
# PwC's Privacy Insights 2021

pwc

www.pwc.com/jp

# はじめに

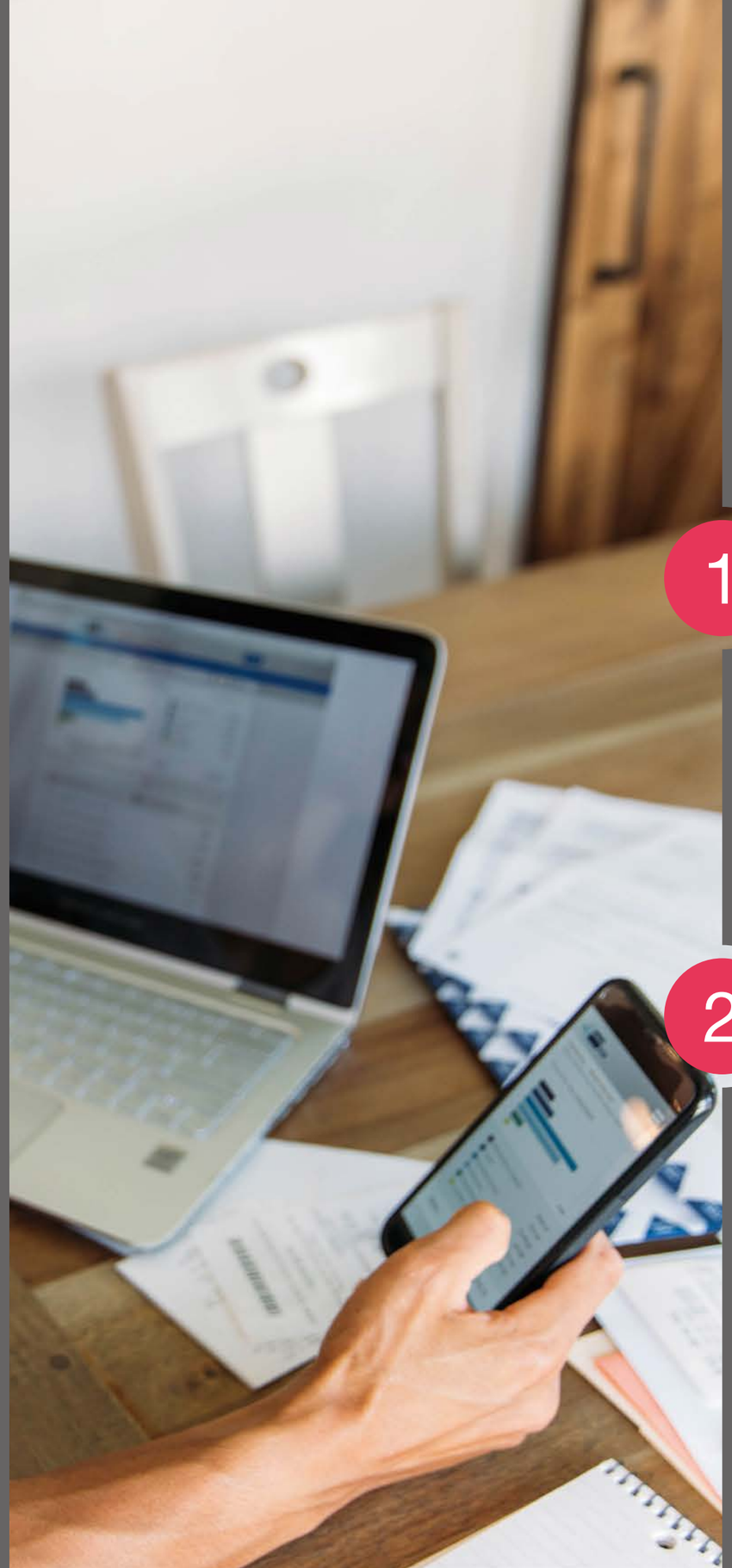
今後わが国が目指すべき社会の姿は、「サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会」だと考えられています。このような社会の実現にあたっては、官民によるデジタル・トランスフォーメーション（DX）の推進が重要かつ必要です。その中で企業は、イノベーションの中心的な役割を担うとともに、イノベーションによって生じる新たなリスクの管理を組織的に実施することが期待されています。

新たなリスクのひとつが、データを提供する個人のプライバシーを侵害してしまうリスクです。もちろん、同様のリスクはこれまでも存在していました。しかし、従来のウェブ上のデータに加えて、無線通信やセンシング技術の進展に伴いインターネットに接続されたあらゆるモノが生み出す膨大な量のデータとその利活用の状況や、いわゆるAIを用いたデータアナリティクスの実用化の進展などを踏まえると、プライバシーに関するリスクはこれまで以上に増大していると考えられます。

また、プライバシー問題への取り組みの難しさのひとつに、プライバシーに関する個人の受け止め方や社会的な受容水準が、コンテキストや時間の経過によって変わり得るという点が挙げられます。そのため、たとえ法令などを遵守していたとしても、多様なプライバシー意識の変化に対応することができなければ、データを提供する個人が不安を感じ、企業から提供されるサービスやプロダクトを拒絶する、あるいは社会的な批判を受けてレピュテーションに深刻なダメージを受けるといった恐れがあります。

増大するプライバシーに関するリスクを、その特徴を踏まえた上で適切に管理しつつ、データの利活用を推進するためにはどのような取り組みが必要でしょうか。法令などの遵守は当然として、プライバシー保護に関する自社の取り組みを能動的に、ビジネスパートナーや消費者などのステークホルダーに対して開示・説明し、そこから得られるフィードバックを踏まえて施策を改善し続ける、そうすることで社会から信頼を確保することが重要です。

本レポートでは、弁護士、データアナリティクスや情報セキュリティ／プライバシーに関わるコンサルタント、そしてアシュアランスやリスク管理の専門家がそれぞれの知見を持ち寄り、今後企業に求められるプライバシーに関するリスクへの対応を多角的に検討していきます。



# Agenda

# 1 AIおよびアナリティクス活用における プライバシーの論点

## 1. パーソナルデータのグループ内共同利用に必要なオプトイン

今やデータは企業活動を支える重要な資源であり、データ活用の推進は企業のビジネス拡大のための戦略課題である。数あるデータ資源の中でも、B2C企業を中心に最近特に注目を集めているのが、パーソナルデータである。パーソナルデータとは、個人の氏名や年齢、行動データ、購買履歴といった個人に関するデータ群の総称で、特定情報に絞られず広く定義されている。

### 1. パーソナルデータの活用目的の代表例

パーソナルデータの活用目的は、昨今の感染症対策を代表とした政府や関連する公共機関が主導する公共目的と、一般企業の事業目的に大別されるが、一般企業の事業目的をさらに分類すると次の4つに整理できる。

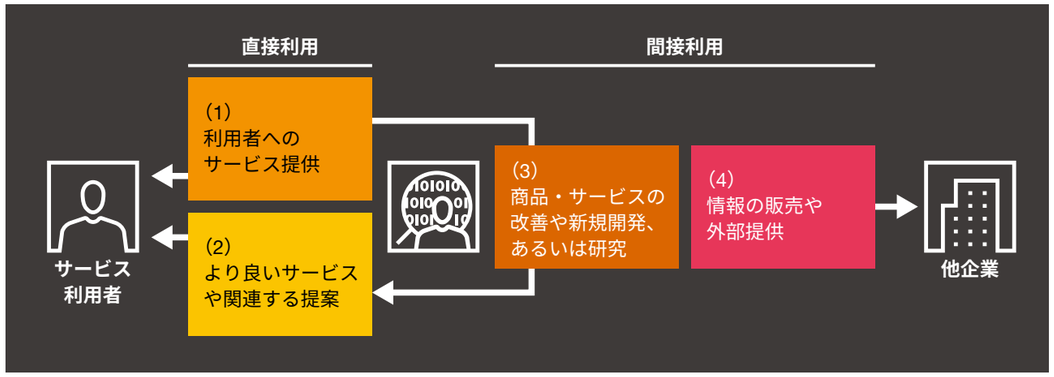
(1) 利用者へのサービス提供（それに必要な渉外活動を含む）
(2) よりよいサービスプランや関連するサービスの提案（情報提供とそれに必要な渉外活動を含む）
(3) 商品やサービスの改善や新規開発、あるいは研究
(4) （利用者へ不利益を出さない配慮を行った上での）情報の販売や外部提供

これまで、一般企業の事業目的達成を念頭に置いたパーソナルデータの活用は、多くの場合、自社内で（1）～（3）のサイクルを回してきた。近年は、利用者に多くの利点／付加価値をもたらすことを前提に、多事業展開している企業においては、グループでデータの共同利用を進め、顧客のさらなる拡大や囲い込みのために活用することが戦略的施策になっている（図表1）。

### 2. パーソナルデータ活用の第一歩は、正しい取り扱い環境の整備から始まる

このように、パーソナルデータの利活用は企業にとって大きな可能性を秘めている。一方で、消費者のプライバシー意識が年々高まっていることを踏まえると、彼らの期待や意向に反したデータの利活用が、企業イメージの低下や顧客離反を招きかねないリスクをはらんでいることを忘れてはならない。法規制に従うのはもちろんのこと、利用者が不利益を被らないよう配慮し、安心・安全にパーソナルデータを取り扱う環境を整えることが求められる。以下に、企業グループがまず取り組むべきことをまとめる。

**図表1：パーソナルデータの活用目的の代表例**




**ポイント（1）：グループ共同利用に向けたプライバシーポリシーの見直し**

多事業展開している企業においては、サービスによっては別法人が主管になっている、といったケースが見られる。このような場合、パーソナルデータを利活用するためには、サービス横断での利用目的とグループでの共同利用（あるいは第三者提供）の明示を含め、統合的なプライバシーポリシーの策定を行い、利用者本人からの同意を得る（オプトイン）ことが必要になる。利用者への不利益がないことを前提に、グループでの共同利用に向けた目的と内容の再定義の検討から始めることになり、多くの場合、個人情報の管理主管も再定義することになるであろう（オプトインについては後述する）。

**ポイント（2）：個人情報の管理・活用に向けた社内環境の再整備**

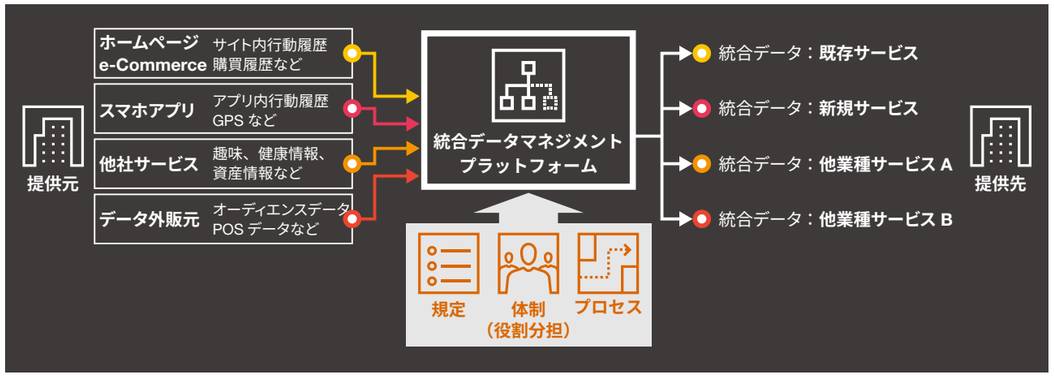
続いて重要視されるのは、厳格なプライバシー保護対応を含め、データガバナンス態勢をきちんと構築することである。態勢整備は、プライバシーに関連するリスク管理の規程類の策定・更新と周知徹底、プライバシーに関する相談窓口の設置、チェックシートに基づきサービス企画・変更内容の審査を網羅的・複眼的に行うプロセス整備が重点施策となるであろう。プライバシーガバナンスに関する取り組みは、法務やセキュリティなどの他のガバナンスとの整合性をとる必要があるため、当初の想定よりも時間をかけて検討を進めることが求められる傾向にある。そのため、計画時には考慮が必要である。

これらの活動を通してパーソナルデータの保護ガバナンスに目途を付けつつ、データの一元管理を担う情報基盤（統合データマネジメントプラットフォーム）を整えることで、データ活用ガバナンスの推進が可能となる。これにより、利用者目線での連携サービス提供とパーソナルデータの有効活用への道筋ができるのである（図表2）。

### 3. オプトインの先進的な事例

さまざまなサービスで生成されるパーソナルデータを流通・統合することは、企業や個人にとって新たな価値を生み出す半面、プライバシーリスクを多く含むことは前述の通りである。個人情報については、多くの国や地域において、その利用や第三者提供を行う前に本人の同意を取得することが求められている。そのため、既存のサービス利用者などからあらためて同意を取得することは非常に負荷が高く、また乱暴な手法では利用者の離反を招くリスクもある。業態やサービスを超えたパーソナルデータの利用について、旧来のように書面や電子メールでの通知やウェブサイトでの公開といった一方的な文書の押し付けと捉えられるような手法をとっていては、法的要求事項をクリアしたとしても、利用者の期待に応えているとは言い難いであろう。先進的と呼べる事例では、法的な要求事項を満たす文書の通知や公開によらず、2つの点を踏まえて、サービス利用者をはじめとするデータ提供者（データ主体）との相互理解を図っている。

**図表2：グループ共同利用のための統合データマネジメントプラットフォーム（イメージ）**



**1. プライバシーに対するコンセプトの提示**

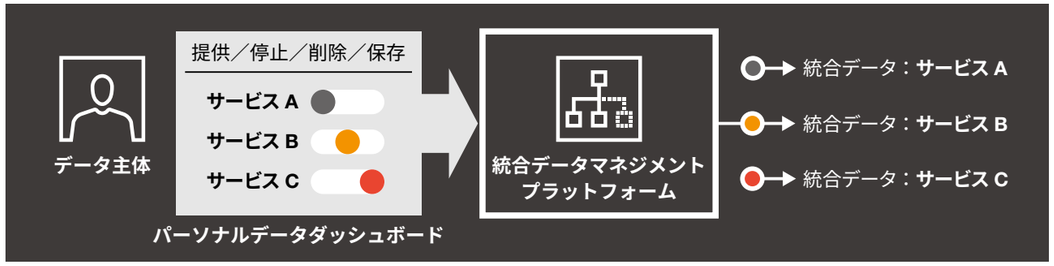
法的文書で全ての利用者から理解を得ることは非常に困難である。そのため一部の企業では、ウェブ動画やテレビCMなどを利用して、プライバシーの保護をどのように実現しているか、そのコンセプトについて利用者に理解してもらうための場を提供している。また、センシティブな情報を提供することで発生するリスクやその対処方法について、動画を用いた研修や簡単な試験を実施した上で、サービスやプログラムへの参加を認めるケースもある。

**2. サービスやデータの可視化、コントロールUIの提供**

データ主体による積極的なデータコントロール権を認める法制度が、世界各国で取り入れられている。一方で、実際の手続きは煩雑かつ書面を利用したアナログな方法が採用されており、データ主体にとってはストレスフルな状態となっている。一部の企業や組織では、データを提供している企業やサービスの一覧、企業のデータの利用状況を可視化したダッシュボードを設け、同一のユーザーインターフェース（UI）から利用停止や削除などに関するコントロールをデータ主体が行えるようなUI・機能を提供している（図表3）。

規約書や契約書などで説明責任を果たすという一方的なアプローチだけでなく、利用者とコミュニケーションをとりながら透明性を増していくアプローチが、今後主流になると考えられる。デジタルを取り入れたコミュニケーションを通じて利用者のプライバシーに関する感度や期待値を明らかにすることで、真に納得した状態でパーソナルデータの利用を行うことができるであろう。

**図表3：データ主体による積極的なデータコントロールのためのUI・機能（イメージ）**






## 2. レコメンデーションで注意すべき「放っておいてもらえる権利」

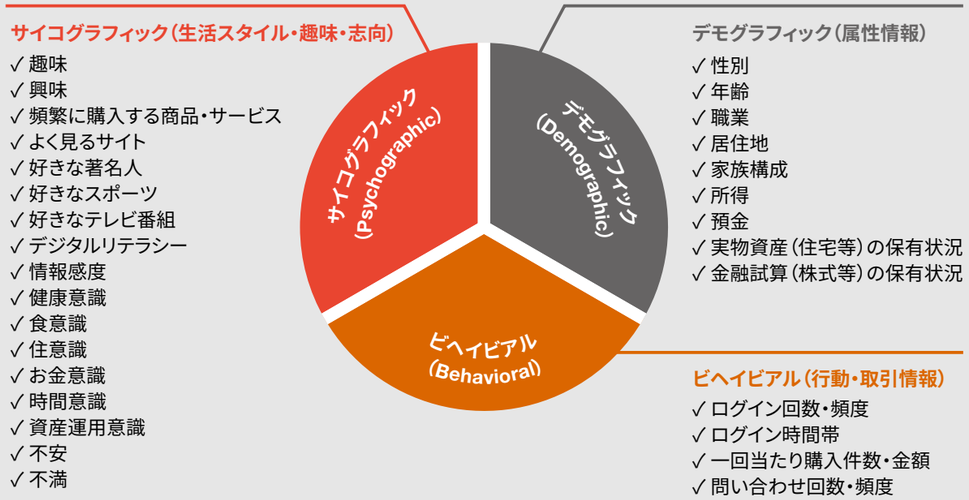
新型コロナウイルス感染症（COVID-19）が世界的に流行する現在、対面でのコミュニケーションは極端に制限され、オンライン会議やECサイトなどの非対面チャネルの活用に拍車がかかっている。これまでECサイトをあまり活用してこなかったユーザーは、至る所で商品を「おススメ」されることに驚いたかもしれない。この「おススメ」機能はレコメンデーションと呼ばれ、消費者（顧客）の購買意欲を大いにかき立てるものになっている。レコメンデーションの進化とそれに伴う弊害、今こそ企業に求められるレコメンデーションの在り方を解説する。

### 1. レコメンデーションがビジネスを左右する時代

国内広告費のうち、インターネット広告費がテレビメディア広告費を超えたことは、記憶に新しいニュースである[1]。インターネットが広告業界の主戦場となることで、企業には、従来のテレビに向けた広告とは異なるマーケティング手法が求められている。

テレビにおける広告は、不特定多数の消費者に向けた「マス・マーケティング」が主流であった。対照的にインターネット広告は、少数の特定消費者に対して広告を配信する。消費者の属性情報（年齢・性別など）、性格情報（趣味・嗜好など）、行動履歴（購入回数・ページ遷移履歴など）を分析し、ニーズに合致した消費者にアプローチすることで、広告に対する反応率（Conversion Rate：CVR）を高めることが可能となる（図表4）。インターネット技術の発達によって、企業はこれら消費者の情報を容易に取得できるようになり、誰に何を「おススメ」すべきかという選択肢の幅が広がった。このような背景から、現代においては「よりレコメンデーションが求められる時代」になったと言える。

**図表4：消費者（顧客）情報の例**




出典：Arthur M, Hughes，1999.『顧客生涯価値のデータベース・マーケティング』ダイヤモンド社．をもとにPwC作成

## 2. 進化していくレコメンデーション技術

より効率的な「レコメンデーション」を行うためには、レコメンデーションの種類と手法に対する理解を深めることが重要である（図表5）。どのような情報をもとにレコメンデーションを実施するかを見定めることで、意味のある顧客の分類が可能になる。例えば、流通小売業のように商品数が多く、購入サイクルが短い商品を扱う企業においては、協調フィルタリング（顧客の行動履歴や、顧客と似た性格情報を持つ別の顧客の行動履歴からおススメを決める手法）に代表される「アイテムベース」でのレコメンデーションが適切であると考えられる。そのために、顧客の購買履歴に着目し、顧客が「何を買ったか」で分類する必要があることは自明であろう。

また、レコメンデーションの精度を維持するためには、逐次レコメンデーションモデルの見直しを行う必要がある。一般に、作成したモデルは時間の経過と共に精度が劣化していくものと考えられている。なぜなら、環境や対象となる顧客自身が時間の経過によって変化していくためである。精度の高いレコメンデーションを維持するためには、継続してデータを収集し、モデルを改善し続ける「仕組み作り」が重要になる。

新しく、より適切なレコメンデーション技術に対応していくため。そして、過去に作成したレコメンデーションモデルが時間とともに劣化していくため。これらの理由から、企業は自社のレコメンデーション技術を日々改善、進化させていく必要がある。

## 3. レコメンデーションで考慮すべき「放っておいてもらえる権利」

ただ、レコメンデーション中に「嫌悪感」を抱く顧客がいることも忘れてはならない。必要のないタイミングで商品をおススメされたり、まったく関心のない商品をおススメされたり、はたまた欲しい商品が当てられ自己の内面を覗かれているようで、逆にストレスを感じたという方もいるかもしれない。レコメンデーションの目的は「顧客が商品やサービスを必要とするタイミングを当てる」ことではなく「実際に購買を促すこと」であるから、レコメンデーションが顧客の「嫌悪感」につながり、商品やサービスに対するネガティブな感情を抱かせてしまっては、逆効果になってしまう。企業には、「放っておいてもらいたい」顧客に配慮することも求められる。

諸説あるが、プライバシー保護の活動は「個人情報」「私的領域」「個人の自律」のそれぞれを対象に構成される（図表6）。従来、特に法務や情報システムの業務領域では、個人データの適正利用や漏えい防止などの「個人情報」の保護に重点が置かれていた。一方、ユーザーサービスの充実や顧客ロイヤルティの向上という観点では、私生活へむやみに干渉しないという「私的領域」の保護、つまりは「放っておいてもらえる権利」への配慮とのバランスが重要になる。

特にレコメンデーションについては、（1）過度なアプローチを控える（2）私的情報に踏み込み過ぎないという2点が、サービス設計の中で検討すべき項目となる。

**図表5：レコメンデーションの種類と手法**

| 種類 | 概要 | 活用が多い業種 | 主な関連手法 |
|---|---|---|---|
| ① アイテムベース | 商品、サービス間の関連性（併売、同時閲覧等）の強さによるレコメンド | 流通小売など、特に商品数が多く購入サイクルが短い業種 | ✓ アソシエーション<br>✓ 協調フィルタ |
| ② ヒトベース | 顧客類似度（行動パターン、嗜好性等）によるレコメンド | 流通小売など、特に商品選択に嗜好性などの顧客特徴が強く影響する業種 | ✓ クラスタリング<br>✓ 商品DNA |
| ③ イベントベース | 取引状況や個人属性の変化をトリガーとしたレコメンド | 銀行、証券、保険、自動車など、ライフステージ等の変化がニーズに影響する業種 | ✓ ベイジアンネットワーク<br>✓ パス解析 |
| ④ 予測モデルベース | 商品やサービス単位で購入予測モデルを構築、予測結果によるレコメンド | 銀行、自動車、製薬など商品やサービス数が少ない業種 | ✓ 決定木<br>✓ ランダムフォレスト<br>✓ ディープラーニング |
| ⑤ その他 | ・目的別のレコメンドアイテム抽出<br>・レコメンドの全体最適化 | 流通小売など商品やキャンペーン数が多い業種 | ✓ シミュレーション<br>✓ 時系列予測 |



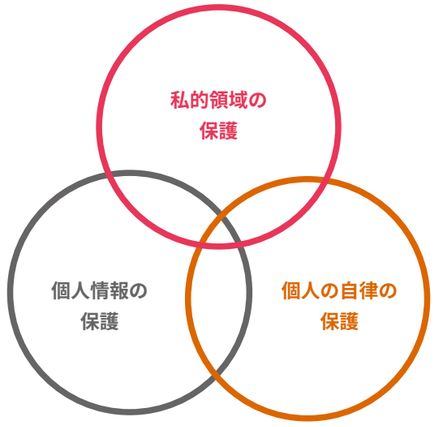
**1. 過度なアプローチを控える**

過去にはダイレクトメールの大量配信、そして最近では動くオーバーレイ広告など、目的を見失って手段に走ってしまい、送信数やクリック数を稼ぐだけでユーザーに「嫌悪感」を抱かれてしまった例は数多くある。ユーザーの私的領域に接するブラウザ上の行動・体験を妨害するアプローチでは、購買活動につながる可能性は低くなる。

**2. 私的情報に踏み込み過ぎない**

レコメンデーションは精度の高いモデルであるがゆえに、顧客のセンシティブな情報を推測することが容易になってきている。例えば、食料品の購買履歴の変化から、当該顧客が妊娠中と推知し、関連商品やイベントをダイレクトメールで案内することが技術的に可能であっても、受け取った側が心地よく感じるとは限らない。病歴や性癖、趣味嗜好など、場合によっては同居する家族にも知られたくない情報があるかもしれない。企業は、レコメンデーションを通じて顧客の知られたくない情報に気付かぬうちに触れてしまっているかもしれない点を考慮する必要がある。

**図表6：プライバシー保護の対象領域**




## 4. いま求められる「オモテナシのレコメンデーション」

レコメンデーションにおいて検討すべき上記2つの課題に対して、企業は以下の対策を講じる必要がある。

**1. 精度を向上させ、かつ適切なタイミングで行う**

「過度なアプローチを控える」ためには、「精度」と「タイミング」が重要になる。取得可能なデータの広がりと、ディープラーニング（深層学習）といった人工知能（AI）技術の発展により、レコメンデーションの「精度」は飛躍的に高まっている。精度の高いレコメンデーションは顧客にとって関心のないおススメを減らし、心理的なストレスを軽減させることにつながる。また、本当にそれを必要とする「タイミング」において適切なおススメを行うことで、レコメンデーションを過度なものと思わせないことも重要である。

**2. インプットとアウトプットを精査する**

「私的情報に踏み込み過ぎない」ためには、「インプット」と「アウトプット」が重要になる。「インプット」として使用するデータの中に、顧客が他人に知られたくないであろう情報をもとにしたものはないか、「アウトプット」としておススメする内容に、他人からアドバイスを受けたくない情報が含まれていないか。おススメされる顧客が気持ちよく情報を受け取ることができるか、企業は十分に検討・精査をした上で発信する必要があるのである。

インターネット技術の進化によって注目を集めるレコメンデーション。必要な時に必要な情報を届けてくれたり、顧客が気付いていなかった潜在的な購買意欲を引き出したりと、情報を発信する側と受け取る側の双方に恩恵をもたらしている。だが、取得または提示可能な情報が増えたことにより、新たな弊害も生まれている。これからの時代に求められる真のレコメンデーションとは、企業がAI技術を駆使しながらプライバシーに配慮し、顧客が安心してサービスを利用できる「オモテナシのレコメンデーション」なのかもしれない。

# 3. データマネタイズで実施すべき匿名化加工

2018年に経済産業省が『DXレポート ～ ITシステム「2025年の崖」克服とDXの本格的な展開～』を発表してから、デジタルトランスフォーメーション（DX）は企業の経営アジェンダとして全社規模での推進が加速され、事業効率化・高度化に向けたデータ利活用が浸透してきている。本章ではデータ利活用に対する機運が高まりつつあることを踏まえて、データ利活用の新たな可能性としてのデータマネタイズ（データ外販）およびその課題に関して説明していく。

## 1. 重要な事業アジェンダを導くデータマネタイズ、4つの具体化方針

テクノロジーの発展に伴い、企業に集積されるデータは増加傾向にある。企業は集積したデータを用いた既存事業の効率化・高度化を推進する以外に、データ利活用による新規事業組成（データマネタイズ）に対する期待を高めている。

データをマネタイズしていくには自社内で保有しているデータの独自性（種類）、需要（想定活用先の規模）の状態に鑑みて利活用の仕方を検討することが必要となる。以下の図表7で、データマネタイズを具体化させるために企業に求められる方針を説明する。インサイトの活用度合い（高低）と対象となるデータセット（シングルドメインデータ、マルチドメインデータ）に照らし合わせて、4つに分類することができる。

**（1）生データ（個人情報）の外部提供**

購買・顧客データなど自社に集積しているデータを外部販売する。

**（2）インサイトの外部提供**

自社に集積しているデータを対象に、アナリティクスにより導出したインサイトを付加価値として外部販売する。

**（3）データバンドル、マルチドメインデータの外部提供**

自社サービスの利用者属性の情報提供など、既存サービスへの付加価値として外部販売する。

**（4）新製品・サービスの追加**

自社で集積しているデータを梃に新規サービス（自社顧客基盤を活用した新サービス）を提供する。

各社が保有するデータの独自性、需要を互いに補完するために、データアライアンス（複数社でデータを提供し、アライアンス内で価値創出を狙う）組成を行う動きが出てきている。こうした状況を踏まえると、データマネタイズの検討はデータ利活用の新たな可能性として、重要な事業アジェンダになることが想定される。

**図表7：データマネタイズにおける4つの具体化方針**


## 2. データ価値とプライバシーのトレードオフ

ただし、どのデータマネタイズ方針を採るにしても、プライバシーの考慮は欠かせない。ここで言うデータは、加工手法により「生データ」「仮名加工情報」「匿名加工情報」「統計化された情報」の4種類に分けることができる（図表8に定義を記載）が、2018年に施行された欧州一般データ保護規則（GDPR）、2020年から施行されたカリフォルニア州の消費者プライバシー法（CCPA）、2020年6月に可決・成立した日本の改正個人情報保護法など、各国の法令では「個人情報」（生データ）が主たる規制の対象となり、「匿名加工情報」や「統計化された情報」は要件が緩和される。しかし、これらを巡っては、未だに（1）「匿名加工情報」の加工手法の難しさ、（2）高度なインサイトの導出が困難、という2つの課題がある。以下にそれぞれの内容を記す。

**（1）「匿名加工情報」の加工手法の難しさ**

「匿名加工情報」の加工手法に関する誤解は未だに少なくない。例えば氏名や住所などを情報から削除する、ユーザーの氏名をIDに置き換えるといった加工だけでは「匿名加工情報」にはならない。個人を識別できる記述などをデータベースから削除したり、個人の特異性がある情報を上位概念や数値に置き換えて一般化したりといった対応が必要となる。個人を特定できる可能性を確率的に下げるのではなく、特定できないように非可逆な手法を施す必要がある。

**（2）高度なインサイトの導出が困難**

「生データ」「仮名加工情報」「匿名加工情報」「統計化された情報」の一つ一つは、「利用」の視点と「管理」の視点に鑑みると二律背反の関係にある。「生データ」は、ユーザーの特性から購買の傾向などのさまざまな情報を特別な加工なしに利用できるため汎用性が高いが、各国の法令の対象となり、さまざまな対応施策を求められる。一方、「匿名加工情報」や「統計化された情報」は法令の要件が緩和されるものの、個人を特定できないようにするための高度な加工を求められるため実装が難しく、また情報量の低下により高度なインサイトの導出が困難というデメリットがある。

2020年に公布された日本の改正個人情報保護法では、他の情報と照合しない限り、特定の個人を識別することができない情報（仮名加工情報）が、新たなデータ形態として追加された。当形態に該当すれば、ユーザーに通知していな

**図表8：各データ形態の定義と利用・管理する際のメリット／デメリット**

流通性 低 ↓ 高　汎用性 高 ↓ 低

| データ形態 | 定義 | 利用視点 | | 管理視点 | |
|---|---|---|---|---|---|
| | | メリット | デメリット | メリット | デメリット |
| 生データ（個人情報） | 顧客や店舗のデータに対し、特に加工なくそのままの形態で流通させる情報<br><br>例：無加工の購買情報、顧客情報 | 加工に伴う情報の損失がなく、最も汎用的に利用可能 | 利用先や目的に対し、最も厳しい制限が課せられる | 加工方法の検討は不要で、安全管理措置のみ講じればよい | 厳格な管理が求められるため、利用サイドとの調整が困難 |
| 仮名加工 | 生データから特定の個人を識別できないように氏名や識別符号などを削除等の加工を実施したもの<br><br>例：氏名や住所等を除外しIDのみを残した購買情報 | 内部利用用途では生データに準じた汎用性で利用可能 | 外部流通は生データと同様の制限が課せられる | 社内に限定した規律の緩和が可能 | 仮名加工されたデータの複製や再加工など亜種の管理が困難 |
| 匿名加工 | 特定の個人が識別できず、個人情報が復元できないように加工を実施したもの<br><br>例：個人情報やID、個人の特異性を排除して抽象化した購買情報、顧客情報 | 自社内外でのデータ流通や利用目的外の利用が可能 | 特定ができないという性質上、ダイレクトマーケティングなどの用途には利用できない | 最低限の安全管理措置を講ずればよい | 匿名化加工の妥当性判断が技術的に困難で、実装が最も難しい |
| 統計化 | 生データなどに対し、共通の分類軸に基づく集計や抽象化などの加工を施し、構成する個別の顧客や店舗を特定できないようにしたもの<br><br>例：商品ジャンルや時間帯、顧客属性などでサマリーにした購買情報 | 最低限の規律でデータを利用可能 | 市場動向の整理などマスを捉える用途でしか利用できない | 他の社外秘情報と同程度のレベルで管理が可能 | 情報資産管理の枠組み外と誤解を招き、利用サイドの一存での利用が生じやすい |

い利用目的への変更が可能になるため、これまでより要件が緩和されたが、内部での分析・利用に限定されている。

これらの背景を踏まえ、企業のコンプライアンス部門は、法律を遵守するために、データ形態や加工手法に係るアドバイスを事業部門に提供する必要がある。事業部門はこれを踏まえながらも、流通性と汎用性を適度に維持しながら自社のデータマネタイズを成功させるために、ベストなデータ形態を選択する必要がある。

## 3. データマネタイズの成功に向けて

ここからは、データマネタイズを成功に導くために企業に求められるアクションを、前述の4つの具体化方針に沿って紹介する。前提として、事業戦略上考慮すべきプライバシーがそもそも異なることを理解しておくことが重要である。

各データマネタイズ方針における必要なデータ形態を以下に示していくが、データ形態としての「生データ」に関しては各国の法令の対象となり、さまざまな施策が求められるため、自社の既存・新規サービスの運営においてのみに限定するなど、最小限の利用にとどめる必要があると言えるであろう。

### (1) 生データの外部提供：外部提供先を考慮したデータ形態の選定

自社に集積しているデータを自社内の他部門のみならず、グループ会社に公開するといった場合は「匿名加工情報」を前提としておき、広く社外にデータを販売・提供していく場合は「統計化情報」を前提として事業計画を策定していくなど、自社内・グループ会社内のデータガバナンス状態も踏まえることで、求められるプライバシーを考慮することが可能になる。

### (2) インサイトの外部提供：インサイト導出時を考慮したデータ形態の選定

「統計化情報」がインサイトそのものとして外部提供される場合が想定されるが、インサイト導出過程での情報漏えいなど不測の事態も考慮し、「匿名加工情報」の利用が最適だと言える。

### (3) データバンドル・マルチドメインデータの外部提供：段階に応じた複層的なデータ形態の選定

マルチドメインデータの外部提供は、「(1) 生データの外部提供」の場合と原則的に同じ扱いとなり、広く社外にデータを販売・提供していく場合は「統計化情報」を前提とするが、グループ会社からはデータ提供を受ける場合もある。そのためグループ会社へのデータ販売・提供は「匿名加工情報」を前提としつつ、自社データおよびグループ会社データを掛け合わせることも想定し「仮名加工情報」も選択肢に入れた上で、流通度合いに鑑みたデータ形態の選択が必要だと言えるであろう。

### (4) 新製品・サービスの追加：データ流通状態を踏まえたデータ形態の選定

新製品・サービスの追加では、企画から市場への提供に至るまでの各段階でマルチドメインデータの利用が想定される。データ集積時は「(3) データバンドル・マルチドメインデータの外部提供」と同様に「匿名加工情報」ないし「仮名加工情報」を選択肢としつつ、新製品・サービス創出につながる社内利用を想定したインサイト導出などの企画時は「(2) インサイトの外部提供」と同じくインサイト導出時の不測の事態も考慮して「匿名加工情報」を利用していくなど、推進状況に応じて最適なデータ形態を選択する必要がある。

企業に集積されたデータ利活用の新たな可能性としてのデータマネタイズ。今後さらにテクノロジーが発展することが予想され、利活用可能なデータが増加し続けるであろう環境下、データマネタイズが当たり前のように事業戦略におけるオプションとなる日が近い将来訪れる可能性は、日々高まり続けている。

**図表9：データマネタイズの各具体化方針における必要なアクション**


# 4. ユーザー行動履歴の活用における落とし穴

## 1. ビッグデータとAIが実現する「人間中心の社会」

内閣府は「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、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）」であるSociety 5.0[2]の実現を目指している。人々のニーズが多様化する中、モノやサービスを、必要な人に、必要な時に、必要なだけ提供することで、快適で活力に満ちた、質の高い生活を実現すると同時に、社会システム全体を最適化し、経済発展と社会的課題の解決を目指すとされている。

こうした「人間中心の社会」を実現するためには、サイバー空間および（IoTなどを活用して）フィジカル空間から取得できるビッグデータを人工知能（AI）技術を駆使して分析することで、人々の嗜好や関心事、生活様式や置かれている環境、ライフイベントやライフステージを把握し、人々の顕在化した、あるいは潜在的なニーズに応じた、適切なモノやサービスが提供される必要がある。簡単に言えば、生活者一人ひとりを知り、一人ひとりに「パーソナライズされた体験」が提供される必要があるのである。

例えば、ユーザーのECサイトでの行動履歴と、現在地情報、近隣店舗のリアルタイムの在庫情報を組み合わせれば、ECサイトで商品Aをカートに入れたまま購入に至っていないユーザーに対して、現在地の近くの店舗に商品Aの在庫があることを知らせると同時に、30%引きのクーポンを届けることが可能である。あるいは、あるころから紙おむつや粉ミルクを購入するようになり、その後、赤い小さな長靴や、傘に興味を示していることがウェブサイトの閲覧履歴から分かっているユーザーに対しては、粉ミルクを買い始めてから6年後の春に、赤いランドセルを紹介することができるであろう。

このように、「人間中心の社会」を実現する上では、ユーザーのオンライン、オフラインの行動履歴に基づいてパーソナライズされた体験を提供することが鍵となる。本稿では、この行動履歴を活用するにあたっての注意点を解説する。

## 2. 拡大するパーソナルデータ活用とそこに潜む落とし穴

ユーザーのECサイトでの行動履歴や購入履歴、現在地情報などは、その匿名性の有無に関わらず一般的に「パーソナルデータ」と呼ばれる。パーソナルデータは、一人ひとりに合わせたパーソナライズされた体験を届ける上で、なくてはならないものである。こうしたデータ単体は、各法制度で保護の対象として規定される「個人情報」ではないと整理されるケースがあるが、パーソナルデータは容易に「個人情報」と紐づく恐れがあることに注意する必要がある。

例えば、ある新規ユーザーがECサイトで商品を閲覧し、いくつかの商品をカートに入れるとする。これらの行動履歴だけでは、個人情報には該当しないパーソナルデータであると言えるであろう。しかし、ユーザーが実際に商品を購入するために、住所や氏名、クレジットカード番号などを提供すると、企業はこれらの情報と、先に取得したパーソナルデータを突合することができる。こうした場合、行動履歴を含め、取得した情報全体で個人情報と見なす必要がある点に注意が必要である。

このように本人を特定・識別しない情報が、他の個人情報と紐づけられることで個人のプライバシーにより踏み込む個人情報となることは、単一の企業・サービスだけで発生するものではない。代表的な事例として、クッキーや広告IDを利用したターゲティング広告や位置情報を利用したジオマーケティングでは、個人の行動履歴をパーソナルデータとして流通させている。こうした取り組みにおいて、個人情報ではないと整理されたデータ[3]が個人情報と紐づけられた場合、上述の通り、全体として個人情報として捉える必要がある。

## 3. パーソナルデータの利活用とプライバシー対応の実態

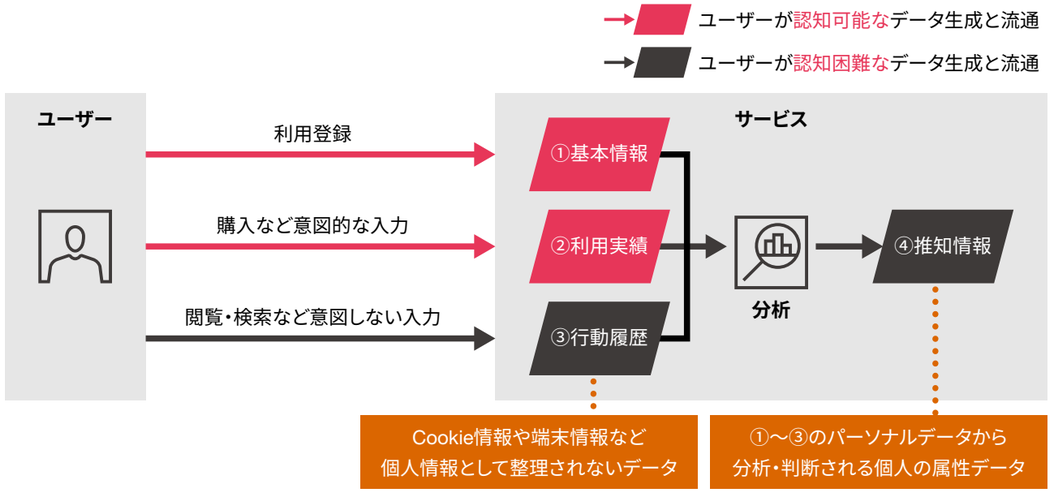
前述のマーケティング用途の事例におけるパーソナルデータの流通について図示すると、図表10の通りとなる。サービス利用にあたっての（1）**基本情報**（メールアドレスなどの連絡先、必要に応じて氏名や住所）に加えて、狭義の（2）**利用実績**（購入履歴や視聴履歴、投稿内容など）や（3）**行動履歴**（Cookieと紐づけられたサイト内の行動履歴など）と、さらにそれら事実の分析による（4）**推知情報**の4種類のデータが、サービスやサイトを通じて生成・流通していく。図表10で示す通り、明示的に入力や選択を行って生成される（1）基本情報や（2）利用実績については、サービス内で何らかの利用がされていることをユーザーが推測することは可能であるが、（3）行動履歴や（4）推知情報については、企業側でどのように利用されているかを感覚的につかむことは難しいであろう。

また、図表10はあくまでユーザーとサービスが1対1の関係でのデータ流通を示しているが、実際のパーソナルデータのエコシステムは、より複雑なものとなる。図表11では、3rd Party Cookieなどを利用したサイトやサービス間でのデータ連携や第三者提供、共同利用、データ販売を含めたパーソナルデータエコシステムを図示している。プライバシーポリシーに記載された第三者提供先や共同利用者への個人情報の提供・共有に加えて、DMP（Data Management Platform）サービスを介することで、複数のサイトにおける行動履歴が集約・分析され、ユーザー自身が関知しないところでパーソナルデータが流通されることになる。

図表11は比較的シンプルなデータ流通形態を示しており、実際には複数の第三者提供先やDMPサービスが存在し、ユーザーにとってはさらに複雑なものとなるゆえ、自身のデータの流通状況を把握することは事実上、不可能と言える。加えて、自社のデータ流通を可視化するためのデータガバナンスやデータマネジメントが機能しておらず、自社のパーソナルデータエコシステムを把握することができていない企業が少なくないのが実情である。

このパーソナルデータ流通の複雑さや管理不全に加えて、プライバシーポリシーの難読さやサービス利用開始時にしか閲覧されない性質も相まって、特に機能拡張によるデータ利用範囲の拡大や外部サービスとの連携、第三者提供にあたっては、何らかの通知などが企業側から行われているとはいえ、誤認を含めて正しくユーザーに伝わっていないことは明らかである。

**図表10：サービス利用を介して生成・流通されるパーソナルデータ**



## 4. 企業に求められる透明性と説明責任

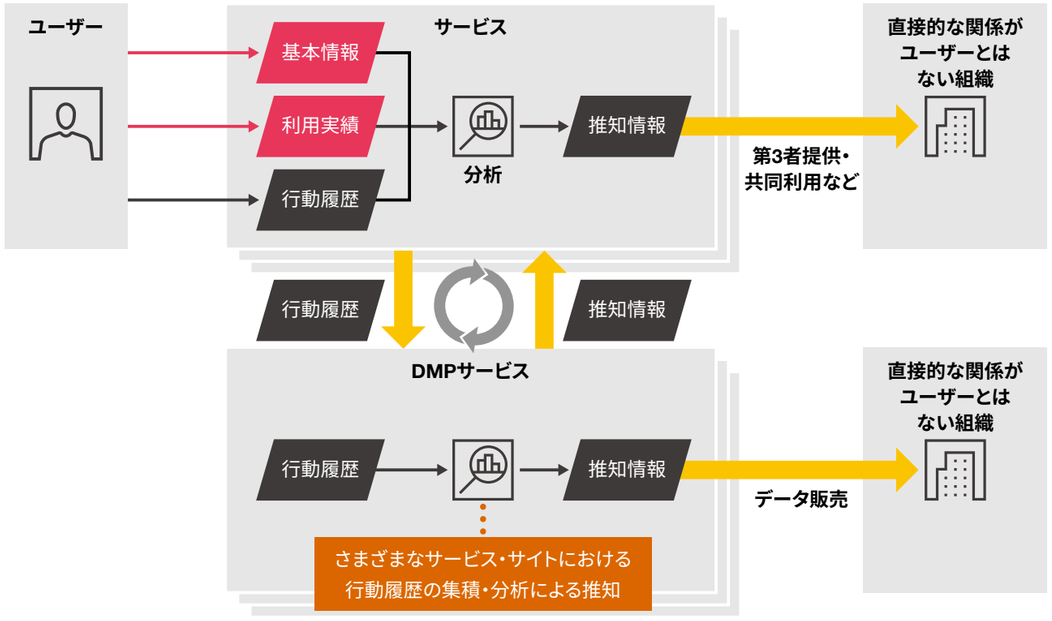
プライバシー保護の観点では、法令で定められている個人情報だけを保護するのではなく、パーソナルデータを含むデータとその流通をエコシステム全体で管理し、利用目的や方法について、できる限り多くのユーザーと認識を合わせていく必要がある。そのためには以下の2点が必要だと考えられる。

(1) パーソナルデータの流通を正しく把握するためのデータガバナンスやマネジメントを行う

(2) データガバナンスやマネジメントの結果として得られるエコシステムの俯瞰図をもって、それぞれの企業や組織がユーザーへの説明や同意取得を行う

パーソナライズされた体験を提供する「人間中心の社会」を実現するには、さまざまな企業が相対するユーザーのパーソナルデータを流通させるパーソナルデータエコシステムと、そのデータ流通を管理するデータガバナンス・マネジメントが不可欠である。しかしながら、どれだけガバナンスやマネジメントにおいてリスクコントロールを行ったとしても、多岐にわたるパーソナルデータの利用方法から、個人のプライバシーを侵害する残存リスクをゼロにすることは難しいであろう。そのため、パーソナライズされた体験の価値というメリットとその残存リスクについて、ユーザーから理解と信頼を得ることも重要になる。つまり、自社内でのガバナンス・マネジメントにとどまらず、ユーザーとのコミュニケーションも併せて実施していくことが重要と言えるのである。

**図表11：DMPベンターなどを介した場合のパーソナルデータのエコシステム**






# 5. ピープルアナリティクスで担保すべき透明性と公平性

新型コロナウイルス感染症の感染拡大に伴い、各企業が急速にリモートワークを促進するなど、私たちのワークスタイルは加速度的に変化した。今後は非対面のコミュニケーションや、勤務する場所を問わない働き方が定着することが予測される。

こうした変化に柔軟に適応できない場合、企業は生産性の低下をはじめ、深刻な課題に直面する危険がある。企業を動かすのは人であるが、人が織りなす対面のコミュニケーションや、経験や勘を加味して判断を下す従来型の人材マネジメントが成り立たなくなる可能性があるからである。各現場が抱える課題にデータをもとにフォーカスし、従業員の言動の傾向やワークスタイルを可視化することで正確な状況把握とその正確性に裏打ちされた意思決定を遂行する「ピープルアナリティクス」が今、求められている。

## 1. 人材のデータ分析がなぜ必要なのか

冒頭で述べた通り、リモートワークが一般的になりつつある現在、対面・非対面のコミュニケーションが混在し、人材のマネジメントが難しくなっている。従業員の評価を例に挙げよう。普段から対面で共に働いていれば、勤務態度をはじめ、評価をする上での材料は多く目に入ることであろう。しかし直接顔を合わせる機会が激減する昨今、評価の指標は、メールやオンライン会議でのようすといったものに偏ってしまう可能性がある。非対面のコミュニケーションが基本となれば、客観的な状況把握を根拠としない限り、従業員の評価の透明性と公平性に対する不満が蔓延してしまう危険があるのである。

クラウドツールやITシステムが発達し、従業員の活動の多くがデジタルフォーマット上で展開されるようになっている。蓄積されるデータを活用して意思決定を行い、データ分析を論拠とした客観的な判断で人材マネジメントを行うことにより、企業は従業員への説得力を増すことができるであろう。では、意思決定の精度向上を図るにあたり、どんな場面でこうしたピープルアナリティクスを活用できるであろうか。具体的に見ていく。

## 2. ピープルアナリティクスの活用が期待される人材マネジメント領域

ここでは人材マネジメントのライフサイクルの中で、採用・就業・退職の3つの領域を対象とする（図表12）。いずれも、データを見て論じるよりも感覚による判断が優先されてきた領域と言えるため、デジタル化が進むに連れて、判断基準にアナリティクスが大きな役割を果たすようになっている。

ここで活用する数多くのデータは、人材の志向・属性・行動のデータという3つに大別される。志向・属性はスキルや資格・経歴情報のような静的データ中心で、行動は各種アプリケーションログのような日々蓄積される動的なデータ中心に成り立つ。図表13に、分類ごとの具体的なデータの種類を記す。

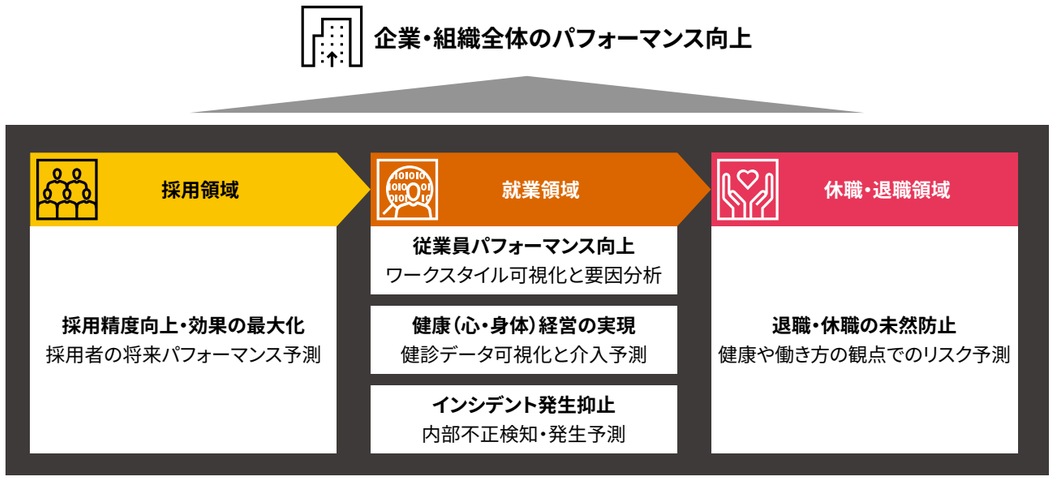
分析の目的に合わせて必要なデータを選択する必要はあるが、ピープルアナリティクスの「ピープル」が指す範囲は必ずしも本人のみとは限らない。その人材の上司・部下との関係や、人材が組織においてどのような役割を担うべきか、といった観点で捉えることもあるため、データの粒度やデータ階層の構造にも注目する必要がある。

志向・属性に関するデータを活用する際に気を付けるべきは、情報鮮度の劣化リスクである。分析当時の断面をデータ化したと言えるため、最終更新から数年経っているデータについては、除外することを検討する必要がある。

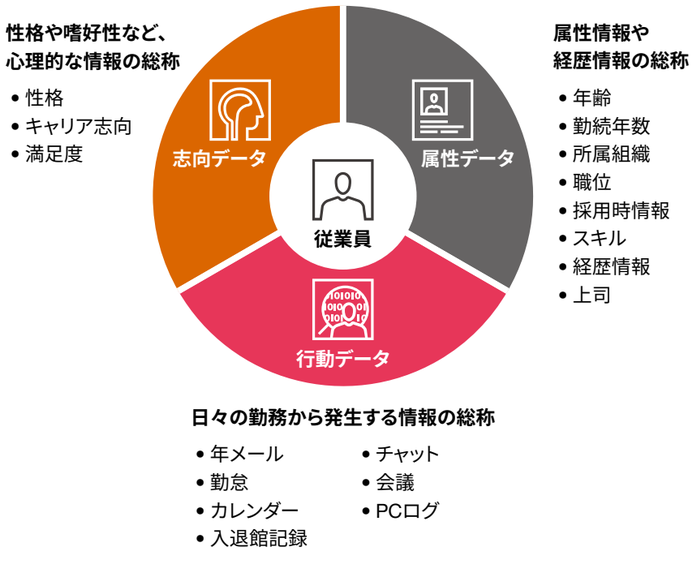
## 3. ピープルアナリティクスの活用事例

人事領域の意思決定は現場で日々発生している。ここでは、スキルや経歴といった定点観測的な静的データよりも、業務を通じて生成されるやり取りをはじめとする動的データの活用の必要性が高まってきている。実際にどのようなデータを活用して意思決定に生かしているのかを、事例ベースで紹介する。いずれも、ワークスタイル分析から業績貢献度の高い人物像を抽出するという、ピープルアナリティクスでよく見られる内容である。

**図表12：ピープルアナリティクスの活用が期待される人材マネジメント領域**




**図表13：ピープルアナリティクスで活用するデータの内容と分類**






**1. 採用・配属マッチング**

採用領域と就業領域における配属が対象の取り組みで、業績貢献度の高い人物像や組織にフィットしやすい人物像をデータから形成し、意思決定の参考情報とする。ここでは、各人材の業務用カレンダーやチャット・メールの内容、業績評価に嗜好性結果なども活用する。分析手順は以下の通りである。

（1）対象組織全体で働き方の類型化を実施し、パターン（朝型・夜型、コミュニケーション発散型、バランス型など）を抽出
（2）類型化されたパターンの中で、貢献度が高い人材が多いグループの特徴を抽出
（3）在籍期間が短かった（休職・退職）人材像を抽出

それぞれから抽出されたものを、組織内での貢献度が高い人物像の特徴組織に定着しづらい人物像の特徴としてまとめ、採用と配属の判断材料とする。

**2. ハイパフォーマー分析**

就業領域における日常業務の生産性や効率性などのパフォーマンスを測定し、「ハイパフォーマー」と呼ばれる業績への貢献度の高い人物像や組織にフィットしやすい人物像をデータから形成、コーチングの参考情報とする。

分析の対象となるデータは、採用・配属の時と同様に業務用カレンダーやチャット・メール、業績評価に嗜好性結果などを活用する。そこから時間の使い方やコミュニケーションの取り方、そうした働き方でどのような業績を残したか、彼らはどのような嗜好性を持っているのか、を分析する。

分析手順は以下の通りである。

（1）対象組織全体で働き方の類型化を実施し、パターン（朝型・夜型、コミュニケーション発散型、バランス型など）を抽出
（2）類型化されたパターンの中で、貢献度が高い人材が多いグループの特徴を抽出

それぞれから抽出されたものを、組織内での貢献度が高い人物像の特徴としてまとめ、コーチングの参考材料とする。

気を付けるべき点として、従業員それぞれに働き方や嗜好性があることへの理解が挙げられる。たとえパフォーマンスを向上させる典型的な取り組みを導き出せたとしても、働き方や嗜好性がかけ離れた従業員にそれを勧めるのは逆効果になり得るため、ロールモデルを形成し、パフォーマンス向上モデルを設けるところまでは同じでも、それぞれに合ったコーチングを実施することが肝要である。

## 4. プライバシー上の懸念事項と対策

このように人材マネジメント領域での高い効果が期待されるピープルアナリティクスであるが、パーソナルデータを利用して従業員の働き方を分析し、その分析結果を利用して組織や本人に還元することから、プライバシー上の問題が発生する可能性がある。

従業員のパーソナルデータそのものに対するセキュリティ対策の実施や個人情報の取り扱いに関する法令の遵守については言うまでもない。加えて、従業員の働くことに関する考え方や、私生活とのバランスの取り方などに踏み込むピープルアナリティクスとスタッフィング・コーチングが、本人のプライベートや自律に影響を与えるアクションになり得ることから、プライバシーを侵害する可能性がある点を考慮しなければいけない。

では、具体的にどのようなことを念頭に置いてピープルアナリティクスを実施するべきであろうか。以下の3点が挙げられる。順に見ていこう。

（1）従業員の信頼関係を醸成するコミュニケーション
（2）分析結果からコンピテンシーへの昇華
（3）働き方の多様性を支える役割の再考

**（1）従業員との信頼関係を醸成するコミュニケーション**

個人情報保護法などの法令を遵守する上でも必要なことではあるが、特にピープルアナリティクスの領域で業績評価などの個人に向けたパーソナルデータ活用を行う場合は、事前から積極的に本人とコミュニケーションを取ることが推奨される。人事関連の業務の多くは、採用時や雇用契約時の個人情報の取り扱いに関する条項などに従い、従業員のパーソナルデータを利用することが一般的である。しかしながら、ピープルアナリティクスのように雇用契約の維持や管理とは直接的に関係せず、取り扱い内容が流動的で雇用関係に影響を与える取り扱いについては、その目的や実施内容の概要について、本人に適切な理解を求めることが望まれる。雇用

契約や従業員規則で定められていない働き方で個人の評価をしているといった見方もできるため、従業員の誤解や不信を招く一因となる。どのようなデータを取得・利用し、分析結果に対して企業としてどのような考え方を持っているのかを、ポータルサイトやダッシュボードといった形で従業員が確認できる手法の採用も検討すべきと考えられる。

**(2) 分析結果からコンピテンシーへの昇華**

パーソナルデータの分析を行う過程で、これまでには見えなかった事実や新たな仮説を導き出すことができるため、ピープルアナリティクスは企業や従業員に有益な情報源になり得る。しかしながら、これらの情報をスタッフィングやコーチングに利用する際、企業理念や行動指針、従来から従業員に対して行ってきた研修プログラムや社員の評価制度からは読み取れない、または外れた考え方については、取り扱いを慎重にすべきである。

例えば、顧客とのコミュニケーション手段（電話やメール）と頻度について全社でピープルアナリティクスを行い、貢献度が高い人材にある特徴が見られたと仮定する。これを営業職の評価指標に取り入れたら、どうなるであろうか。営業職は一般的に、売上目標や利益目標などが主要なKPIになると考えられる。目標を達成している人の中でもコミュニケーションの手段や頻度はまちまちだろうから、急にコミュニケーション手段や頻度といった側面から評価がされた場合、公平性に欠けるとして、モチベーションの低下を招きかねない。仮に働き方と業績に因果関係が見られたとしても、その働き方を支える企業理念や評価制度（コンピテンシー）が伴っていなければ、従業員は「個人の裁量に任せられていた領域でスタッフィングやコーチングが突如行われたと」と、違和感を抱かざるを得ない。分析結果を生かすのにまず必要なのは、組織としての理念やコンピテンシーの制定、企業文化の醸成である点に留意する必要がある。

**(3) 働き方の多様性を支える役割の再考**

P7「レコメンデーションで注意すべき『放っておいてもらえる権利』」でも挙げているが、プライバシー保護の観点では、本人の人格や自律に配慮することも必要になる。雇用契約に従って労働力を提供している従業員を一個人・一契約先として考え、私生活への配慮は当然ながら、働くことに対する意識へのアプローチやアクションも慎重になされるべきである。ハイパフォーマーの働き方や考え方をそのまま横展開する発想では個々のプライバシーを保護することはできないし、そもそも従業員にとっては、雇用契約にない内容に従う義務はない。従業員とのコミュニケーションや透明性・公平性の担保と共に、個人の在り方そのものを尊重すること、組織としてさまざまな個人がいることを認め合う姿勢が重要になる。

組織を支えるのはハイパフォーマーと呼ばれる人材だけではない。組織内での情報共有や指標に直結しないオペレーションにおいて、彼らを支える無数の支援が存在しているはずである。こうした支援者の行動様式は、売上などの業績から直接判断することが困難であるため、従来通りの管理者によるアナログな観察・分析が非常に重要となる。スタッフィングやコーチングに当たっては、組織全体の適切な人材配置を見据えて、個々人の趣向に沿った働き方の実現とそれに応じた役割の再定義が重要になると言える。そうすることでプライバシー保護のみならず、組織としてのパフォーマンス向上につながるスタッフィングやコーチングが可能となる。

## 5. 真に個人が活躍できる企業を目指して

従来、特に日本においては、顧客の個人情報保護が優先され、従業員に対する配慮が後回しになる傾向が見られがちであった。しかしながら、働き方改革やワークライフバランスの実現、それらの施策としてのリモートワークやシェアワークといった、働き方の多様化とその高度化が求められる現在、従業員のプライバシー保護は、顧客と同等かそれ以上に行われるべき事項である。

そのためには、これまで以上に従業員とのコミュニケーションを密にし、企業の働き方に透明性・公平性を持たせることが求められる。従業員向けホットラインの構築や個人情報保護・情報セキュリティ対策など実施すべきことは多くあるが、プライバシーに配慮したピープルアナリティクスを利用したスタッフィングとコーチングは、組織内の多様性の最適化やさらなる活性化を実現する可能性を有す。本章がよりよい働き方の実現の一助になれば幸いである。



# 2 積極的なデータ活用を見据えた『攻め』と『守り』のプライバシー

## 1. デジタル化するビジネスにおいて考慮すべきプライバシーリスク管理

世界経済フォーラムが公表した報告書において「パーソナルデータは新たなオイルになる」という見通しが示されたのは2011年1月のことであった[4]。それ以降に私たちが経験してきたことは、この見通しが正しかったことを物語っている。「プラットフォーマー」と呼ばれる事業者は、サービスやコンテンツを提供する基盤を構築・運営することを通じて、購買履歴などの個人に関連する膨大なデータを幅広く収集し、利活用している。さらに、これらのデータを中心にさまざまな製品やサービスを提供する企業が連携することで巨大なエコシステムを形成し、圧倒的な競争力を生み出している。今後は従来のウェブ上のデータに加えて、無線通信やセンシング技術の進展に伴いインターネットに接続することが可能になったあらゆるモノが生み出すデータの収集と利活用が、企業の競争力を左右すると考えられる。

一方、個人に関連する膨大なデータが収集・利活用されることによる個人情報の漏えいやプライバシーの侵害に対する不安も増大している。重大な情報漏えいやプライバシー侵害を引き起こしてしまった企業や組織が、法令などに基づく行政指導や罰則の適用に加えて、社会的な批判を受けることで、事業からの撤退を余儀なくされる、あるいはレピュテーションに深刻なダメージを受けるというケースが散見されるようになってきている。そのため、データの利活用にあたっては、法令などの遵守はもちろんのこと、ビジネスパートナーや消費者などのステークホルダーに対して個人情報およびプライバシー保護の取り組みに関する情報を積極的に開示すると共に、説明および対話を通じてステークホルダーからの信頼を得ることが重要である。

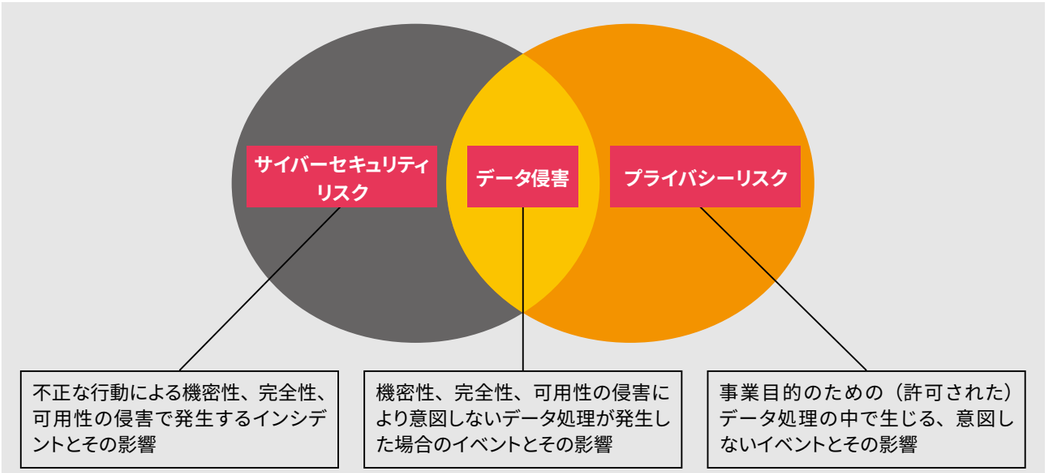
### 1. プライバシーおよびプライバシーリスク

プライバシーという考え方の始まりは、19世紀末に米国の2人の弁護士が発表した論文にさかのぼる。当時は、他人の私生活上の出来事や秘密を煽情的な記事にするメディアが隆盛していた。そのような中で「プライバシーへの権利（The Right to Privacy）」と題して「放っておいてもらう権利（right to be let alone）」が必要であると主張した。20世紀の後半になると、コンピューターを活用した情報処理の進展に伴い、個人の情報を含む広範な情報が集積・活用されるようになったことから、プライバシーについてもより積極的に「自己情報コントロールする権利」と捉えられるようになった。データの利活用を行う企業や組織においては、消費者などからデータを収集する代わりに、それを適切に取り扱うことが求められる。

しかしながら、こうした企業や組織はデータの利活用を行う上で、常にプライバシー権を侵害するリスク（プライバシーリスク）を抱えている。米国国立標準技術研究所（National Institute of Standards and Technology：NIST）が2020年1月に公開したプライバシーフレームワーク（NIST Privacy Framework： A Tool for Improving Privacy through Enterprise Risk Management[5]）を参照すると、プライバシーリスクは、事業目的のための製品やサービスにおける許可されたデータ処理の中で意図しない問題や結果が生じるリスクであると読み解くことができる。購買履歴などのさまざまなデータの分析を通じて個人の属性や性質を類推するいわゆるプロファイリングによって、センシティブ情報さえも推定されてしまうことなどが挙げられる。またプライバシーリスクとは別にサイバーセキュリティリスクについても言及されており、これについては、情報システムや情報資産の機密性、完全性および可用性を侵害する不正な行動によってインシデントが発生するリスクと考えられる。システムの脆弱性を突いた外部からの攻撃といった例が挙げられる。両者の関係は図表14の通りである。

プライバシーリスクとサイバーセキュリティリスクが重なり合った時に生じるのが、データ侵害である。故意または過失による個人情報の漏えいといったセキュリティインシデントが挙げられる。データの利活用は企業や組織に多くの恩恵をもたらすが、同時にこうしたリスクと常に隣り合わせであることを自覚しておく必要がある。

**図表14：プライバシーリスクの位置づけ[6]**




## 2. AIの利用原則におけるプライバシー

ここからは、AIの利活用においてプライバシーがどのように扱われているかを紹介する。急速に社会への実装が進むAIを正しく有効に活用するため、その利用原則に関する議論が、これまで精力的に行われてきた。日本を含む多くの国際機関や各国・地域で、その結果がAI利活用原則として取りまとめられている。2019年6月のG20茨城つくば貿易・デジタル経済大臣会合においては「人間中心」の考えを踏まえたAI原則が採択されるなど、「AI原則の項目については、国際的にほぼコンセンサスが得られつつ」[7]ある状況である。図表15に代表的なAIの利活用原則を示す。

**図表15：代表的なAIの利用原則（例）[8]**

| 国際機関／国／地域 | 概要 |
|---|---|
| OECD | AIに関するOECD原則（一部抜粋）<br>・人権等を尊重するように設計され、また公平公正な社会を確保するために適切な対策が取れる<br>- 例えば必要に応じて人的介入ができるーようにすべき<br>・人々がどのような時にそれと関わり結果の正当性を批判できるのかを理解できるようにするために、透明性を確保し責任ある情報開示を行うべき など |
| 日本 | 人間中心のAI社会原則（一部抜粋）<br>・プライバシー確保の原則<br>- 個人の自由、尊厳、平等が侵害されないようにすべき<br>- パーソナルデータを利用するAIは、当該データのプライバシーにかかわる部分については、正確性・正当性の確保及び本人が実質的な関与ができる仕組みを持つべき<br>- パーソナルデータは、その重要性・要配慮性に応じて適切な保護がなされなければならない。利活用と保護のバランスについては、文化的背景や社会の共通理解をもとにきめ細やかに検討される必要がある など |
| 米国 | 米国商工会議所：AI原則（一部抜粋）<br>・強固かつ柔軟なプライバシーレジームの追求<br>ー明確で一貫したプライバシー保護は信頼に足るAIに必須の構成要素である など |
| EU | AIの倫理指針（一部抜粋）<br>・プライバシーおよびデータガバナンス<br>- プライバシーの侵害を未然に防止するためには、使用されるデータの品質と整合性を確保するデータガバナンスが求められる など |

日本では図表15の「人間中心のAI社会原則」を踏まえ、AIネットワーク社会推進会議が「AI利活用ガイドライン～ AI利活用のためのプラクティカルリファレンス～」を公表している[9]。当該ガイドラインは、適正利用、適正学習、連携、安全、セキュリティ、プライバシー、尊厳・自律、公平性、透明性、アカウンタビリティからなるAI利活用原則を定めると共に、同原則を実現するための具体的方策について取りまとめている。

## 3. 「AI利活用ガイドライン」における プライバシーに関する原則

「AI利活用ガイドライン～ AI利活用のためのプラクティカルリファレンス～」[10] において、プライバシーの原則は「利用者及びデータ提供者は、AIシステム又はAIサービスの利活用において、他者又は自己のプライバシーが侵害されないよう配慮する」と定義されている。また、その前提として、日本においては個人情報保護法の遵守が必要であるとされている。その上で、主な論点が3つ提示され、次のように解説されている。

**1. AIの利活用における最終利用者及び第三者のプライバシーの尊重**

- AIサービスプロバイダ及びビジネス利用者は、AIを利活用する際の社会的文脈や人々の合理的な期待を踏まえ、AIの利活用において最終利用者及び第三者のプライバシーを尊重する。
- また、最終利用者及び第三者のプライバシーを侵害した場合に講ずるべき措置について、あらかじめ整理しておくことが期待される。
- 加えて、当該措置について、最終利用者及び第三者に対し、必要な情報提供を行うことが期待される。

**2. パーソナルデータの収集・前処理・提供等におけるプライバシーの尊重**

- AIサービスプロバイダ、ビジネス利用者及びデータ提供者は、AIの学習等に用いられるパーソナルデータの収集・前処理・提供等において、また、それらを通じて生成された学習モデルの提供等において、最終利用者及び第三者のプライバシーを尊重する。

**3. 自己等のプライバシー侵害への留意及びパーソナルデータ流出の防止**

- AIサービスプロバイダ、ビジネス利用者及びデータ提供者は、AIの判断により本人同意なくパーソナルデータが第三者に提供されることがないよう、同意が得られていないデータはシステム上第三者に提供できないこととするなど、適切な措置を講ずることが期待される。

図表16の（1）で言及されている「プライバシーを侵害した場合に講ずるべき措置」とは、どのような措置が想定されているのであろうか。パーソナルデータを利用するさまざまなシーンでのプライバシーの尊重や流出の防止は当然のこととして、次の2つが例示されている[11]。

**図表16：プライバシーの原則と主な論点、期待される措置**

| プライバシーの原則 | 利用者及びデータ提供者は、AIシステム又はAIサービスの利活用において、他者又は自己のプライバシーが侵害されないよう配慮する |
|---|---|

| 主な論点 | | 期待される措置（主な論点（1）の解説より） |
|---|---|---|
| （1） | AIの利活用における最終利用者及び第三者のプライバシーの尊重 | 最終利用者及び第三者のプライバシーを侵害した場合に講ずるべき措置について、あらかじめ整理しておくことが期待される。 |
| （2） | パーソナルデータの収集・前処理・提供等におけるプライバシーの尊重 | 加えて、当該措置について、最終利用者及び第三者に対し、必要な情報提供を行うことが期待される。 |
| （3） | 自己等のプライバシー侵害への留意及びパーソナルデータ流出の防止 | |

## 4. プライバシー侵害時に講ずるべき措置の例

- 最終利用者及び第三者のプライバシーを侵害する情報を誤って取得した場合における、当該情報の消去、AIのアルゴリズムの更新 等
- 最終利用者及び第三者のプライバシーを侵害する情報を拡散した場合における、保存先への消去の依頼、AIのアルゴリズムの更新 等

プライバシーを侵害された被害者の救済のためにも必要かつ重要な措置であることに異論はないと筆者は考える。その一方、システム管理者などの立場からすると、当該情報の「消去」は実務上、とても大きな困難を伴うことも事実である。「消去」を当該情報の物理的な削除と想定すると、当該情報の消去によってシステム内でデータの不整合が発生し、最悪の場合、システムが停止する恐れがあるからだ。また、バックアップデータなどを含めて当該情報を網羅的に洗い出し、「消去」するためには、相応の労力が必要になる。そのため、データ利活用を含むサービスや製品においては、データ主体の消去・訂正・開示請求に応じる場面を含めプライバシーに関わる情報を取り扱うあらゆる側面で適切な対応ができるよう、その設計段階から、プライバシー保護のために必要となる措置をあらかじめ考慮しておくプライバシー・バイ・デザインの考え方が、今後ますます重要になると考えられる。

## 5. プライバシーリスク管理のための フレームワークなど

企業や組織がプライバシーリスクを適切に管理しながらデータを利活用するためには、具体的にどのような取り組みが求められるのであろうか。多くの企業や組織では、従来の情報セキュリティや個人情報保護法などへのコンプライアンスを主管する部門が中心となり、情報システム部門といった関係部門と連携しながらプライバシーリスク管理を実施しているものと思われる。関係者間の利害や立場の違いを超えて、企業や組織として適切にプライバシーリスクを管理しデータの利活用を推進できるよう、参考になると思われるフレームワークなどを紹介する。

**■NISTプライバシーフレームワーク**

NISTが2020年1月にVersion 1.0を公開したこのフレームワークは、プライバシー保護のために企業や組織が遵守すべきベースラインとして、次の3つを目的に策定されている。

1. 製品やサービスなどの設計や開発において、プライバシー保護の合理的な説明責任を果たすこと
2. プライバシー保護活動の情報発信やコミュニケーションをしやすくすること
3. 評価結果をもとに経営層、法務部門、IT部門などの間で、部門横断的なコラボレーションを実現できること

セキュリティ領域におけるデファクトスタンダードとなっている「NIST Cyber Security Framework」の姉妹版ということもあって、日本でも普及が想定されるフレームワークの1つである。

**■ISO/IEC 29100：2011（JIS X 9250：2017）プライバシーフレームワーク**

この規格は情報通信技術（ICT）システムにおける個人識別可能情報（PII）の保護のためのフレームワークであり、企業や組織がICT環境におけるPIIに関連するプライバシー安全対策要件を定義するための一助となることを目的として、プライバシー安全対策要件の説明などを提供している[12]。

また、2019年8月に発行されたISO/IEC27701：2019 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC27002 for privacy information management – Requirements and guidelinesも本規格と整合して策定されていることから、既存のISMSに基づいてプライバシー情報マネジメントを確立したい企業や組織にとっては、本規格の理解が有用である。

プライバシーに関連する主な国際規格を図表17に示す。

**■プライバシー・バイ・デザイン**

製品やサービスの企画・設計段階から、プライバシーに関連する情報を取り扱うことが想定されるビジネスプロセス全般においてプライバシー保護の施策を事前的・予防的に組み込んでおこうというコンセプトで、次の7つの原則が示されている[13]。

このコンセプト自体は1990年代の半ばに提唱されたものであるが、データの利活用に伴うプライバシー保護が企業や組織にとって喫緊の課題となりつつある今、あらためて注目されている考え方である。

**図表17：プライバシーに関連する主な国際規格**

| | |
|---|---|
| ISO／IEC 29100：2011（JIS X 9250：2017） | プライバシーフレームワーク（プライバシー保護の枠組みおよび原則） |
| ISO／IEC 29101：2018 | プライバシー・アーキテクチャ・フレームワーク |
| ISO／IEC 29134：2017 | プライバシー影響評価のガイドライン |
| ISO／IEC 29151：2017 | 個人識別可能情報（Personally Identifiable Information：PII）保護の実践規範 |
| ISO／IEC 29184：2020 | オンライン・プライバシー通知と同意 |
| ISO／IEC 27018：2019 | パブリッククラウドコンピューティング環境における個人情報（PII）保護のための管理目的および管理策 |

**■プライバシー影響評価（Privacy Impact Assessment：PIA）**

上述のプライバシー・バイ・デザインの考え方に基づき、製品やサービスの企画・設計段階でプライバシーへの影響を事前に分析・評価するリスク管理手法として、プライバシー影響評価が知られている。国際標準規格としては、ISO/IEC 29134：2017 Guidelines for privacy impact assessmentが2017年6月に発行されている。本規格は、プライバシー影響評価の実施プロセスとその報告書の構成と内容についてのガイドラインを提供している。

企業や組織が製品やサービスの企画・設計段階でプライバシー影響評価を実施することで、プライバシーリスクを適切に管理することができるのはもちろんのこと、その実施や結果をステークホルダーに対して積極的に開示し、自らのプライバシー保護への取り組みに対する説明と対話を行うことで、ステークホルダーからの信頼を得るリスクコミュニケーションツールとして用いることも考えられる。

**図表18：プライバシー・バイ・デザインの7原則**

| | |
|---|---|
| (1) | 事前的・予防的であること |
| (2) | デフォルトの設定でプライバシーが保護されること |
| (3) | プライバシー対策が企画・設計時に組み込まれること |
| (4) | ゼロサムではなくポジティブサムであること |
| (5) | ライフサイクル全体を通じて保護されること |
| (6) | 可視化され透明性が確保されていること |
| (7) | 個人のプライバシーが尊重されていること |



# 2. 「アフター GDPR」におけるプライバシー保護のグローバリゼーション

## 1. GDPRを機に厳しくなる各国の個人情報保護法

2018年の欧州一般データ保護規則（GDPR）の施行を機に、各国の個人情報保護法は厳格化の傾向をたどっている。特にブラジル、インド、タイ、日本で施行予定の法令は、GDPRに類似していると言われている。さらに、中国サイバーセキュリティ法や中国個人情報安全規範は、GDPRの影響を受けて個人の権利を強化している。

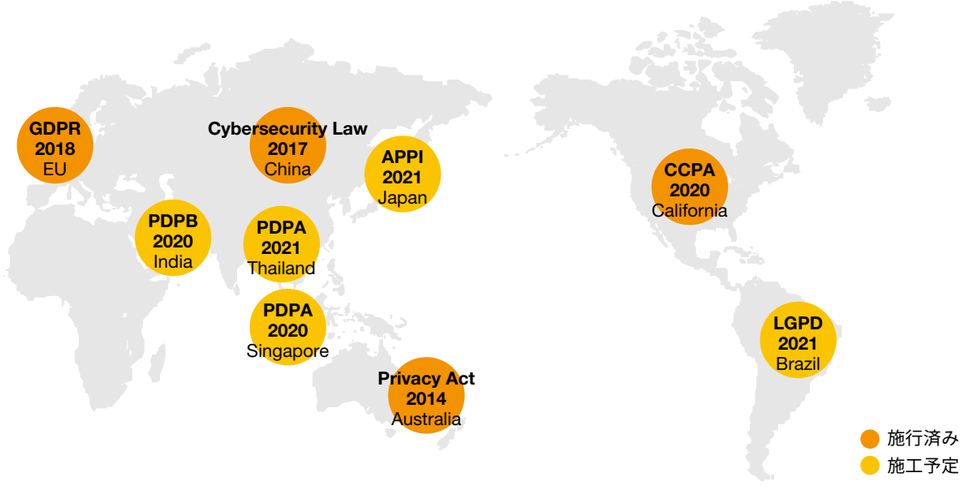
プライバシー保護は元来、1980年に経済開発協力機構（OECD）が策定した「個人情報保護に対する8つの原則」（目的明確化の原則、利用制限の原則、収集制限の原則、データ内容の原則、安全保護の原則、公開の原則、個人参加の原則、責任の原則）が基礎となっている。当原則を礎とし、欧州や日本などでは、EUデータ保護指令、個人情報保護法などが策定された。

一方、当原則はOECDの加盟国のみに適用され、かつ当原則に対する解釈は、各国に委ねられているため、プライバシー保護のレベルは国ごとに異なった。特に欧州は、複数の国から成る経済統合体を築いており、これらの国における共通秩序を実現するため、個人情報保護法にも均質性が求められてきた。そこでEU加盟国[14]においてプライバシー保護レベルの乖離を平準化するために施行された法令が、GDPRである。

これまでは、個人情報を含む情報を利活用することで新たなビジネスの創出や知見を獲得しようという企業のビジネス上の利益が優先されてきたが、GDPRの施行を機に、個人情報保護法が厳格化し、ユーザーのプライバシーも尊重されるようになった。

図表19に、GDPRを皮切りに厳格化する各国の個人情報保護法施行の動きをまとめた。これらの法令には、当該国に拠点がない場合にも適用され得る国外適用の要件も含まれている。そのため、グローバルにビジネスを展開する企業は、各国のグループ会社が個別に対策を講じるのではなく、どの法令へも対応できるようにプライバシー保護をグローバライズし、グループ全体へ適用する必要が出てきたと考えられる。

**図表19：各国で厳格化する個人情報保護法**



## 2. プライバシー保護のグローバリゼーションのために企業が行うべき3つの施策

それでは企業は、こうした状況下でどのような施策を講じればよいのであろうか。実際にプライバシー保護のグローバリゼーションに取り組んでいる企業の事例をもとに説明する。

プライバシー保護施策は一般的に、データマッピング、規程類の策定、グループ管理体制の構築、越境移転への対応、データ主体（ユーザー）の権利への対応、委託先への対応、データ保護影響評価、従業員教育が挙げられる。その中でも特に肝となる論点は、「グローバル管理体制の構築」、「ミニマムのプライバシー保護レベルの設定」、「データマッピングとデータ主体の権利への対応」の3点である。

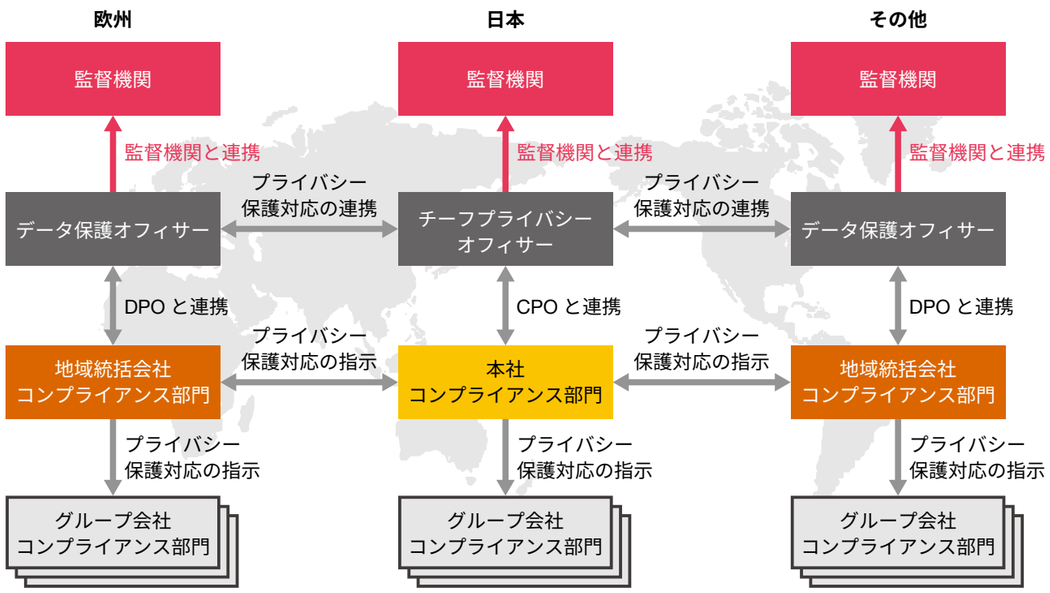
### 1）各グループ会社が連携するグローバル管理体制の構築

各国の個人情報保護法の動向を把握し、プライバシー保護をグローバライズするためには、まずは各グループ会社が連携を行う管理体制の構築が必要となる。各国の法令下でデータ保護オフィサー（DPO：Data Protection Officer）の設置が求められているか否かに関わらず、企業のビジネス戦略やプライバシー保護へ関与する責任者であるチーフプライバシーオフィサー（CPO：Chief Privacy Officer）やそれを支援するコンプライアンス部門の設置が推奨される（図表20）。

既にこうした取り組みを実施している企業は、ビジネスを展開する地域の統括拠点へCPOを設置し、各CPOが担当する地域内のグループ会社のコンプライアンス部門と連携しながら、プライバシー保護に係るアドバイスの提供や監視を行っている。またコンプライアンス部門は、CPOからのアドバイスなどをもとに、プライバシー保護の施策を導入・運用している。

さらに、全従業員が、CPOやコンプライアンス部門が策定したプライバシー保護に係るルール、体制、運用手順などの情報に対して簡単にアクセスできるように、これらの情報を集約した共有サイトを構築することが推奨される。

**図表20：チーフプライバシーオフィサー（CPO）を設置したグローバル管理体制の例**




### 2）ミニマムのプライバシー保護レベルの設定

先に述べたように、各国の個人情報保護法は異なっている。一般的に、欧州、北米、東アジアはプライバシー保護レベルが高く、その他の地域は、未だ途上段階にあると言われている。欧州のGDPRは、プライバシー保護の「グローバルスタンダード」であると言われてはいるものの、当該法令の要件をグループの全拠点へそのまま適用することは、地域特性の違いから難しいであろう。一方で、多額の制裁を科されるリスクも避けなければいけない。そのため、グローバルにビジネスを展開する企業は、各国の法令の特異性を考慮した上で、ミニマムのプライバシー保護レベルを設定する必要がある。既に取り組みを実施している企業は、自社の地域統括拠点がある国々の法令と要件の差分を把握した上で、独自のグローバルプライバシー保護レベルを設定し、それをもとにグループ会社へプライバシー保護対策を導入・運用している。

### 3）グループ内外におけるデータマッピングに基づいたデータ主体の権利への対応

法令の厳格化、データ主体の権利強化に伴い、各国では、ユーザーが個人情報の取り扱いやプライバシーポリシーに係る問い合わせを企業に行うケースが急増している。実際に、ユーザーからの問い合わせに適切に対応することができず、監督機関から制裁を科されたり、レピュテーションが低下したりした企業も出てきている。

これらのリスクを最小限に抑えるために、企業は、ユーザーから問い合わせを受けた際に、なるべく早く、また正確に応じなければいけない。そのために、企業はグループ内外におけるデータマッピングを行い、自社がユーザーから取得している個人情報の種類、利用目的、適法性の根拠、プライバシーポリシーへの同意の取得状況、第三者提供の状況などを整理しておく必要がある。既に取り組みを実施している企業は、グローバルプライバシー保護レベルをもとに、グループ共通のデータマッピング項目を策定し、CPOや各グループ会社のコンプライアンス部門を通じて、個人情報の取り扱い状況を洗い出している。

## 3. グローバライズされたプライバシー保護がビジネスに貢献する

近年、企業の先進的な取り組みとして、合併・買収やジョイントベンチャーの設立などのビジネス戦略と並行して、プライバシー保護のデューデリジェンスを効率的に行う方法を模索しているという例が挙げられる。その取り組みの一つとして、企業は、データマッピングツールやユーザーからの同意状況を管理するコンセントマネジメントツールといったプライバシーテックを採用し、プライバシー保護の柔軟性を高めている。

ビジネスがグローバル化する社会にあっては、企業内のプライバシー保護をグローバライズすることが今後、ますます求められると考えられる。各国の法令に準拠してユーザーの個人情報を適切に管理し、彼らのプライバシーをグローバル規模で保護することが、企業がビジネスを成功させるための礎となるであろう。GDPRの施行を契機に、こうした取り組みは既に各国で始まっている。

# 3. デジタルトランスフォーメーションにおけるプライバシー・バイ・デザインの実装

## 1. デジタルトランスフォーメーションに求められるプライバシー保護

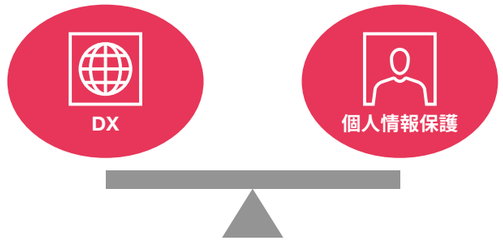
2007年にスマートフォンが発売されて以降、多くの人が自分専用のモバイル端末を保有し、現在では複数台の端末を持ち歩く時代になった。

それまで情報のやりとりは、紙や会社で使用するPCなどの端末間に限定されていたが、現在では多くの人が複数の端末を使ってインターネットやソーシャルメディアを利用し、あらゆる情報を共有するようになり、そこから膨大な量のデータが生まれている。

また、近年、デジタルトランスフォーメーション（DX）という言葉を耳にする機会が増えた。データを人工知能（AI）などで分析し、ユーザーに対してカスタマージャーニーに最適なユーザーエクスペリエンス（UX）を提供したり、分析したデータを活用して企業の既存プロセスを最適化したりといった取り組みが行われている。

DXの加速に伴い、2017年施行の中国サイバーセキュリティ法、2018年施行のEU一般データ保護規則（GDPR）を皮切りに、各国ではプライバシー保護関連の立法や改正が進み、より厳格な要求を企業に課している。日本でも2020年に個人情報保護法の改正法が公布された。GDPRにより、特に企業が対応に追われている要件は、ユーザーの権利を強化すること、また個人情報を越境移転する際の規制が強化されたことである。万が一、法令に違反した場合、企業は監督機関から法令上の制裁金を科されることに加え、刑事上・民事上の責任を問われ、企業イメージを損なう可能性もあり、各社は対応に追われている。

**図表21：DXとプライバシー保護のバランス**




さらに、法令の厳格化だけではなく、近年問題視されているインターネット上の誹謗中傷などによる個人情報漏えいの被害が増えたことで、ユーザーによるプライバシー保護への関心が高まってきた。

こういった背景から、企業はDXを促進する一方で、プライバシー保護に関しても考える必要に迫られている。また、DXとプライバシー保護を従来のように二律背反の関係と捉えるのではなく、DXを通じた企業価値の向上に必要な投資であることを認識する必要がある。

## 2. ユーザーセントリックなプライバシー・バイ・デザイン

DXなどの組織改革、新サービスやシステムの導入にあたって、企画や設計段階からユーザーのプライバシー保護をあらゆる側面で検討し、あらかじめプライバシー保護対策を組み込む考え方を「プライバシー・バイ・デザイン」と呼ぶ。この考え方は1990年代半ばに提唱されたものであるが、GDPRにより法的要求事項になったことやGDPR違反による有名企業に対する制裁事例が生じたことから、企業やユーザーにプライバシー・バイ・デザインが広く認知され、今ではグローバルスタンダードな設計思想になった。

プライバシー・バイ・デザインは、次の7つの原則から構成されている[15]。

**（1）事前的／予防的であること**

ユーザーのプライバシーを侵害するイベントが発生する前に、プライバシー対策を導入する必要がある。

**図表22：プライバシー・バイ・デザインの概念図**


**（2）初期設定であること**

サービスやシステムにあらかじめプライバシー保護対策を組み込んでおくことで、ユーザーが自身の個人情報の提供範囲や利用方法を設定せずとも、プライバシーが自動的に保護される必要がある。

**（3）デザインに組み込むこと**

プライバシー保護対策は、サービスやシステムが稼働した後に追加で導入されるのではなく、企画や設計といったデザインの段階から組み込むことで、そのサービスやシステムの基本機能とする必要がある。

**（4）ポジティブサムであること**

プライバシー・バイ・デザインは、サービスやシステムによって生まれる利便性とユーザーのプライバシー保護のどちらか一方というゼロサムの関係であるべきではなく、双方に利益があるポジティブサムを目指す。

**（5）実装ライフサイクル全体で保護されていること**

プライバシー情報を収集・利用・保管・廃棄というというライフサイクル全体を通して、エンド・ツー・エンドの強力なセキュリティで保護することが不可欠である。

**（6）可視化し透明性を維持すること**

ユーザーのプライバシー情報を保護する仕組みが可視化され検証可能であること、またその仕組みが適切に機能することを全ての関係者に保証する必要がある。

**（7）ユーザーセントリックであること**

プライバシー・バイ・デザインでは、上述の通り、デザインや初期設定として組み込む、強力なセキュリティを実装する、個人情報の取り扱いに関してユーザーに通知するといった対応をする上で、ユーザーのプライバシーを中心に考え、最大限に尊重する必要がある。

## 3. 成功事例から読み解くプライバシー・バイ・デザインの実装モデル

では、実際にプライバシー・バイ・デザインをどのように実装すればいいのであろうか。

一般的に、プライバシー・バイ・デザインというと、企画・設計段階でプライバシー情報の有無を確認する、開発段階でセキュリティ対策を実装するなどの一時的な対応を想像する方が多いかもしれない。しかし、真の目的は、ユーザーのプライバシーを恒久的に保護することであり、下図に示す通り、企画・設計・開発、そして運用においてもプライバシー保護対策を続け、定期的に見直しや改善を図ることにある。

実際に取り組みを成功させている先進的な事例をご紹介する。企画・設計段階で、ビジネス部門が策定したサービスの企画書・設計書に対し、プライバシー保護部門がプライバシーレビュー、システム部門がセキュリティレビューを行う。これらのレビューで、プライバシーやセキュリティにリスクがあり、リスク低減策をとることが困難で、ユーザーのプライバシーに大きな影響を及ぼす可能性があると指摘された場合は、ビジネス部門はサービスを開発することはできない。なお、プライバシー保護部門は、当該サービスのユーザーによる個人情報の提供有無、個人情報の取り扱いに関する同意の取得粒度や、プライバシーポリシーをレビューする。また、プライバシー保護に関する情報へのアクセスのしやすさ、内容の平易さといったユーザーエクスペリエンスについても確認する。

**図表23：プライバシー・バイ・デザインの実装**

| | 企画 | 設計 | 開発 | 運用 |
|---|---|---|---|---|
| **ビジネス部門** | ✓サービスで利用する個人情報の使用方法を明確にする。<br><br>✓プライバシー保護部門とシステム部門へ相談を開始する。 | ✓ユーザーへ個人情報の使用方法を通知するログイン画面や提供する個人情報を選択できる管理画面を設計する。 | ✓プライバシー保護部門やシステム部門からの改善案を反映したプライバシーを考慮した設計書をもとにサービスを開発する。 | ✓サービス上でプライバシーが考慮されているかを定期的にモニタリングし、必要に応じて改善する。<br><br>✓ユーザーからプライバシーに関する問合せ（例：開示請求など）があった場合は、ビジネス部門・プライバシー保護部門・システム部門で協力し、彼らのプライバシーを尊重したスピード感のある対応を行う。<br><br>✓万が一、プライバシーを侵害するイベントが発生した場合は、社内外の関係者と連携し、被害を最小限にとどめるよう軽減策を即座に施し、個人情報の監督機関等と連携しながら、二次対応、ユーザーへの通知サービスの復旧を行う。 |
| **プライバシー保護部門** | ✓個人情報の使用方法の合理性を確認する。<br><br>✓個人情報の使用方法に関する通知・同意の文言を策定する。 | ✓ビジネス部門の設計書を確認し、ユーザーセントリックな構成となっているかを確認し、必要に応じて改善を提案する。 | ✓サービスの設計書どおりに開発されているかを適宜確認する。<br><br>✓当サービスで委託先やクラウドベンダーを利用する場合は、個人情報の適切な取り扱いに関する契約書を用意する。 | |
| **システム部門** | ✓個人情報が保管される予定のシステムと実装されている、もしくは実装すべきセキュリティ対策を明確にする。 | ✓ビジネス部門の設計書を確認し、セキュリティ対策と競合してしまう設計はないかを確認し、必要に応じて改善を提案する。 | ✓サービスの設計書をもとに、強固なセキュリティ対策を実装したシステムを構築する。 | |

## 4. プライバシー・バイ・デザインによるサービスの創造とユーザーエクスペリエンスの実現

近年、一部の企業では映像や画像を活用し、自社におけるプライバシー保護の取り組みを積極的に公表している。これは、プライバシー保護が「法令対応」だけではなく、「ユーザーに個人情報の活用で実現できるサービスの価値を感じてもらう」という位置づけになりつつあるからだと考えられる。

このように、DXを進めていく上で、プライバシー・バイ・デザインを導入し、社外にその取り組みを公表することは、新たなサービスの創造とユーザーエクスペリエンスの向上へとつながるであろう。



# おわりに

プライバシーに関するリスクへの従来の対応は、いわゆる個人情報保護法の遵守というコンプライアンス上の問題として取り扱われることが多かったのではないでしょうか。そのため、プライバシー保護に関する取り組みは「コンプライアンスコスト」と捉えられ、法務部門やコンプライアンス部門など一部の専門家によって実施されてきたと思われます。

しかし、パーソナルデータを含むデータの利活用が企業の競争力を左右すると考えられる時代にあっては、データの取り扱いやプライバシー保護に関して、データを提供する個人ひいては社会から信頼を確保することが必要です。信頼が損なわれてしまっては、データの提供が行われなくなったり、データの利活用を伴うビジネスそのものが受け入れられなくなる恐れがあるからです。そして、ステークホルダーからの信頼を確保するためには、従来の法令遵守（Comply）に加えて、プライバシー保護に関する取り組みを企業が主体的に開示・説明（Explain）するComply&Explain型の組織としての在り方が求められています。

そのため、プライバシーに関するリスクへの対応を、ビジネスリスクの低減に加えて中長期的な企業価値の向上に寄与する取り組みとして捉えなおし、経営者のリーダーシップとコミットメントのもと、データを提供する個人の権利利益の保護に取り組む全社的な態勢を整備することが必要とされています。他社に先駆けてこのような態勢を整備し、ステークホルダーからの信頼を獲得した企業が、ビジネス上の優位性を確保し中長期的に企業価値を向上させることになるでしょう。

# 参考資料


1 日本経済新聞，2020.「ネット広告費、テレビ抜く スマホ普及で動画好調」（2020年7月15日閲覧）
https://www.nikkei.com/article/DGXMZO56810290U0A310C2EA1000
2 内閣府,「Society 5.0」（ 2020年9月29日閲覧） https://www8.cao.go.jp/cstp/society5_0/
3 こうした形で個人情報と紐づけられることが容易に想定されるパーソナルデータについては、2020年に改正・公布された個人情報保護法では「個人関連情報」として定義され、新たな義務が規定された点を留意する必要がある。
4 World Economic Forum Report. Personal Data：The Emergence of a New Asset Class Feb. 17, 2011.
5 NIST Releases Version 1.0 of Privacy Framework Jan16,2020
6 NIST Privacy Framework：A Tool for improving privacy through enterprise risk management, version 1.0 Jan16,2020 P.3 Figure2：Cybersecurity and Privacy Risk Relationship
7 報告書2019概要 AIネットワーク社会推進会議 令和元年8月9日
8 OECDニュースルーム 42 ヵ国がOECDの人工知能に関する新原則を採択 2019年5月22日
人間中心のAI社会原則 統合イノベーション戦略推進会議決定 平成31年3月29日
U.S. Chamber of Commerce U.S. Chamber Releases Artificial Intelligence Principles Sep.23, 2019.
European Commission Futurium Ethics Guidelines for Trustworthy AI
9 総務省 AIネットワーク社会推進会議 報告書2019の公表
10 AI利活用ガイドライン～ AI利活用のためのプラクティカルリファレンス～ AIネットワーク社会推進会議 令和元年8月9日
11 AI利活用原則の各論点に対する詳細 AIネットワーク社会推進会議 令和元年8月9日
12 JIS X 9250：2017 情報技術―セキュリティ技術―プライバシーフレームワーク（プライバシー保護の枠組み及び原則）
Information technology -- Security techniques -- Privacy framework
13 堀部政男、一般財団法人日本情報経済社会推進協会編（2012）プライバシー・バイ・デザイン プライバシー情報を守るための世界的新潮流
14 GOV.UK, “Countries in the EU and EEA” ,（2020年8月12日閲覧）
15 Ann Cavoukian, 2010. “Privacy by Design: The 7 Foundational Principles”

# お問い合わせ先


**PwC Japanグループ**
https://www.pwc.com/jp/ja/contact.html

**【監修】**

**林 和洋**
PwCコンサルティング合同会社 パートナー

**藤川 琢哉**
PwCコンサルティング合同会社 パートナー

**平岩 久人**
PwCあらた有限責任監査法人 パートナー

**【執筆者】**

**高橋 功**
PwCコンサルティング合同会社 ディレクター

**奥野 和弘**
PwCコンサルティング合同会社 ディレクター

**森田 成祐**
PwCあらた有限責任監査法人 ディレクター

**山上 真吾**
PwCコンサルティング合同会社 シニアマネージャー

**篠宮 輝**
PwCコンサルティング合同会社 マネージャー

**遠藤 祐輔**
PwCコンサルティング合同会社 マネージャー

**木村 俊介**
PwCコンサルティング合同会社 マネージャー

**宮内 美里**
PwCコンサルティング合同会社 シニアアソシエイト


**www.pwc.com/jp**




発刊年月：2021年1月　　管理番号：I202010-05