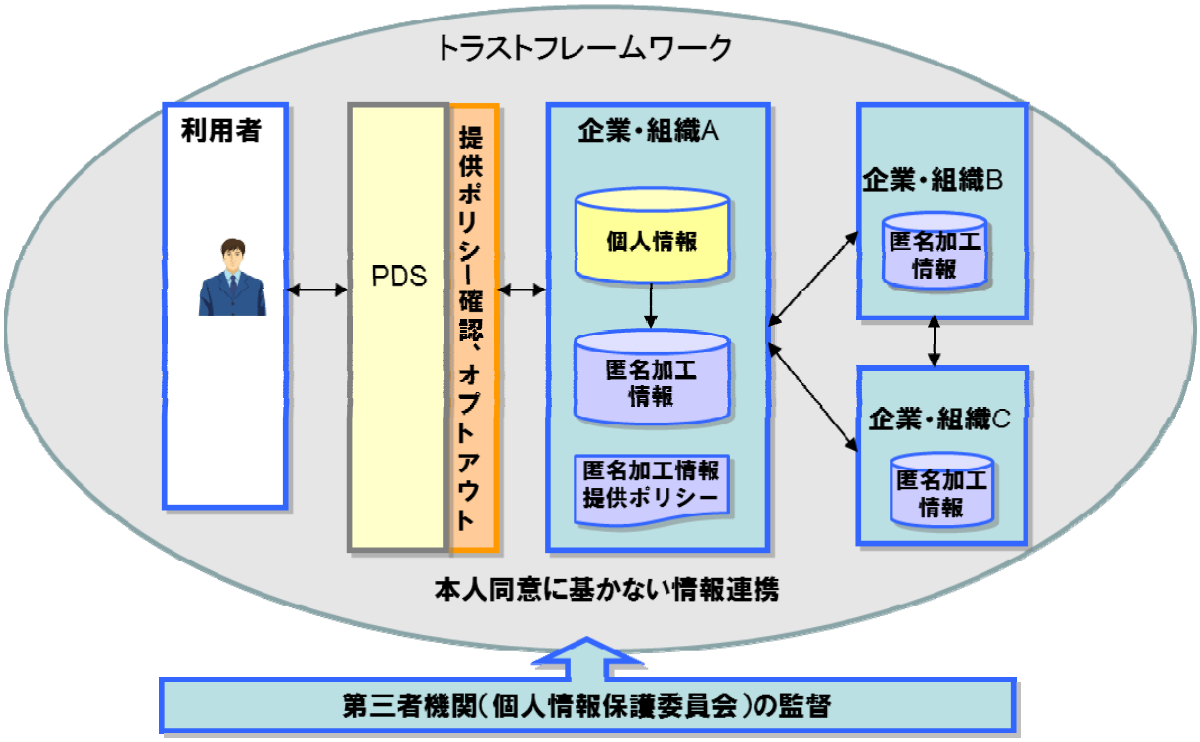


図２－５　本人同意に基づかない利活用／情報連携（匿名加工情報流通基盤）

本人同意に基づかないパーソナルデータの利活用／情報連携を行うためのシステムを仮に「匿名加工情報流通基盤」と呼ぶが、広い意味では前節の「日本版パーソナルデータ・エコシステム」の一部である。匿名加工情報流通基盤上で流通させる匿名加工情報については、企業の保有するデータであれば有償での情報提供が主体となるだろうし、公共機関が保有するデータであれば公益利用のために無償で提供を行うことも考えられる。

匿名加工情報流通基盤については、少なくとも以下のような機能要素が必要となろう。

（１）提供ポリシー確認機能
（２）オプトアウト機能
（３）トラストフレームワーク

（１）提供ポリシー確認機能

匿名加工情報は、本人同意なくデータを第三者提供できる仕組みであるため、個人が自分のデータの取扱いについてコントロールを利かせることが難しい。少なくとも、企業・組織は匿名加工情報を「どのように加工して」作成し、「どのようなデータ」を「どのような相手」に「どのよ

うな場合」に提供するのかについて、「提供ポリシー」という形で公表するべきである。
　個人はPDSを通じて、自分が個人データを開示するかもしれない企業・組織の「提供ポリシー」を簡便に確認することができ、提供ポリシーに賛同できない企業・組織に対しては自分のデータを開示しない等の選択を行えるようにするべきである。

（２）オプトアウト機能
　匿名加工情報では本人同意なき第三者提供が法的に認められることになるが、特定個人が再識別されないことが制度的にいかに担保されているとしても、個人にとっては自分起源のデータが歯止めなく流通している事実を「気持ち悪い」と感じる場合も多いと思われる。特に、匿名加工はされているものの統計化されていない「個票」が流通する場合には、そのような「気持ち悪さ」は強いであろう。
　個人による自己情報コントロールを尊重する立場からは、匿名加工情報であっても、個人が自分起源のデータの提供を希望しない場合には、元々のデータ開示先に対して、匿名加工情報の第三者提供の停止を請求できるようにするべきである。

（３）トラストフレームワーク
　２．２．２の説明を参照されたい。

第３章　具体的なケースでの検討

（１）目的

本章では一般論ではなく、具体的なケースを想定した上で、オープンデータとして活用可能なパーソナルデータを含めた運用の仕組み構築に向けた課題や施策を明らかにする。具体的なパーソナルデータの取り扱いに着目し、データを段階的・階層的に開示することへのインセンティブ（メリット）を明確にした上で、コンセンサスの形成につなげる。

（２）方法

総務省が 2014 年に実施した「ICT の進化がもたらす社会へのインパクトに関する調査研究」によると、個人がパーソナルデータを提供しても良いと考える利用目的は公共目的では

・大規模災害などの緊急時の場合や防災に関わる内容の場合

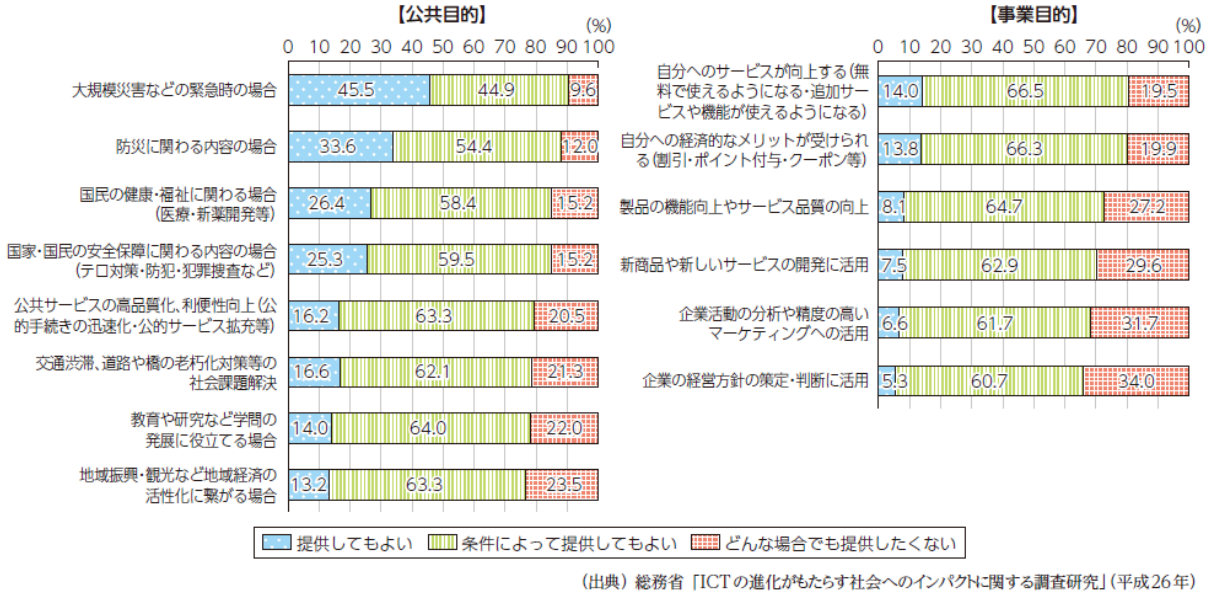
・国民の健康・福祉に関わる場合

などが上位を占めている。また事業目的では

・自分へのサービスが向上する

・自分への経済的なメリットが受けられる

のように直接的にメリットが感じられればパーソナルデータを提供しても良いと考える傾向にある（図３－１）。



（出典）総務省「ICTの進化がもたらす社会へのインパクトに関する調査研究」（平成26年）

図３－１　パーソナルデータを提供しても良いと考える利用目的（総務省調査）

これを踏まえて具体的なケースとしては、個人としてパーソナルデータを提供するメリットがわかりやすい「防災」「医療・ヘルスケア」「オリンピック・パラリンピック」とする。表３－１に具体的ケースの概略を示す。

表３－１　具体的ケースの概略

①防災/災害緊急時対応

タイトル	被災者一人ひとりの物資ニーズに合わせた最適な物資配給
説明	自治体が避難所生活の被災者一人ひとりの物資ニーズを把握し配給することを支援。避難所生活における医薬品切れなどに起因する持病の悪化、災害関連死等の二次被害を抑止する。
取り扱い情報	・基本個人情報(氏名、年齢、性別、住所、個人番号) ・服薬・アレルギー等の健康情報
要件	・個人が自分の検診情報や医療情報を集約し、個人の意志で特定の自治体等に提供できること ・災害情報システムとパーソナルデータストア(PDS)のシステム連携

②医療・ヘルスケア

タイトル	一人ひとりに合わせた最適な医療・ヘルスケアサービスの支援
説明	医療従事者が診療を行う際に、医療ビッグデータを活用することで、正確な診断および最適な処置・投薬を行うことを支援する
取り扱い情報	・基本個人情報（氏名、住所、性別、生年月日、連絡先） ・診療情報（カルテ、処方箋、検査結果、治療計画・履歴など） ・体質・嗜好（血液型、アレルギー、飲酒、喫煙など） ・ライフログ（血圧、体重、消費カロリー、摂取カロリー、睡眠など）
要件	・日本全国の医療機関で診療データをオンラインで横断的に利用できること ・診療データに含まれるデータ（検査結果、症状など）の表記や意味が統一されていること ・個人が保有するデータを必要に応じて医療従事者にオンラインで提供できること

③オリンピック・パラリンピック

タイトル	訪日外国人に向けたおもてなしアプリ
説明	多言語対応の音声翻訳システムを活用し、海外からの来訪者など日本語の読み書きが困難な人々と円滑にコミュニケーションする
取り扱い情報	・基本個人情報(氏名、住所、連絡先、決済手段、パスポート) ・位置情報(商品・サービス購入時) ・医療・健康(アレルギー食材) ・コミュニケーション(使用言語) ・趣味・嗜好(旅行計画、購入商品・サービス、食事メニュー)
要件	・情報取得時に本人意思確認 ・料金の無償化、割引などのインセンティブを提示

３．１　防災：被災者一人ひとりの物資ニーズに合わせた最適な物資配給

３．１．１　シナリオ

（１）避難所生活中の物資配給

（ａ）平常時

東京都Ｓ区在住のＡさんは生活習慣病を患っており、医師からは食事のカロリー制限と食後の医薬品服用を指示されている。レストランでの外食が中心のＡさんは、カロリーを気にしながらメニューを選ぶことにストレスを感じていた。ところが、パーソナルデータストア（PDS）サービスを利用するようになってからは、予約時にレストラン事業者に PDS に登録されているカロリー制限情報を参照させることで、レストランがＡさんに適したメニューを提案してくれるようになり、ストレスを感じるどころかレストランの提案が楽しみになっていった。

#	イベント	個人情報	相手
1	PDS へのデータ登録	・服薬・アレルギー等の健康情報（カロリー制限も含む）	PDS
2	民間事業者とのデータ共有	・服薬・アレルギー等の健康情報（カロリー制限も含む）	民間事業者（レストラン等）

（ｂ）災害時

ＡさんはＩ市を観光中に地震に遭遇した。Ｉ市自治体職員の適切な避難誘導もあり、Ａさんは無事に避難所にたどり着いたが、これから続く旅先での避難所生活を不安だと感じている。というのも、Ａさんは処方された医薬品を常に持ち歩いているが、今、手元には１日分しか残っていないためである。観光時はいつもそうだが、Ａさんは旅行期間に必要な分だけの医薬品を旅行用ボストンバッグに備えていた。しかし、観光地で外出中に被災したため、手元にはポーチに入れた１日分の医薬品しか残っていないのだ。

避難所での身元確認の際に、Ｉ市がアレルギー等の個人の事情にも対応した物資提供を行っていることを知ったＡさんは、さっそく避難所に設置されたタブレット端末を使ってＩ市の PDS 参照権を設定し、その旨をＩ市自治体職員に伝えた。職員によれば、Ｉ市の災害情報システムは PDS サービスと情報連携が可能であり、自分自身の物資配給については PDS から参照可能のようだ。Ａさんは早速タブレット端末から PDS にアクセスし、明日の夕刻には医薬品が物資配給されることを確認した。Ａさんは、これからの避難所生活に不安を感じていたが、将来の物資配給が分かることでこれほどまでに不安が解消することに驚いていた。

#	イベント	個人情報	相手
3	個別物資配給のためのパーソナルデータ提供	・氏名・住所・生年月日等の基本情報 ・服薬・アレルギー等の健康情報等	自治体

（ｃ）復旧時

地震発生から数週間後、道路や鉄道などの交通インフラが復旧し始めた。Ａさんの住まいである東京都Ｓ区は地震の影響を受けておらず帰宅環境も整ったことから、ＡさんはＩ市自治体職員から避難所退去の指示を受けた。手続きの際、Ｉ市から今後Ａさんの PDS へのアクセスは行わない旨、及びＩ市の PDS への参照権解除の設定依頼を文書で示された。確かにアクセスしない旨を宣言してもらえるのはありがたいが、やはり自分自身の手でパーソナルデータへのアクセス権をコントロールできることが明らかに分かる方がプライバシーに対する安心感はあるとＡさんは実感した。

#	イベント	個人情報	相手
4	（右記データへの）参照設定解除	・氏名・住所・生年月日等の基本情報 ・服薬・アレルギー等の健康情報	自治体

（２）地域防災計画

Ａさんの生活は東京都Ｓ区の住まいでの普段のものに戻っていた。旅先での震災を経験したＡさんは、もしも勤務先で震災に遭遇したらどうなるのか、通勤中に震災に遭遇したらどうなるのか等、色々なシチュエーションを想像していた。ホームページをアクセスしたところ、住まいである東京都Ｓ区や勤務先である東京都Ｍ区もＩ市のような被災者支援を準備しているらしいことが分かった。

東京都Ｍ区では在住区民が避難生活に必要となる特別な物資に関する情報を収集、把握しているらしい。物資の備蓄計画を策定する際に、必要となる物資のおおよその量を把握するためだ。ホームページにはＭ区在勤者に対しても避難生活に必要となる特別な物資に関する情報を収集している旨が示されていた。Ｍ区は日本有数のビジネス街であるため、発災のタイミングによっては、在住区民に加え在勤者への支援も必要となるためだ。収集した特別な物資に関する情報はプライバシーに配慮した形に加工した上で、小売事業者や流通事業者などの民間協力者と共有されるらしい。Ａさんは、データを民間事業者と共有することについてプライバシーの不安を感じたが、それよりもＩ市の避難所生活での安心感を思い出し、震災時に必要な物資を配給されることを望み、Ｍ市に情報を開示することにした。

申請の方法は紙でもよいし、PDS への参照権付与でも良いようだ。発災時にどんな病気を患って、どんな医薬品を必要としているかを今の時点で明確に把握するのは難しいことから、Ａさんは紙による申請ではなく、PDS への参照権付与による情報提供を選択した。

#	イベント	個人情報	相手
5	災害時に必要な物資の申請	・基本個人情報(年齢、性別) ・特別な救援物資（アレルギー、薬、おむつ等)、及びそれらを必要とする理由	自治体

３．１．２　考察

前節（１）において、パーソナルデータを活用することにより高度化する物資配給の姿を示した。

確かに、このような物資配給は本人メリットが大きい。しかし、そのメリット享受のためにどのようなパーソナルデータが利用されているのかを本人が明確に理解していなければ、プライバシーに対する不安は拭いきれない。従って、本人のメリット、及びそのために利用されるパーソナルデータが何であるかを十分に理解した上で、パーソナルデータ提供の可否を本人が判断するような仕組みが求められる。

また、シナリオに示したように常服薬の個別配給の場合、物資提供に時間上の制限がある。シナリオではPDSを活用することで、自治体が必要な物資情報を迅速に把握する状況を示した。しかし、現状ではアレルギーや常服薬の情報は医療機関や民間検査会社等、様々な事業者が保有しているため、自治体が個別に最適な物資配給を行うのに必要なパーソナルデータについて、その保有者（医療機関等）を特定し、保有者から支援対象者（被災者）の分だけデータ提供を受けることは困難である。従ってシナリオに示したように予め個人が自分自身のデータを主導的に管理し、災害発生時には自治体が即座に活用できる環境を整備する等の対応が求められる。

前節（２）において、パーソナルデータを活用することにより高度化する備蓄計画の姿を示した。

高度な物資配給を実現するためには、シナリオのように平常時から必要物資を想定し備蓄していくことが求められる。もちろん現状においても自治体は地域防災計画に基づいて適切な備蓄計画を立てている。しかし、備蓄されるものは水や乾パン等の一般的な物資に限られており、シナリオに示したような個別の物資ニーズを反映した備蓄にはなっていない。個別の物資ニーズを収集することが現状では非常に困難な上に、それらの物資ニーズはシナリオに示したように時々刻々と変化するからである。従って、より高度の備蓄を実現するためには、変化する物資ニーズを収集する仕組みの構築、備蓄計画への多くの住民や勤務者の参加の双方が求められる。

３．２　医療・ヘルスケア：一人ひとりに合わせた最適な医療・ヘルスケアサービスの支援

３．２．１　シナリオ

ここでは、医療・ヘルスケア分野のシナリオを描き、パーソナルデータ利活用の課題を検討する。次のような状況設定を置く。

《社会や個人の状況》個人の健康管理に関する関心が高まり、日ごろから ICT を活用して食事や運動に関する記録を取る人が増えている。様々なデバイスが市販され、またスマートフォンのアプリなどが供給され、種々の健康サービス事業が立ち上がっている。

医療機関では ICT の活用、診療データの収集・蓄積が推進されている。これまでのサービス効率化の取り組みに加えて、膨大な診療事例の分析による新たな医療知識の獲得や、患者ごとの最適な処置・投薬の選択など、医療ビッグデータの活用も試行されはじめている。

- マイナンバーの利用が始まっている。マイナンバーと健康保険とは連携している。
- パーソナルデータの新しい管理方式が利用され始めている。個人が自分自身でデータを管理し、必要に応じて事業者やアプリに個別にアクセスを許可する、パーソナルデータストア(PDS)と呼ばれるモデルである（１．１．４、１．２．７）。これまでは、事業者がデータを一括管理し、各ユーザに自分のデータへのアクセス許可を与える形が一般的であった。
- 医療機関での ICT の活用は進んでいるが、異なるシステム間の相互運用性やデータの可搬性は低い。結果として、診療データの共有や利活用の取り組みは医療機関単位またはグループ単位にとどまっている。

《登場人物などの設定》Ｂさん（58 歳）は、以前に脳溢血で倒れたことがある。すぐに専門病院で治療を受けて大事には至らなかったが、再発防止のために運動・食事・睡眠を改善したいと思っている。しかし、単身赴任中のＢさんは仕事が忙しくてなかなか運動できず、飲酒・喫煙も減らせない。また、血圧や体重の計測も面倒で、記録がない日も多い。離れて暮らす家族は、Ｂさんの生活習慣が改善しないことを心配している。

民間の事業者Ｐは、ライフログ用の腕時計型ウェアラブルデバイスの製造・販売と、それらのデバイスで取得したデータを活用した健康サービスを提供している。スマートフォン用のアプリがユーザとのインタフェースになっている。

病院Ｘは、他の医療機関と連携して診療データの共有・蓄積を進めており、データ分析に基づいて診断や処方などの意思決定を支援するシステムを構築・運用している。新しい治療方法や薬など、最新の医療情報も随時追加される。このシステムによって、医療業務の効率化が図られると同時に検査漏れや診断ミスを防ぎ、個々の患者に最適な医療サービスを提供できることが期待されている。

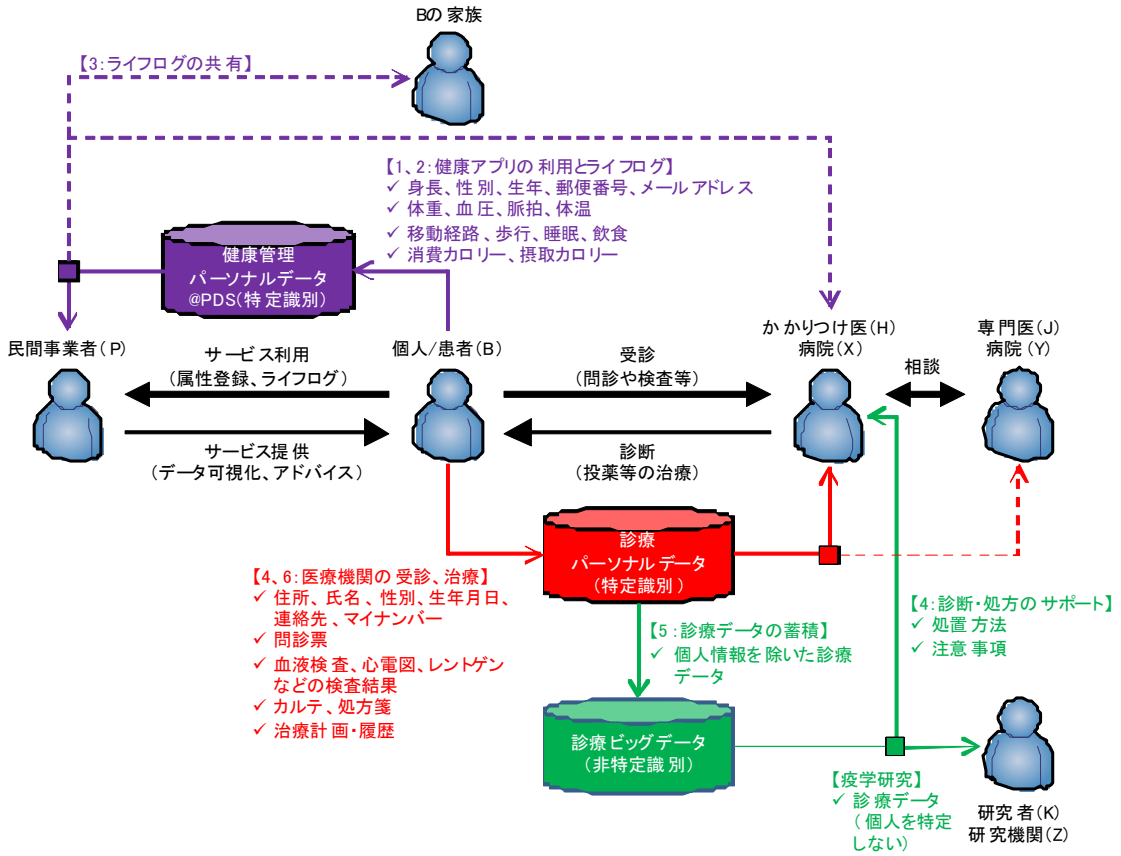


図３－２　シナリオの全体像（番号はイベントに対応）

（１）シナリオ１：ライフログに基づく普段の健康管理

《ライフログと健康アプリ》Ｂさんは、誕生日に家族から腕時計型ウェアラブルデバイスと体重計をプレゼントされた。息子も同じものを使っているという。血圧や心拍数、運動量、睡眠状態などを常に記録しておいて、スマートフォンでグラフにして見せてくれるという。家庭用血圧計では１日に１回の計測が精いっぱいだが、これは防水で風呂に入るときも付けたままで大丈夫、一日中ずっと記録してくれるらしい。

早速スマートフォンにアプリ（以下「健康アプリ」と呼ぶ）のインストールを開始して、指示通りに性別や年齢などの必要事項を入力すると、「利用規約」というとても長い文章が表示されて「最後まで読んで同意ボタンを押すとサービスを開始します」とのこと。他のアプリと同じくこの手の文章は読み飛ばして「同意します」ボタンを押すと、デバイスとの通信が始まってデータが取り込まれ始めた【イベント 1】。同じアプリで体重計の設定も行った。スマートフォンが近くにあれば、乗るだけで体重や体脂肪率などを記録してくれる【イベント 2】。

《家族とのライフログの共有》Ｂさんが使う健康アプリには SNS のような機能があって、友達や家族の承認をすると互いにデータを見せたり比べたりできる。息子からの家族申請を承認すると、2 人のデータを横並びで見られるようになった【イベント 3】。つまり、息子からはこちらのデー

タが見えることになる。血圧や体重、歩数や睡眠時間などに加えて、移動経路まで見える。遠くに住む家族の生活の様子や健康の状態が、電話でしゃべらなくてもなんとなくわかるのは悪くない。それにしても、このデバイスとアプリはよくできていると思うが、何か設定する度にいちいち長い文章が表示されて「同意します」ボタンを押さなければならないところが面倒でならない。

《さまざまな広告》Ｂさんは脳溢血で倒れた経験から、健康アプリで主に血圧の具合を見ているが、ここ最近はたびたび正常範囲を超えている。毎週、健康診断や人間ドックの受診を勧めるメールが事業者から届くようになった。今週はさらにスポーツジムから入会キャンペーンの広告が届いて、「そういうことか」と思った。つまり、データを分析してだれが何を必要としているか見極め、その情報でビジネスをしているのだ。次は保険会社からの広告ではないかと思い、不快に感じた。

#	イベント	データ	相手
1	ウェアラブルデバイスおよび健康アプリの利用開始	身長、性別、生年（年齢）、郵便番号（居住地）、メールアドレス（連絡先）	民間事業者（デバイスメーカー）、PDS
2	ウェアラブルデバイスおよび健康アプリによるライフログ	体重、血圧、脈拍、体温、移動経路、歩数、睡眠（時間、質）、飲食（内容、写真）、消費カロリー、摂取カロリー	同上
3	ライフログの共有	上記 1、2	家族

（２）シナリオ２：かかりつけ医の受診と診断・処方

《かかりつけ医の受診》ある日の午前中、Ｂさんは職場で手足がしびれ、気分が悪くなった。しばらくするとしびれは収まったが、職場の保険・健康管理担当部署に病院Ｘを紹介してもらって午後の受診予約を取った。以前にも利用したこの病院は、先進的な取り組みをしており、治療期間が短く保険料の観点でも効率がよいとのこと。

午後、Ｂさんは病院Ｘを訪れ、診察カードを読み取り機にかざして受付を行った。この診察カードは病院内で自分のマイナンバーと結びついている。受付で渡されたタブレット端末で問診票への記入をしながら順番を待った。順番が来て、医師Ｈの診察を受けた。Ｂさんの基本属性や既往歴、問診票はすでに医師のデスクトップ PC に表示されている。Ｂさんは自覚症状について説明し、最近は血圧が高めであることを自分のスマートフォンでグラフに表示して見せた。血圧は測定環境によるぶれが大きいため日ごろの血圧を参考にしたいとのことで、PDS に保存されているライフログや職場で受けた健康診断結果へのアクセスを医師Ｈに許可した。血液検査、レントゲン、心電図などの検査の結果、軽い脳梗塞の疑いがあるとのことで、以前と同じ血圧を下げる薬 α と血液を固まりにくくする薬 γ を処方された【イベント 4】。さらに詳しく調べるが、場合によっては専門病院にデータを送って診断を支援してもらうとのこと。Ｂさんは診療データの共有を承認し、次回の受診予約をして帰宅した。

#	イベント	データ	相手
4	医療機関の受診	個人情報（住所、氏名、性別、生年月日、マイナンバー、連絡先）、問診票、検査結果（血圧、血液、レントゲン画像、心電図など）、PDS のライフログで診断の参考になるもの（血圧など）	医療機関および医療従事者

《データに基づく診断と処方》Ｂさんが受診した病院Ｘは、データ分析に基づいて診断や処方を支援するシステムを導入している。Ｂさんの診断・治療計画において、システムは医師Ｈと同じく脳梗塞と予測してきた【イベント 4】。しかし、原因として高血圧の他に不整脈も考えられるとのこと。システムが推奨する処置は、医師Ｈが処方した薬αは第 2 位で、1 位は最近市販された食事制限を必要としないβであった。Ｂさんのアレルギーも考慮されている。

《診療データの二次利用の許諾》Ｂさんは医師Ｈから最終的な診断結果と新しい処方薬βについて説明を受けた。高血圧ぎみで動脈硬化などの症状に発展する可能性があるので、血圧を下げる薬βを継続的に飲んで様子を見ることになった。この薬は食事制限がないので助かる。最後に、この病院Ｘでは診療データを診断や研究に生かすために蓄積して、他の医療機関とも共有する旨の説明を受け、データ提供の同意を求められた。もちろんＢさんを特定するような個人情報はきちんと保護され、医学的な見地から必要なデータだけを共有するとのこと。Ｂさんの診察でも、データの分析から最適・最新の薬が選ばれているそうだ。そういうことならば協力しようと、Ｂさんはタブレット端末上で同意ボタンを押した【イベント 5】。診察後、Ｂさんは薬局に行って個人識別カードを読み取り機にかざし、処方薬βを受け取った【イベント 6】。その場でスマートフォンの服薬アプリにデータを取り込むと、服薬を忘れないようにアラームが設定された。

#	イベント	データ	相手
5	診療データの蓄積	個人を特定できないように加工した診療データ	医療機関および医療従事者、大学などの研究機関
6	処方薬の受け取り	処方箋（薬の種類と服薬の量・回数・期間）	院外薬局、スマートフォンのアプリ、PDS

（ｃ）シナリオ３：別の病院での診察

《専門医療機関の受診》Ｂさんは薬βを指示通りに服用し続けたところ、血圧が正常範囲に戻り安定してきた。家族からも安心した旨のメールが届いた。まだ薬は残っているがもう大丈夫だと思い、薬を持ち歩くのをやめて服薬アプリのアラームを解除した。しばらくすると、また例の手足のしびれがあり、再度病院Ｘを受診したところ、専門病院Ｙで脳ドックなどの精密な検査を受けることになった。

《医療機関をまたがるデータの共有》病院Ｙでは医師Ｊの診察を受けた。脳ドックで血栓は見つからなかったので、やはり高血圧を原因とする軽い脳梗塞だったのであろうとのこと。病院Ｘで処方された薬βをまだ飲んでいるはずではないかと言われて、なぜそれを知っているのかと思ったが、すぐに例のデータ共有云々のことを思い出した。「どの病院に行ってもこんな風に過去の受診歴がわかっちゃうなんて、すごいですね」とＢさんが言うと、「理想はそうですが今のところ提携病院だけで、マイナンバーと完全に連携できていないから全国どの病院に行っても大丈夫ってわけじゃありません」と医師Ｊは不満そうである。

《サービス事業者の切り替え》Ｂさんの息子は、もっとよい健康サービスはないかと探していたところ、診療データを取り込める新しいサービスを見つけたので、Ｂさんにも切り替えを促した。Ｂさんは、PDS に病院Ｘ とＹのデータをダウンロードしてから、スマートフォンに新しいアプリをインストールして PDS へのアクセスを許可した。これまで使ってきた事業者Ｐの健康アプリのアクセス許可は解除した【イベント 7】。

#	イベント	データ	相手
7	健康アプリの乗り換え	1、2 と同様	民間事業者

３．２．２　考察

（１）医療・ヘルスケア分野におけるパーソナルデータ利活用の意義

健康に関する国民の関心は高く、パーソナルデータを利活用することによって最新・最適のサービスを受けられるという個人のメリットは理解しやすい。また、蓄積した診療データの分析による医学研究の進展や、治療方法の最適化および治療期間の短縮による診療費・保険料の削減などは、パーソナルデータが公益に資することを納得できるわかりやすい効果と言える。

当該分野はパーソナルデータ利活用の先行的な取り組みの対象として最適であり、国民にも政府にも訴求しやすい。

（２）プライバシーに関する不安

医療・ヘルスケア分野では個人の身体や嗜好に関する情報を扱う【シナリオ 1、2】。医療機関で診療サービスを受けるにあたり、個人（患者）がこの種のデータを提供することは自然であり不安を感じることは少ない【シナリオ 2、3】。医療機関・医療従事者は法令やガイドラインで制約が課せられているからである。しかし、ICT の活用によってデータの電子化やシステムのネットワーク化が進み、民間事業者が当該分野に参画してくると、国民は以下のような不安を感じるであろう。

- サイバー攻撃や不正持ち出しによる情報漏えい事故が起きて、病歴などが他人に知れるのではないか。そのような事故があった場合に適切な処置や補償がなされるのか。
- 他の事業者にデータが渡り、広告などに利用されて不快な思いをするのではないか。
- 匿名化をしていても、稀な疾病・体質の場合には個人が特定されてしまうのではないか。

当該分野のパーソナルデータを扱う医療機関や民間事業者では、システムの導入時には高度な情報セキュリティやアクセス制御などの技術的な裏付けや、内部規定などのルール作りを行うことが求められる。また、運用時には情報セキュリティに関する監査を義務化し、かつ情報公開していくことが望ましい。法令に基づく医療機関とそれ以外の民間事業者とでそれぞれの制度づくりが必要であろう。さらに、個人のプライバシーを尊重しつつ、疫学研究などの医学発展に有効であるような診療データの匿名化方法について、具体的な検討を行う必要があろう。

（３）パーソナルデータの二次利用に対する不安

健康寿命の延伸や、医学発展、行政効率化など、当該分野のパーソナルデータの利活用が個人にも社会にも貢献することは理解しやすい【シナリオ 1、2、3】。この点は積極的に啓蒙すべきであるが、二次利用の目的や方法を簡単かつ誤解のないように説明することが求められる。経済産業省の「消費者向けオンラインサービスにおける通知と同意・選択のためのガイドライン」における情報共有標準ラベルをベースとした、食品表示のような共通化された情報提示の枠組みが有効であろう。

一方、広告などの商業利用を目的とした二次利用は消費者の納得を得にくいであろう【シナリオ 1】。当該分野のパーソナルデータに関する、利用目的の制限や合理的な範囲内での目的変更の手続きなどのルール整備を早急に行う必要がある。

（４）パーソナルデータのコントロールに関する不満

民間事業者のサービスを利用する場合、ユーザは次のような裁量を望むであろう。

- 任意の時点でサービスの利用を取りやめる。
- 蓄積したデータを生かしたまま、サービス提供事業者を切り替える。

このような要求にこたえるには、データの取り出し機能、データフォーマットの標準化や API の提供など、データの可搬性またはアプリケーションの相互運用性に関する技術的な整備が必要になる。また、PDS のような管理モデルが普及することによって、可搬性や相互運用性の問題だけでなく、データの消去やオプトアウトのし忘れなどの課題を解決できる可能性がある。

一方、遠方の家族の見守りや健康状態の把握などの目的で、家族や友人とデータを共有したいという要求もある。

- 申請・承認に基づいて、特定の範囲のデータへのアクセスを許可する。
- だれにアクセスを許可しているかを容易に把握できて、その解除を簡便にできる。

これらの要求に対しても、PDS が普及すれば VRM の仕組みを用いることができる。つまり、データの提供先と提供範囲を個人が自らコントロールする。特定のサービスではこのようなデータ共有機能を実装している場合もあろうが、ベンダーロックインの問題を回避するには PDS のモデルが都合がよい。

（５）診療サービスの向上・発展を阻害するデータ共有の課題

医療機関や医療従事者の専門化・細分化が進み、複数が連携して診断・治療にあたるケースが増えている。また、かかりつけ医から専門医への橋渡し、医療機関と介護機関との連携、引っ越

しや勤務地の変更などに伴う人の移動などに柔軟に対処するためには、一つの地域や医療機関に閉じない診療データの共有が求められる。

しかしながら、医療機関には国、独立行政法人等、地方公共団体、民間事業者など異なる運営母体がある。それぞれに異なる法令・条例と独自の施行体制・ガイドラインなどがある。このため、複数の医療機関にまたがった横串での診療データの流通が困難である。いつでもどこでもすべての国民の診療データを利用できる制度と仕組みが必要である。医療機関をまたがるデータ共有の利便性はすべての関係者が認識していることであろうが、個人情報保護法やマイナンバー制度との関係も含めて、制度・システムとも今後の取り組みが期待される。

３．３　オリンピック・パラリンピック：訪日外国人に向けたおもてなしアプリ

３．３．１　シナリオ

（１）想定する状況

五輪などの大きなイベントに来日する外国人に対して、おもてなし精神を発揮し、利便性高く、より豊かな体験をしてもらい、日本国のファンを増やしたい。そこで、来日を予定している外国人には事前に登録してもらい、パーソナルデータストア(PDS)環境を整備してもらう。

特に、初めて来日する人にとっては言語の障壁が課題となる。その障壁を乗り越えるサービスとして、多言語対応の音声翻訳サービスを提供する。専用アプリをインストールしたスマートフォンから利用でき、来日する外国人は無償で利用できる。

PDS 環境は多言語で用意されており、個人のデータを格納できる。この環境と自分のパスポートの情報を連携することにより、訪日観光者 ID が発行される。来日前から利用可能で、個人毎の好みを学習させることができる。観光サイトや情報サイトと連携し、五輪の競技スケジュールの他、日本国内の観光案内が閲覧でき、来日スケジュールと組み合わせて個人用のポータルサイトとして利用できる。

（２）シナリオ

（ａ）来日前

訪日外国人Ｃさんは 2020 年の東京五輪に合わせて訪日を計画している。PDS 環境を整備し、「オリンピック会期中の旅行の提案を募集」と掲示した。連携している旅行代理店からの提案を見比べて、自分の好みにあった航空券と観戦チケットを購入した。同様に、好みにあった宿泊先を選んで予約する。PDS に入力した食物アレルギー情報をホテルが参照できるようにした。

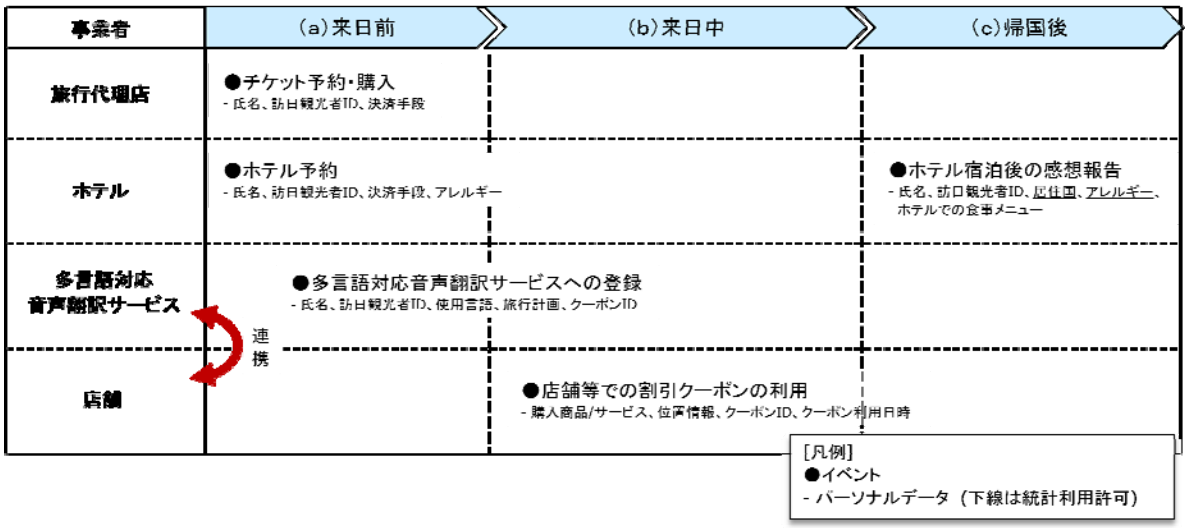


図３－３　訪日外国人のパーソナルデータ利用内容(時間軸)

日本滞在中に役立つと思われる「多言語対応音声翻訳サービス」が無償で利用できるとの情報を入手。専用アプリをダウンロードする。このアプリがPDS環境と連携できるように訪日観光者IDを入力。データストア内の使用言語が反映される。

PDS環境は個人用のポータルサイトとして利用できる。五輪の競技スケジュールの他、日本の観光案内が閲覧でき、個人ごとの旅行計画を組み立てることもできる。使用言語と旅行計画については、個人を特定しない形での統計利用および第三者提供を許可することで、観光地での割引クーポンが配信されるとのことなので、利用を許諾する。

#	イベント	個人情報	相手
1	チケット予約・購入	氏名、訪日観光者ID、決済手段	旅行代理店
2	ホテル予約	氏名、訪日観光者ID、決済手段、アレルギー	ホテル
3	多言語対応音声翻訳サービスへの登録	氏名、訪日観光者ID、使用言語、旅行計画	音声翻訳サービスユーザー登録サイト

（ｂ）来日中

到着した空港の最寄り駅でICカード乗車券を購入する。日本ではICカード乗車券の利用範囲が広がっているため、これ一枚で競技観戦や観光などの移動がスムースになる。

予約したホテルに到着。フロントやレストランなどで必要に応じて音声翻訳サービスを利用する。食物アレルギーについてホテルに事前に伝えておいたので、当該素材を利用していない旨がＣさんの使用言語で説明されている。

競技観戦などのスケジュールは音声翻訳サービスの個人ポータルにまとめてあるのでわかりやすい。食事や土産物などでさまざまなクーポンが利用できるが、利用したときの位置情報の取得を店舗側に許諾すると割引率がさらによくなるとのことなので、位置情報の取得を許諾した。特に個人を特定する目的ではなく、クーポンの利用場所を集計する目的とのこと。

観戦・観光も終わり、ホテルをチェックアウトする際、ホテルの感想を帰国後に報告してもらえるなら、次回以降の宿泊割引券を送付するとの申し出がホテルからあり。とりあえずアンケート依頼メールを送付することを許可した。

#	イベント	個人情報	相手
4	店舗等での割引クーポンの利用	購入商品/サービス、位置情報、クーポン利用日時	店舗（およびシステム）

（ｃ）帰国後

早速ホテルからアンケート依頼メールが届いている。ホテルの印象の他、アレルギー食材を除いたメニューへの感想も聞かれていた。回答結果は個人を特定しない形で統計的に分析し、今後のメニュー改善につなげるとのこと。許諾してアンケートに答えた。

#	イベント	個人情報(下線は統計利用許諾)	相手
5	ホテル宿泊後の感想報告	氏名、訪日観光者ID、住所、居住国、アレルギー、ホテルでの食事メニュー	ホテル

３．３．２　考察

（１）パーソナルデータの階層的開示

図３－３の中でパーソナルデータを階層的に開示(統計利用許可)している部分として、多言語対応音声翻訳サービスと店舗の利用について取り上げる(図３－４)。多言語対応音声翻訳サービスは訪日観光者 ID で利用できる。使用言語や旅行計画を登録する。この際、店舗で利用できるクーポンの発行を受けるが、クーポンについても個別に管理 ID(クーポン ID)を発行する。店舗ではクーポンを利用するため使用したクーポン ID の他、購入商品/サービス、位置情報、クーポン利用日時がパーソナルデータとして生成される。

これらのパーソナルデータの中から統計利用を許可したものがビッグデータ(訪日外国人対応)のデータの一部として利活用される。商品/サービスの需要や来店者数の予測などが考えられる。

インセンティブの点ではこのシナリオでは直接的に割引クーポンとして配付することを想定している。これはパーソナルデータを直接売買するイメージである。この他、間接的なメリットとしては商品/サービスの需要予測の結果として、商品/サービスの品切れ防止につなげることができる。これはユーザーメリットだけでなく事業者側のメリットでもある。

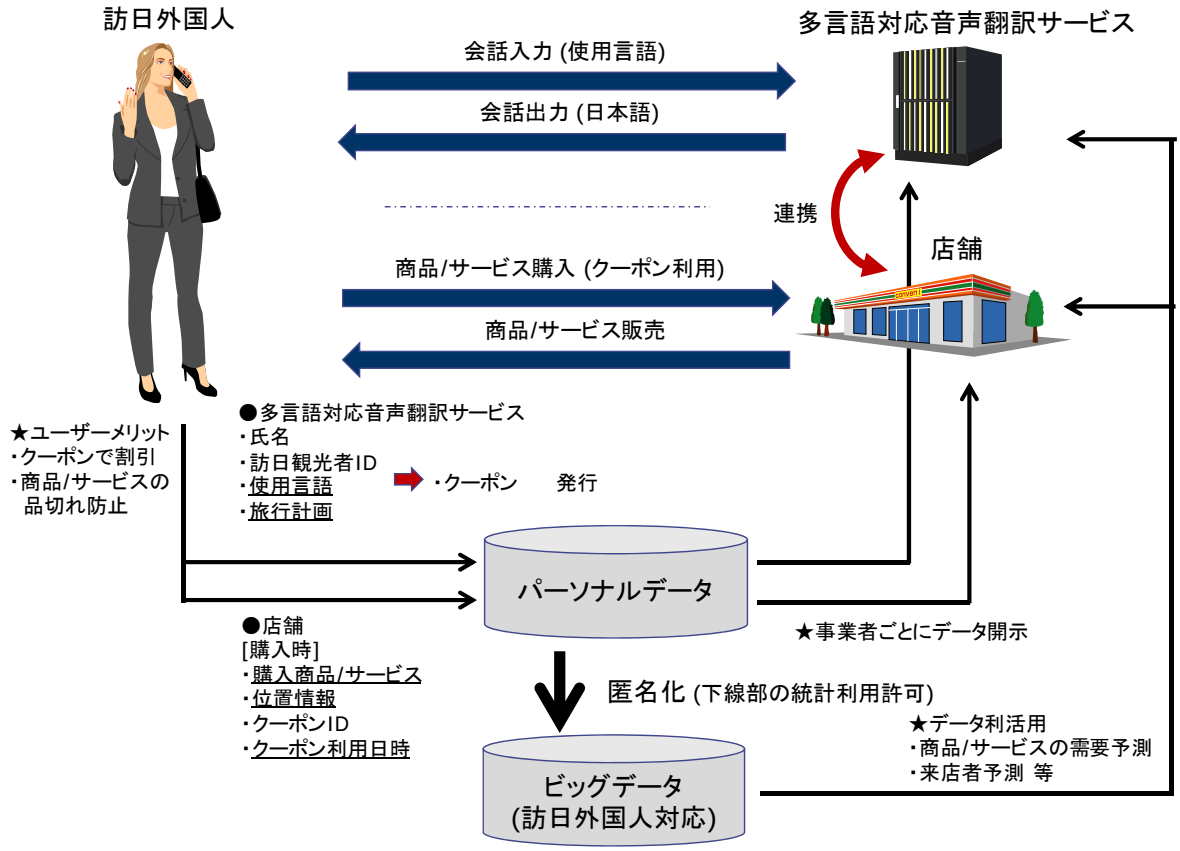


図３－４　訪日外国人のパーソナルデータの階層的開示

（２）コンセンサス形成に向けた課題と対応

（ａ）個人情報利用許諾時の不安の解消

「３．３．１　シナリオ」では「使用言語」「旅行計画」「購入商品/サービス」「位置情報」「クーポン利用日時」「アレルギー」「ホテルでの食事メニュー」について統計利用する旨を申し出、利用許諾を得ている。それぞれに割引サービスなどで利用者に対して直接的なインセンティブを提示することで利用許諾を得ているが、許諾した情報が実際にどのように利用されるのか、個人を特定しないと書かれているがそれはどのようにして保証するのかについての説明(と納得感)が不足している。

個人を特定しないことについて、技術的な裏づけだけでなく、一定の認証取得(定期的な監査を含む)を前提とした公的な保証があれば、許諾の可否を利用者が判断する上での参考となる。

（ｂ）個人情報利用許諾後の不満の解消

一旦利用を許諾した後で、やはり許諾を取り消したい場合の選択肢や実現手段が提示されていない。ここでは統計利用に限定しているため、逆に統計処理したデータとして第三者と共有したり公開したりした後には訂正や削除が困難となる可能性がある。

統計利用するということは、当該データをオープンデータの一部として組み込むことを意味している。すなわち、利用者の求めに応じて削除する手段が本質的に用意できない。このような民間での統計利用のあるべき姿についてガイドラインを定める必要がある。

（ｃ）個人情報利用許諾後の満足感

割引クーポンとの交換というインセンティブ視点だけでなく、提供した個人情報が商品やサービスの改善につながり、ひいては利用者個人だけでなく社会全体の改善につながるシナリオが必要不可欠である。「３．３．１　シナリオ」の中ではアレルギー食材に関するアンケートからメニューの改善につなげるという直接的な活用しか言及されていない。このシナリオの中だけでもさらに多種の情報について利用許諾を得ており、それらを個人を特定しない形で横断的に活用する方向へ道を開くのが望ましい。

とはいえ事業者間での情報共有にはさまざまな高いハードルがある。逆に、ここで採用したPDSのように、個人の側に利用許諾をした情報は全て管理しておき、個人主導で情報の横断的活用を許諾するアプローチが望ましい方向と考えられる。たとえば、クーポンの利用履歴は店舗だけに許容するのでなく、ホテルや旅行代理店、音声翻訳サービスサイトなどにも利用を許可することで、より深い分析結果を得ることが期待される。第２章で提案したパーソナルデータ・エコシステムはこのようなデータ利活用に道を開くものである。。

第二章で説明したモデルに基づき、パーソナルデータを利活用するプロセスを改めて図式化する（図４－１）。法令の規定による義務として個人情報を利活用するもの（①）、本人の同意に基づくもの（②）、匿名加工したデータを利用するもの（③）がある。このうち①と②は表１－１のカテゴリーで言うところの識別特定情報、③は識別非特定情報である。

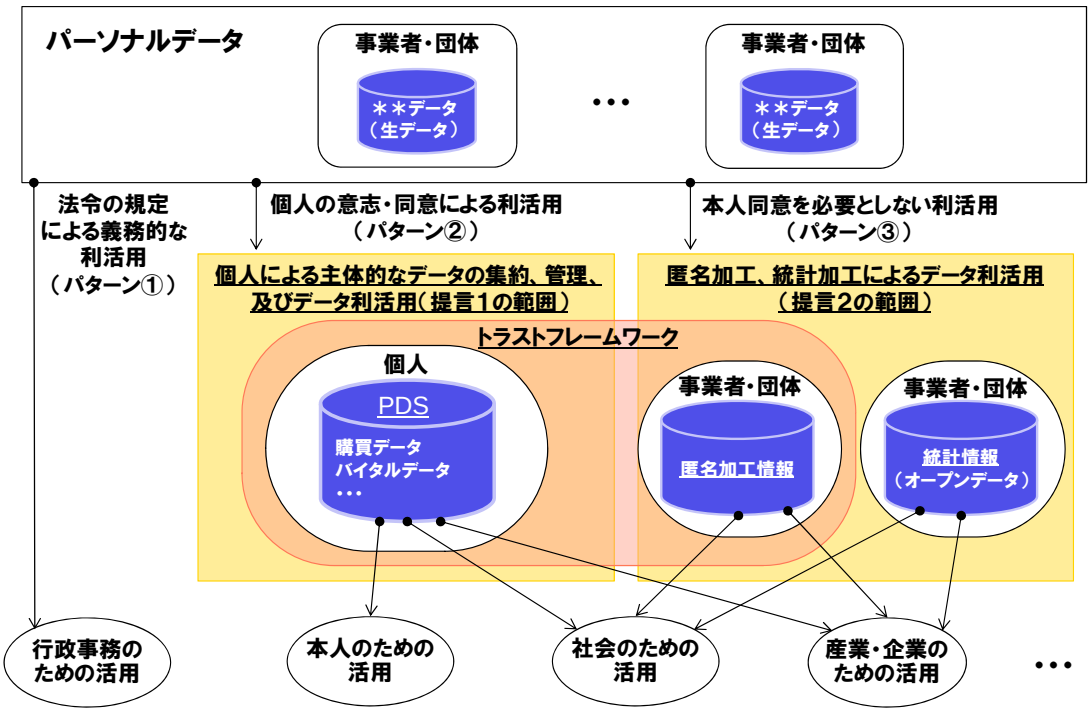


図４－１　パーソナルデータを利活用するプロセス

さらに利活用の一形態として統計処理を想定し、表１－１に示した 3 つのカテゴリーの関係について示す（図４－２）。統計処理結果は非識別非特定情報と考えられる。このように匿名加工や統計処理を加えることでデータ利活用の進展が期待される。

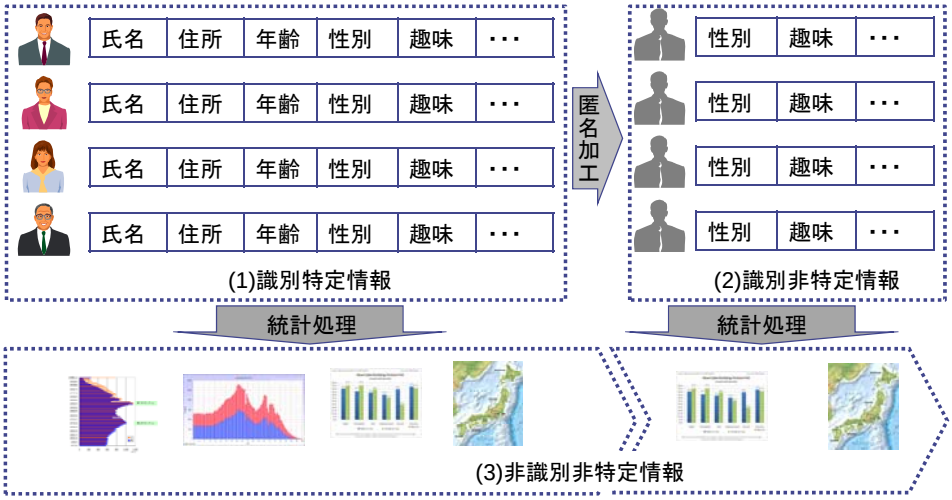


図４－２　パーソナルデータの匿名加工と統計処理のイメージ

以上述べた形態での利活用を前提として、本研究会では以下の事項を提言する。

［提言１］日本版パーソナルデータ・エコシステムの構築

我が国におけるパーソナルデータ利活用の促進のために、個人情報保護法の改正作業が進められているところである。今回の法改正は企業がデータを利活用するためのルールの明確化を通じて、民間分野における新たな経済価値を創出し、我が国の経済成長に資するためのものである。他方で、個人や消費者の側から、自分のデータを企業の便益に利用されることへの抵抗感やプライバシー保護に対する不安等が生じており、たとえ法改正を通じて企業が守るべきルールが明確化されたとしても、個人の不安感や不利益感という根本的な問題までが解決されるわけではない。

従って、パーソナルデータを利活用しようとする日本企業は、単に法令を遵守するのみならず、個人のプライバシーを守りながら個人に対して新たな価値やメリットを提示するような仕組み（日本版パーソナルデータ・エコシステム：２．２．２）を構築していくことが求められている。このような仕組みの実現に向けて、官民で連携して下記の施策を推進するべきである。

（施策１）個人によるデータコントロール環境整備の推進

個人の意思を尊重したデータ利活用を促進するためには、個人が自己情報コントロール権を発揮し、自分のデータの利用許諾やその撤回等を自分で管理できるパーソナルデータストア(PDS)のような仕組みが必要となる。そのためには、企業等によるマシンリーダブルな形式でのパーソナルデータ開示と、開示にあたってのデータ形式の標準化が鍵となる。

また、企業等が足並みを揃えた取組みを行うように、英国 midata 等の諸外国の施策を参考に、国には PDS 推進のための積極的な旗振りが期待される。

（施策２）トラストフレームワークの整備

個人が企業等に対して安心して自分のデータを提供し、データを利活用したサービスを享受するためには、データを授受する者が互いに相手を「信頼できる」とみなすための仕組み（トラストフレームワーク）の整備が必要となる。また、国境を越えたデータ移転が増加していることから、トラストフレームワークのグローバルな相互運用性を推進することが重要である。

（施策３）パーソナルデータ・エコシステムを活用した新産業創出の支援

パーソナルデータ利活用に対する国民のコンセンサスを得るためには、不安感の払拭とともに、個人に対して金銭的対価・利便性向上・社会的意義といったインセンティブを与えることが重要である。そのためには、個人により集約、管理しているパーソナルデータを活用することで新たな本人メリットを提供する事業者を育成、支援することが重要である。

［提言２］産業競争力強化に向けた環境整備

オープンデータの利活用加速のため、オープン化した行政情報だけでなく企業や個人の持つパーソナルデータの利活用を促進する。プライバシー保護に配慮した形でパーソナルデータの利活用を進めるためには国民のコンセンサスが必要不可欠である。コンセンサスの壁を構成する国民

の不安や不満を解消するため、パーソナルデータを利活用するプロセスに関する環境整備を官民共同で加速する。

（施策１）匿名加工に対する安心感の醸成に向けた国民への発信

パーソナルデータの匿名加工は利活用を促進する上で重要な根幹を成す。個人情報保護法の改正を通して匿名加工に対する理解を得、国民の中に安心感を醸成することが欠かせない。このため、匿名加工に対する運用規定の整備や具体例を通したメリットの体験など、国民に対する不断の情報発信を行う。

（施策２）オプトアウト規定の見直しを踏まえた利活用ガイドライン整備

個人情報保護法では事業分野ごとに多数のガイドラインが策定されている。オプトアウト規定の見直しを踏まえ、パーソナルデータ利活用に資する側面だけでなく、個人の求めに応じた利活用の円滑な停止にも対応するため、IT の導入を前提とした事業分野ごとのガイドラインを整備する。

（施策３）個人が利活用できるパーソナルデータの政策的な充実と管理強化

諸外国での先行した取り組みでは、ヘルスケア等の複数の事業分野において、個人の求めに応じてパーソナルデータを事業者から個人に提供する取り組みが政府主導で進められている。わが国においても同様のパーソナルデータの充実策を進めるとともにパーソナルデータの管理におけるセキュリティ対策についても強化する。

（施策４）国民が自ら実践できるプライバシー保護対策の認知度向上

スマートフォンに代表されるモバイル機器とソーシャルネットワークサービスの普及により、いつでもどこでも誰でも簡単に情報発信ができるようになった一方で、個人情報を安易に公開しトラブルになるケースが多発している。法制度整備や技術の向上に頼るだけでなく、自ら実践できるプライバシー保護対策の認知度を向上し、安全な情報化社会を構築する。

［提言３］具体ケースでの実証によるコンセンサスの形成

「防災」、「医療・ヘルスケア」、「オリンピック・パラリンピック」についてはパーソナルデータの提供メリットが個人にとってわかりやすいものとして具体ケースでとりあげた。今後これらの分野において先行した実証実験を行うことで国民がメリットを実感できるようにし、国民のコンセンサスを形成する。匿名加工の技術実証の場としても活用する。

【おわりに】

●今後の課題と展開

本研究ではパーソナルデータの利活用に対する国民のコンセンサス形成を目的として、パーソナルデータの利活用とプライバシー保護を両立するモデルを立案し、個人がパーソナルデータを提供することのメリットがわかりやすい具体ケースでの適用を検討した。パーソナルデータストアなどから構成されるパーソナルデータ・エコシステムや匿名加工情報流通基盤等について論じたが、前者の前提とする姿としては個人が自分のパーソナルデータを自分で管理するという将来像がある。また後者については適切に匿名加工されかつオプトアウトが有効に機能する前提でパーソナルデータを第三者に提供する将来像を描いている。前記提言と施策ではこのような将来像を具現化するために必要な事項を列挙した。

ここでパーソナルデータ・エコシステムは本人同意に基づくものであり、現行個人情報保護法を補完しながら、利活用を進めるための仕組みである。匿名加工情報流通基盤についてはまさしく法改正の重要部分であり、パーソナルデータを利活用する姿を一変させる可能性を秘めている。例えば IoT(Internet of Things： モノのインターネット)の時代においては、カメラ、センサー、カードリーダー、カーナビ、駅自動改札、自販機など様々な場面で本人の同意なくパーソナルデータが収集・利用される可能性がある。こうした膨大なパーソナルデータに対してどのように個人のコントロールが及ぶようにするか、またどのようにして匿名加工を実施し、オプトアウトを保証するかは、匿名加工に対する汎用的な技術がないことも踏まえると、具体ケースで個別に検証していかなければならない。

例えば監視カメラ画像の活用がプライバシーの観点でしばしば話題となるが、防犯目的で入手した個人が特定できる程度の鮮明な画像を元に、匿名加工して第三者提供し他の目的(例えば人流分析・予測等)に利用するなどの運用は、撮影された個人のメリットが見えづらいためかなりハードルが高いものと考える。パーソナルデータの利活用については、具体例を通した国民のコンセンサス形成が不可欠で、そのためにはパーソナルデータを提供するメリットを個人にわかりやすく伝えるとともに、データ利活用やプライバシーに関する個人のリテラシーを向上させることが必須である。本研究ではこの点を念頭において報告としてまとめた。今後は提言や施策に挙げた内容を官民連携して加速していく。

【用語集】

本報告書で頻出する用語について解説する。

用語	解説
個人情報	個人情報保護法の対象とする個人情報。現行法では次のように定義される。 「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む)」
パーソナルデータ	「個人情報」に限らず「広く個人の行動・状態等に関するデータ」 (IT 総合戦略本部「パーソナルデータに関する検討会」での定義より)
パーソナルデータストア(PDS)	パーソナルデータを安全に格納するとともに効率的な利活用を図る仕組み。データの保管、管理、アクセス制限などを行うとともにパーソナルデータに特化した様々な機能を持つ。
パーソナルデータ・エコシステム	パーソナルデータを個人が集め、管理し、様々な組織や企業に利用させることで個人が直接的に利益を得るシステム。
オプトアウト	opt-out。opt には「どちらかを選ぶ」意があり、opt-out は除外を選ぶこと、または除外を選ばせることを前提とした仕組み。代表的な例として初期の広告宣伝メールの配信方法に採用されていた。これに対して同意を前提としてメール配信するのがオプトイン。

産業競争力懇談会（ＣＯＣＮ）

東京都千代田区丸の内一丁目６番６号　〒100-8280
日本生命丸の内ビル（株式会社日立製作所内）
Tel：03-4564-2382　Fax：03-4564-2159
E-mail：cocn.office.aj@hitachi.com
URL：http：//www.cocn.jp/
事務局長　中塚隆雄