応般

サービスのパーソナライズ化とデータ利用

―事業者・利用者の信頼関係の構築を目指して―

坂下哲也（JIPDEC（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）

データ利用を巡る課題

技術の進展や，責任あるデータの利用は，経済的・社会的な実益をもたらす．特に，インターネットによるグローバル化や，持続的な通信環境の実現によって，「個人情報（本稿では，個人情報保護法第2条に該当するものを指す）やパーソナルデータ（本稿では「単独で個人情報に該当するか否かにかかわらず，個人と連結可能なデータ」を指す）」は，行政，個人の私的な活動や，企業活動において重要なものになってきた[2]．たとえば，現在位置を使った購買や店舗の来訪は数倍に増加していることや，流通事業者が利用者個別の購入情報を分析してフードロス（廃棄処分量）をなくすことなどが挙げられる．一方で，スマートデバイスの普及やセンサネットワークの充実によって，多様なパーソナルデータが持続的に取得される機会も増え，個人のプライバシーに対するリスクも高まっている．

具体的には，利用者は，「個人情報やパーソナルデータ」が取得されたときには予想されなかった方法で利用される可能性があることや，その活動がディジタル・データとして蓄積されるため，個人の行動の監視などが容易になるのではないかという懸念を持つ．また，事業者は，利用者のさまざまな情報を取得・分析し，個別最適化されたサービスを提供することを検討・試行するが，そのようなサービスを始めた場合に，利用者への説明が不足していたり，技術的な不備や，現行の法規やガイドラインにおける解釈の相違等から，インターネットを始めとする各種メディアで集中的な批判を受け，サービスを撤退するような事態が確認される．

このような状況は，利用者の「個人情報やパーソナルデータ」を活用したビジネスは非常に大きな可能性を秘めているにもかかわらず，利用者が想定しない方法で事業者がパーソナルデータを利用することでトラブルに発展することや，事業者がプライバシーや個人情報保護に過度に配慮する結果，それらのデータを活用したサービスが活発に創出される状況に至っていないことを示唆している．

国際的に2012年は，本人の忘れられる権利（the right to be forgotten）に始まり，各国でプライバシー・個人情報の国際的な枠組みの見直しが始まった年となった．これは，データは大量に，瞬時に国境を越えることから，ビッグデータの利活用の進展に対応できる新しい枠組みの構築が始まったことを示しており，我が国においてもそのような環境整備の推進が期待される．

本稿は，以上のような課題意識の下で，利用者がより便益を得て，また事業者も効果的な事業展開を推進するために相互にどのような関係性を築くことが必要なのかという点について，欧米や国内の取り組み例を通じて解説する．

利用者による管理

◆ 海外の取り組み

本節では，ユーザを管理者として「個人情報やパーソナルデータ」を取り扱う仕組みについて，欧米で取り組まれている事例を紹介する．なお，本節では，「個人情報やパーソナルデータ」を便宜上，「パーソナルデータ」として述べる．

パーソナルデータ・エコシステム

『プライバシー・バイ・デザイン』[1]の著者であるアン・カブキアン（Ann Cavoukian）博士（カナ

ダ・オンタリオ州プライバシー・コミッショナー）が2011年に『Privacy by Design and the Emerging Personal Data Ecosystem』[3]を発表した．これは，個人が“自分の公式記録”の共有を管理し，何かの目的でその情報にアクセスして使用できる人物（事業者等）についてルールを設定することによって，ユーザを管理者としてパーソナルデータを取り扱う仕組み（パーソナルデータ・エコシステム，以下，PDEという）を提唱したものである．またこの前年に，“パーソナルデータ・エコシステム・コンソーシアム”が設立され，30社以上の事業者が参加し，ユーザ中心のモデルの検討を進めている．PDEにおいて，現時点で成熟しているモデルとしてパーソナルデータ・ヴォールト（Personal Data Vaults，以下PDV）が挙げられている．PDVは，個人が自分のパーソナルデータを完全に自分のコントロール下に置く方法で収集，保管，使用，共有，アクセス権提供，管理することを助けるものである．前記，アン・カブキアン博士のレポートでは，PDVに近いデータ共有プラットフォームの例として，Respect Networkと，Personal.comの2つを挙げている．前者は，プライバシーを保護したパーソナルデータの交換のために相互運用性のあるネットワークをオープン・スタンダードのOASIS XDI（Extensible Data Interchange）プロトコルを基盤に構築したものであり，後者はWebと携帯機器で利用できるサービスである．両者の特徴等を**表-1**に記す．

PDVは，①ユーザのパーソナルデータ（興味，連絡先，所属，好み，友人など）の中心点（結節点）となるものであり，②格納することが選択された情報は，医療や教育情報といった特定のトピックと関係づけることができ，③ユーザが自身のパーソナルデータをコントロールして押し出すこと（controlled push）や，自分の基準（たとえば，自動車保険の最安値）に基づいて異なる情報源からデータを要求して，データを引き込むこと（informed pull）を可能にするものである．これによって，ユーザを管理者として自身のパーソナルデータを取り扱う仕組みができるとされる．なお，PDVの市場は，米国では，

名　称	特　徴
Respect Network	• 異なるプロバイダの複数のPDVの相互運用性と，接続を希望するビジネスとの相互運用性を実現している． • ビジネス・モデルもクレジットカードのネットワークに類似している（クレジットカードのネットワークでは，取引額に応じた手数料を支払うモデルであるが，ここでは，ネットワーク上の消費者間の関係を維持するために手数料を支払う）． • ネットワーク全体のピア・ツー・ピアの評判システム（レイティングのようなもの）が売り手と消費者に平等に適用される．
Personal.com	• 個人が他のユーザ，企業，アプリと個人的なネットワークを通して自分のパーソナルデータの価値を管理，共有，獲得するためのデータ保管場所とツールを個人に提供する． • 個人はPersonalを使って自分の生活と身元に関する構造化データ，メモ，ファイルの集合化，活用，交換が安全にしかも簡単にできる．

表-1　PDVの例

投資規模が100万～1,100万ドルの新興企業で大部分が構成されている．また，英国では，2016年までに3,000万ポンドに達するとされている．

midata（英国）の取り組み

英国政府は，消費者の取引履歴と消費データをコンピュータで処理できるオープン・スタンダード形式で消費者の求めに応じて提供することを義務付ける法的要素を導入する提案を検討している（データ保護法1998（Data Protection Act，DPA）では，個人は企業が保管しているパーソナルデータにアクセスを要求することができるが，その形式については自由裁量に任されている）．

対象となる「消費者の購入・消費に関する取引データ（transaction data）」はデータだけであり，データ保管者が情報について，後に試みたいかなる分析も対象としない．ここで言う義務は，この情報を電子的にすでに保管している企業（特定のセクタ（エネルギー，金融，電気通信分野）を対象）だけに適用される（ただし小規模事業（従業員10名未満）は義務対象外，中小企業も義務免除を検討）．

2012年7～9月にパブリックコメント『midata 2012 review and consultation』が実施され，その法令の具体化が開始されたところである．このような動

きも，前述「PDV のデータを要求して，データを引き込むこと（informed pull）」に類するものであり，これによって，利用者にとっては，最適なサービスの選択が可能になるとともに，これまで価格による供給者側の需給調整の仕組みから，需要側のコントロールへ移行できるのではないかという期待があるものと思われる．

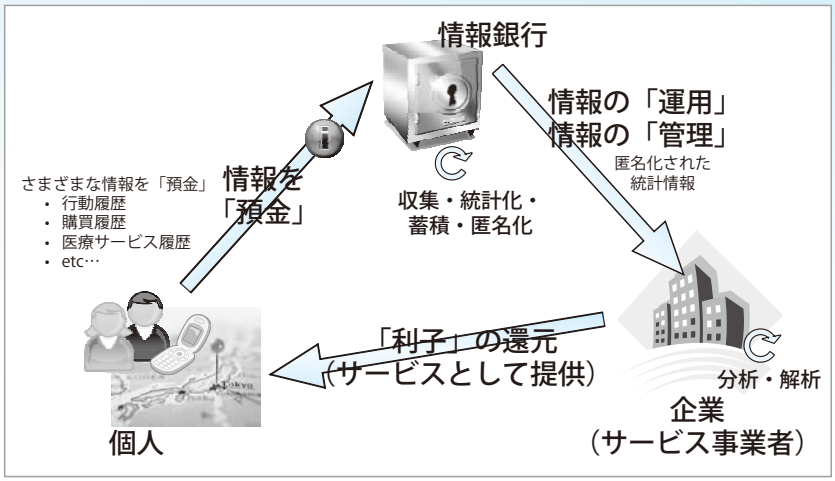

図 -1　情報銀行の考え方

◆ 国内における取り組み

前節でみたような利用者が自身のパーソナルデータを管理するサービスについては，購買履歴の閲覧など一部の情報に限られており，前記 personal.com のような広範囲なパーソナルデータを取り扱うものは少ない．一方で，それを目指す取り組みは，国内でもいくつかある．本節では，情報銀行，PPM（Privacy Policy Manager）について紹介する．

情報銀行

情報銀行（**図 -1** 参照）は，2009 年近未来バリューチェーン研究会（座長：國領二郎慶應義塾大学教授）において，柴崎亮介東京大学教授により提唱された概念である．現状，利用者がさまざまな事業者に分散してパーソナルデータを渡しているため，事業者は正確な個人の情報を持たないことから誤った推測を生み，購買等に結び付けられず，また，利用者も誤った推測（運転免許を持っていないのに，自動車が勧められるなど）により不快を感じるという懸念がある．それらの分散する情報を，信頼できる“銀行”のような機関に預け，利用者の管理の下でデータを取り扱えるプラットフォームについて検討された．この効果としては，集積された情報を，安全に 2 次利用することによって，さまざまな場面に活かす（移動履歴から街づくりに活かす，食事履歴や疾病履歴から疫学研究に活かすなど）ことができることが挙げられる．

当協会の実証実験では，情報銀行によって，時空間（いつ，どこ）を含めた実在確認を行うことで動的なセキュリティが実現できる点などの効果があげられた一方で，事業者の信頼性を既存の認証（JIS Q 15001 や，ISO 27001 など）だけでは担保できないのではないか，との課題も整理された．特に，後者では，民間の認証だけでなく国の機関による監視（第三者機関）の必要性などが指摘された．

PPM（Privacy Policy Manager）

少子高齢化に伴い，生活のトータルライフサポートを目指す事業者が顕在化している．たとえば，ポータルサイトを用意し，日々の購買から健康管理まで提供する試みなどがある．しかしながら，提供する事業者は，サービスを新たに追加するごとに，当該サービスの事業者と利用者との合意を取る必要があり，利用者はそのたびに，長文の約款を読み，合意ボタンを押さなくてはならない．しかし，往々にして，利用者にとってはクリックトレーニング（反射的に同意をクリックすること）となってしまい，後になって問題になるか，または最初から“面倒くさい”という理由からサービス利用までたどり着かないという課題がある．

これらの課題を解決するために，パーソナルデータのライフサイクル（Plan → Do → Check → Action）の中で，適切に保護・管理する基盤として検討されているのが，PPM である（制度課題などを精査するため，IT 融合プロジェクトにおける実証実験として行われている）．具体的に PPM は以下の主な機能から構成されている（**図 -2** 参照）．

①ユーザや状況によって異なるパーソナルデータの保護要求レベルに応じたポリシー設定，パーソナルデータの開示条件の設定機能
②ユーザリクエストによるパーソナルデータ削除機能
③第三者による本人特定を防止するために，個人が特定される可能性がある識別 ID（デバイス ID 等）に対し，サービスごとに異なる仮名 ID を割り当てて個人特定を防止する機能

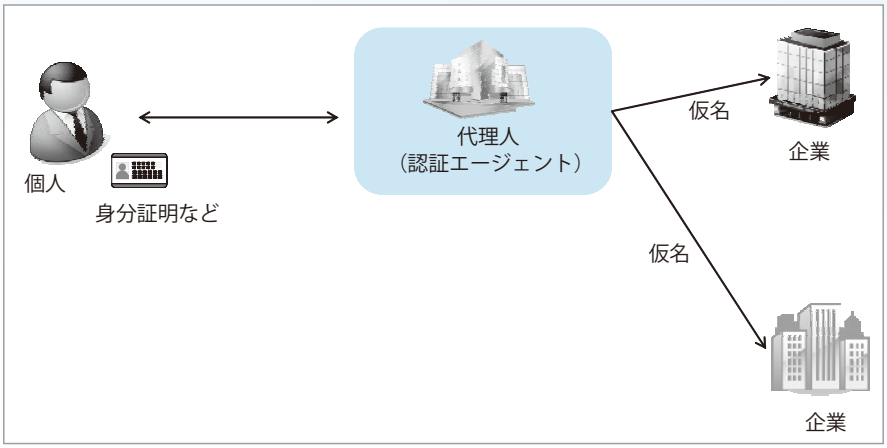

図 -2　PPM の考え方

これを利用する事業者は，たとえば複数の空間（居住地域と，商業圏など）において，この仕組みを適用することによって，利用者のレベルに応じたサービスの提供ができ，また，利用者も PPM の信頼性を担保に，長文の約款を読むことなく（分かりやすい合意を取り），適材適所のサービスを受け，その履歴を閲覧できるとともに，削除要求も可能になることを目指している．

つまり，利用者は当該事業者へ自身の情報を信託し，事業者は利用者の個々の状況に応じて，その代理人となり，基盤上に参加しているサービス提供者のサービスを提供し，サービスのパーソナライズ化を目指すものである．

この実証の中でも情報銀行と同様に，既存の認証だけでなく，第三者機関などの必要性や，本人確認（利用者の実在を何をもって担保するか）の課題などが挙げられている．

信頼関係の構築に向けて

前章で挙げた PDE，情報銀行，PPM の取り組みは，その中央に位置する事業者の信頼性をもって，サービスの便益と個人情報の保護（プライバシーの調整）を両立しようという試みである．そして，これを実現するためには，利用者や企業に何らかの信頼関係が築かれている必要がある．このユーザと企業，企業と企業との間で信頼を確保する仕組みを“トラストフレームワーク”という．今後，サービスのパーソナライズ化やデータ利用が進むにつれて，“トラストフレームワークをいかに構築するか”という点が重要になってくるのではないだろうか．

図 -3 に，就職や転職にトラストフレームワークを適用した事例を示す．一般的に，就職や転職を行う場合，関係する書類（卒業証明書や資格証明など）を郵送等により集め，関係先へ送付する．これをトラストフレームワークに適用すると，本人確認の下で，電子署名が付与された関係する書類を集約し，関係先へ送付することができる．また，従来，その業務等に関係のない個人情報まで提示していた部分がなくなり，必要最小限の個人情報のみを提供することが可能になる．

このトラストフレームワークを構成するプレイヤを**表 -2** に記す．

アイデンティティ・プロバイダ，アトリビュート・プロバイダ，リライング・パーティは必ずしも事業体として切り分けられるわけではなく，同一事

業者が行う場合もあり得る．現状では，アイデンティティ・プロバイダ，アトリビュート・プロバイダおよびリライング・パーティの3つの役割を行政機関や民間事業者が，それぞれ単独ですべての役割を担っている．そのため，ヨコの連携が困難であり，しばしばタテのつながりの断絶が生まれ，煩雑な手続きなどが強いられるという課題がある．これらの問題を解決するには，各プレイヤの信頼性を評価すると同時に，アイデンティティ・プロバイダが，アトリビュート・プロバイダおよびリライング・パーティが求める確かな本人確認を実施し，その結果を関係者全員で互いに信頼しあう（同じプラットフォーム上にのせる）ことで，本人確認をした属性情報が関係者間でタテにもヨコにもつながるようになり，より属性情報が有効に活用されるような環境整備が必要である．

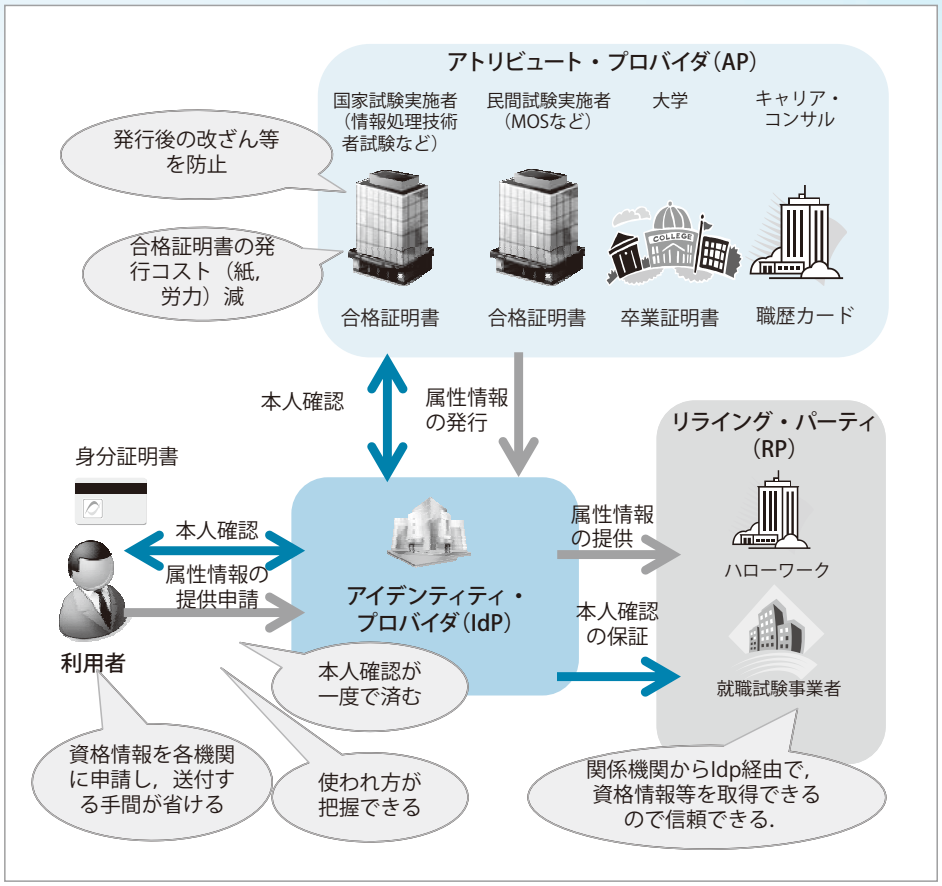

図-3　就職・転職サービスへの適用例

また，トラストフレームワークでは，電子化された個人に関する属性情報が複数の事業者間で交換される．このことは消費者に利便性をもたらす一方，プライバシーやセキュリティに関する懸念を生じさせる．一度漏洩した個人情報を取り戻すことは事実上不可能であるから，漏洩や改ざんなどの事故を未然に防止することが重要であり，プライバシー影響評価（Privacy Impact Assessment，以下PIAという）をリスク管理手法として実施し，プライバシー問題を回避・低減するために，個人情報を取得する情報システムの導入や改修に際し，プライバシーへの影響を「事前」に評価し，設計の変更を促すことが必要になる（なお，PIAの国際標準化状況として，ISO/IEC JTC 1 SC 27/WG 5では，プライバシー影響評価に対しワーキングドラフトとして標準化が検討されている．この標準化にあたっても日本の積極的な関与が必要であろう）．

役割	用語	想定する関係者	図-3での該当者
本人確認を行う者	アイデンティティ・プロバイダ	本人確認を行う行政機関・民間事業者	就職・転職支援事業者（図中のIdP）
属性情報を提供する者	アトリビュート・プロバイダ	属性情報を提供する行政機関・民間事業者	学校，教育機関（図中のAP）
属性情報を受け取る者	リライング・パーティ	属性情報を受け取り，サービスを提供する民間事業者	就職・転職先企業（図中のRP）
（本人確認をされる）対象者	ユーザ	対象者	図中の利用者

表-2　プレイヤと用語

ユーザが理解しやすいようにするという観点から

項目	記述例
取得者	example（http://www.example.com/）
サービス提供に必要な取得される情報	氏名，住所，年齢，性別，趣味，好きな楽曲，好きなスポーツ ･･･
取得者の分析に取得される情報	IP アドレス，位置情報 ･･･
オプトアウトの方法	コントロール画面よりチェックボックスを外す
取得元	Web ページより利用者が入力したもの
取得時	約款の『同意ボタン』を押したときから
利用目的	1. 友人と状況を共有するため ･･･
利用期限	ユーザ登録を抹消するまで
開示先	自分とユーザのタイムラインおよび ･･･
2 次利用の有無	有
2 次利用の情報項目	性別，IP アドレス ･･･
2 次利用の目的	新サービスの研究・開発 ･･･
2 次利用の方法	識別情報を削除して個人を特定できない状態で利用（データサンプル http://www.example.com/sample）
第三者提供の有無	有
第三者提供の情報項目	性別，趣味 ･･･
第三者提供の目的	広告精度の充実 ･･･
提供先	Google，マイクロソフト ･･･
基本契約	2011 年 ･･･
第三者評価	ToS-DR での評価（http://tos-dr.info/）Example レーティング
規約の変更	7 日間の掲示をもって変更

表 -3　情報共有標準ラベルの例

は，利用者への利用規約やプライバシーポリシーを分かりやすく通知することで解決をはかることも必要である．対応策として，カンターラ・イニシアティブや，IT 融合パーソナルデータワーキンググループで検討されている“情報共有標準ラベル”[4] などを適用することが有効であろう（**表 -3** 参照）．また，

事業開始前に相談する仕組みや，トラブル等があった場合に分野横断的に判断する仕組み（駆け込み寺のような存在）などの検討が必要であろう．

情報の流通はグローバルに展開されるものであり，パーソナルデータも，その利活用にあたっては，国境を越えて相互利用される可能性も高い[5), 6)]．そのような状況において，国際連携の仕組みの構築を前提にした安心・安全なフレームワークが構築されることを期待している．

参考文献

1) 堀部政男・JIPDEC 編：プライバシー・バイ・デザイン，日経 BP（2012）．
2) POU 情報利活用の法制度に関する調査研究報告書，JIPDEC（2011）．
3) Cavoukian, A. : Privacy by Design and the Emerging Personal Data Ecosystem（2012）．
4) パーソナルデータ利活用の基盤となる消費者と事業者の信頼関係の構築に向けて，経済産業省（2013）．
5)「パーソナルデータの利用・流通に関する研究会」報告書，総務省（2013）．
6) 坂下哲也：パーソナル情報を取り巻く最近の動向，信学技報（2012）．

（2013 年 6 月 3 日受付）

坂下哲也｜sakashita-tetsuya@jipdec.or.jp

データベースエンジンや OS にかかわるシステム化計画の立案，要求定義の作成，基本設計等上流工程の業務に従事した後，2002 年度より（財）データベース振興センターにて，「g コンテンツ流通基盤整備」等の実施責任者を務める．2008 年，（財）日本情報処理開発協会（当時，現 JIPDEC）電子情報利活用推進センター副センター長に就任．2013 年 4 月より現職．IT 戦略本部電子行政オープンデータ実務者会議データワーキンググループ構成員，ISO IEC JTC 1 SC 27/WG 5 エキスパート．