第 79 回 JIPDEC セミナー講演レポート

GDPR から考える、デジタル時代のプライバシー

KPMG コンサルティング株式会社
テクノロジーリスクサービス
パートナー　大洞　健治郎氏

デジタル時代の消費者意識とプライバシー保護

■デジタル時代の個人データの取扱いとは

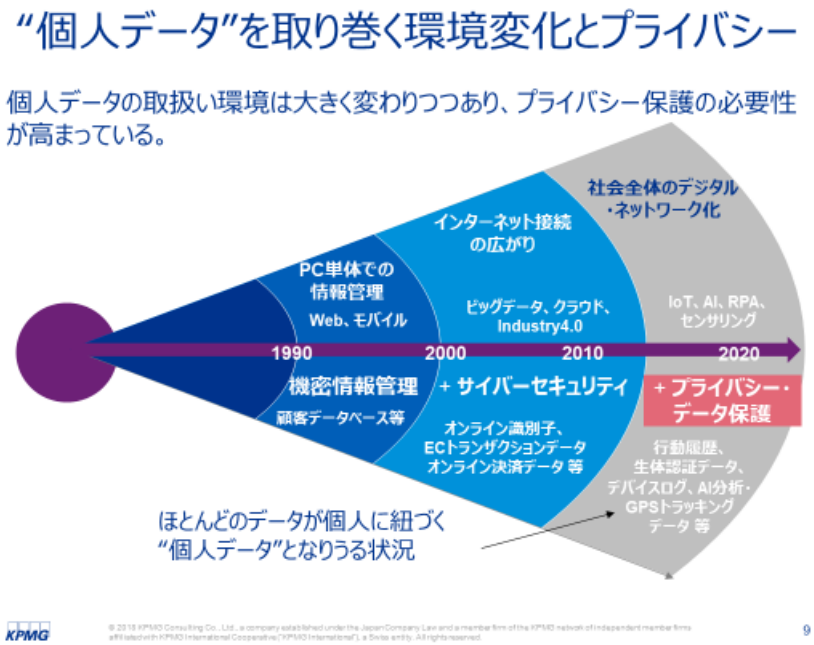
現在、世界中でプライバシー関連の規制が一斉に見直されている。2018 年 5 月に欧州連合（EU）の一般データ保護規則（GDPR）が施行されたが、その 1 か月後には米国カリフォルニア州で消費者プライバシー法が成立（2020 年 1 月施行）、またインドやブラジルでも GDPR と同様の内容の個人データ保護関連法案が議会に提出、可決されている。

なぜ今、このタイミングで規制が見直されているのか。それは、デジタル時代になってプライバシーに対する新たなリスクが顕在化し、その手当てが必要となってきたためである。

では、従来との違いは何か。一例としては、消費者が意識していないところでデータが継続的に収集され、個々人のビッグデータとして海外のどこかのサーバーに蓄積されていく点や、それらのデータをもとに行われる人物像の推定（プロファイリング）は本当に正しいのか、さらには推定に使用されている自分のデータは本当に正確なものなのかを本人が把握できない点が挙げられる。このような問題からも新たな規制が必要となってきている。

GDPR の前身である EU 一般データ保護指令が採択された 1995 年当時、インターネット利用者は世界人口の約 0.3%だったが、現在は約半数にまで伸びている。また、約 9 千万件だった携帯電話の回線契約数も 2017 年には 50 億件と世界人口比 75%まで伸びており、デジタル化、インターネット化は著しい。

デジタル化が進むほどプライバシー保護は重要となる。2015 年に世界経済フォーラムが今後 10 年間に予想されるイノベーションのメリットデメリットを公表しているが、そこで挙げられたほとんどのイノベーション項目のデメリットとして「プライバシー侵害」が挙げられている。デジタル化やイノベーションが進めば進むほど、プライバシーの問題は避けて通れないものとなってきている。



各国の法規制見直しが進む中、注意すべき点として国内と海外規制における個人情報の定義の違いが挙げられる。GDPR や中国サイバーセキュリティ法、米国児童オンラインプライバシー保護法（COPPA）など、IP アドレスや Cookie、デバイスの型番等までを個人データとして定義している例は多いが、現状、日本ではこれらの項目が個人情報という意識が薄い。例えば、IP アドレスに関しては、IPv6 になるとユニーク Identifier の組み込みが可能となり、異なる wi-fi 環境から接続してもトラック可能となるため、リスクがあると指摘されている。

また、各国では様々な経緯から個人データをかなり幅広くとらえている。例えば、GDPR を作成した第 29 条作業部会は、従業員データに関するリスク評価の要請例として、

- 情報漏えい防止対策として導入する DLP（メール送受信の自動チェック等を行うもの）ツールや MDM（モバイル機器のリモート制御サービス）の利用
- 社用車の GPS トラッキング
- 採用段階での SNS 等によるバックグラウンドチェック
- 従業員に貸与するウェアラブルデバイスのデータ管理　等

を挙げている。今やデータはマーケティング部門だけでなく、企業のあらゆる部門で活用されているが、ここまで個人情報管理台帳に入れている日本企業は少ないと思われる。

Cookie に関しては、本来の目的で訪れた Web サイトをきっかけに、それ以外の Web サイトの閲覧状況等も収集された後、事業者間で共有され、広告配信などに利用される仕組み

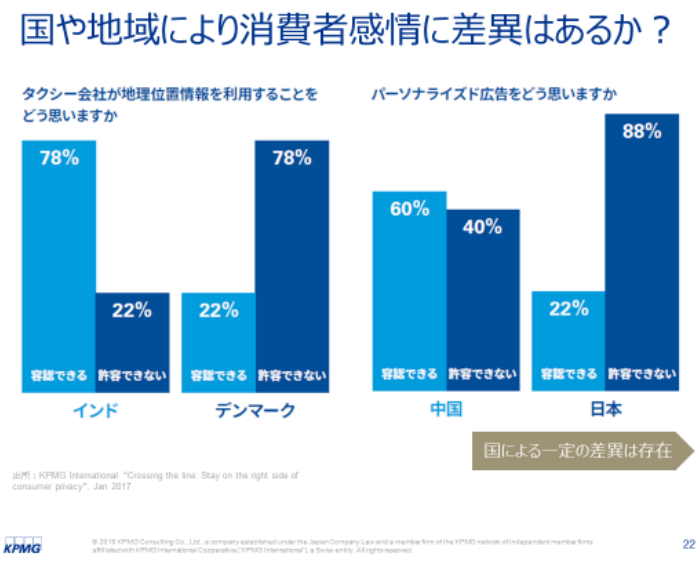
が出来上がっている。本人が最初に訪問した Web サイトの利用目的に同意しているので法制度上は問題ないが、KPMG が実施した調査では個人情報の取扱いに関する同意文を確認している消費者は 1 割にも満たず、何をどこまで同意したのかがわからなく不安や懸念が高まっている。報道などでもプライバシー問題が取り上げられるようになり、社会の意識が向けられる中で企業には、法律だけでなく消費者に寄り添った対応が求められる。

消費者プライバシーに関するグローバル意識調査

KPMG が 2017 年に世界 24 か国で行った消費者のプライバシーに関する意識調査では、企業のデータ管理に対し、56%が強い懸念を抱いており、特に中国、インド、シンガポールでは企業への信頼度が低かった。また、業種別でみると公益企業に対しても高い懸念を持っており、消費者は、Cookie の設定や SNS の設定変更などで能動的に自らを守ろうとしている。しかし日本の回答者は、企業に個人データを渡したくないという回答が最も多かったにも関わらず、プライバシー保護のための行動をとっている割合が 24 か国の中で最も低く、具体策を理解していないという結果が出た。

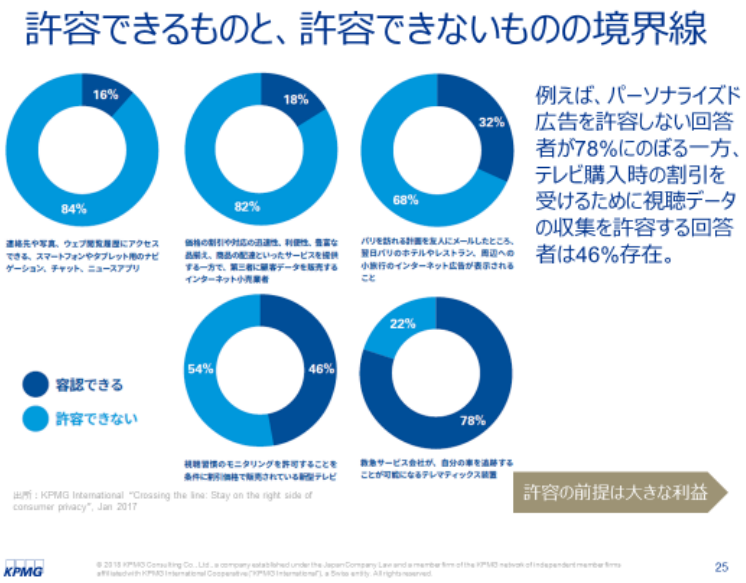
「消費者は何を不快に感じるのか」に関しては、半数以上が性別や教育水準、民族等通常機微と思われる個人データのネット公開には抵抗がないとする一方、ネットの検索履歴や所得、住所等本人到達性が高い情報や行動履歴の公開には抵抗が強く、さらに企業が自身の個人データを販売し利益を得ることに対しては、大きな不快感を抱いているという結果となった。

また、調査では所得や教育水準による消費者感情の違いはほぼ見られなかったが、国や地域によって許容できるサービス等には差が見られた。日本で常識的に問題ないと思われるものが他国では不快感を生じさせる可能性があり、企業としては炎上リスクを考慮すればセンシティブな人・地域にレベルを合わせることが重要となる。



利便性とプライバシーに関しては、約 3 分の 2 の回答者が個人データを利用するスマホアプリやタブレットアプリを不快に感じており、ほとんどの国の回答者が、プライバシーに関する管理策の実施が、利便性よりも重要と考えている。

一方で、プライバシーへの懸念を抱きつつも実際には個人データを渡すケースは多い。これは、デフォルトの設定を敢えて変えようとしない、メリットによりデメリットが隠されるといった行動バイアスによるもので、英国やオーストラリアの規制当局では、企業が行動バイアスを仕掛けることを監視する動きも出ている。このような状況の中では、自分が不快なことは行わない、が確かな指針となり得る。



参考：[「消費者プライバシーの境界線を越えないために：消費者プライバシーデータに関するグローバル意識調査」](#)（外部サイト：KPMG コンサルティング）

プライバシー保護のために必要なこと

今後のビジネスでデータ活用は必須であり、適切なデータ取扱いを確立できれば、グローバル大手企業とも戦うことができる。ビッグデータが実際に活用される状況を踏まえ、これまでの対応から、データポータビリティの権利、プロファイリング拒否の権利、忘れられる権利、同意撤回の権利といった本人の権利保護のために、1)本人への必要十分な情報の提供、2)本人への選択手段の提供、3)問合せへの対応体制整備を行っていく必要がある。

データのオーナーシップについてはいろいろな議論があるが、個人情報に関しては本人のコントロール権が重要になってくると考えられる。

施行半年、企業の GDPR 対応における課題と対策

基礎編：GDPR 対応のために実施すべき事項

GDPR には個人情報の保護とデータ流通促進の二つの面がある。データ流通という点から言えば、1995 年に採択された EU 一般データ保護指令は、それに基づき各国での法整備を求めていたが、各国の規制にばらつきがあり、EU 域内でのデータ流通の障壁となっていた。デジタル・シングル・マーケット（DSM）を実現させるためには、域内共通に適用されるルールが必要となり、指令から規則に格上げされ、EU 加盟国すべてに強制力を持つ一般データ保護規則（GDPR）が整備された。

欧州経済領域（EEA）域内各国に適用されるルールだが、以下のような場合には域外の企業にも適用される。

・EEA 在住者に商品やサービスを販売している。
・EEA 在住者の行動モニタリングを行っている

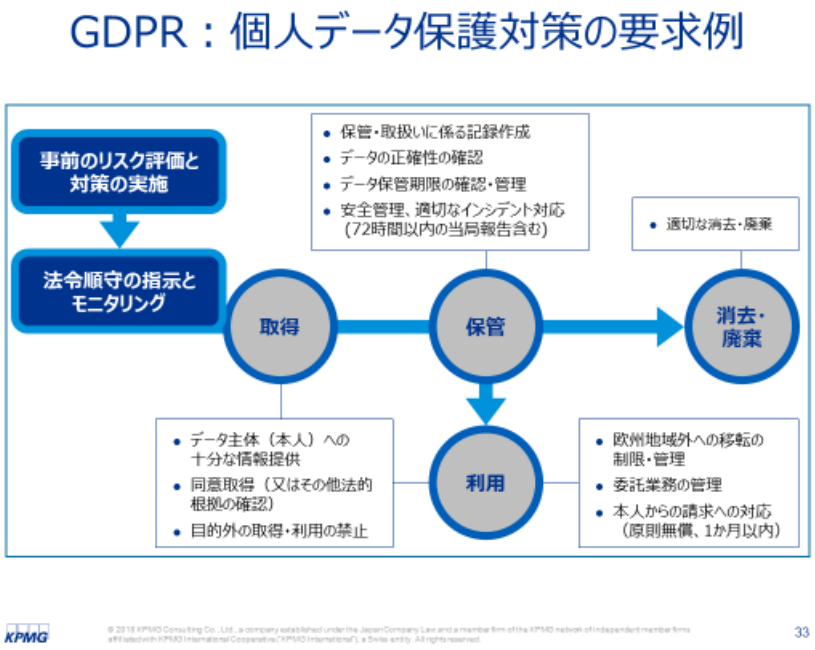
域外適用の枠組みがないと結果として法律が骨抜きになってしまうため、世界各国で域外適用の考え方は取り入れられている。

KPMG では、Web サイトで無料の GDPR 対応簡易診断ツールを提供しており、以下のような質問に答えることで自社の GDPR 対応状況を概観することができる（質問は全部で 16 項目）。

参考：GDPR 対応プロジェクト簡易診断（外部サイト：KPMG Web サイト）

- 自社グループ内で収集、処理、保存されている EU 在住者の個人データを網羅的に把握できているか。（顧客、従業員）
- EU 在住者の個人データ取得の際の同意取得にかかるルール手順を定め実施しているか。（日本の国内法より詳細な条件が設定されており、騙し打ちのような同意取得はいつでも無効とするとなっている。）
- データ保護オフィサー（DPO）の設置要否を判定し、設置する場合に役割・責任を定めているか。（大規模にデータ主体の監視を行う場合やセンシティブな情報を大量に扱う場合は DPO の設置が必要となる。DPO の要件としては、法令遵守状況をモニタリングし指導できること、経営から独立していること、専門知識を有していること、監督機関からの要請に対応できること等が求められる。このほかにも各国で独自に追加要件を設定することができるため、留意する必要がある。）
- データ保護影響評価（DPIA）を実施するルール・手順を定めているか。
- 個人データのリスクレベルに応じたセキュリティ対策を講じているか。
- 事故を認識してから 72 時間以内に監督機関へ報告できるように具体的な報告手順を定めているか。（ただし、データ主体にリスクを生じ得ないような状況であれば報告不要。）

・ EU 在住者の個人データを EEA 域外へ移転する場合のルール・手順を定め運用を開始しているか。（適切に移転先で管理が行われるよう契約がなされていればよい。）
・ グローバルで利用される IT システムにおいて、意図しない国際移転リスクに関する評価・対策がなされているか。（アクセス権を持つ末端に至るまで同じ管理義務を課す必要があり、逆にアクセス不要な部分についてはアクセス遮断の措置を講じる。）



応用編：顕在化した課題と解決のアプローチ

多くの企業が GDPR 施行前に「必要最低限の対応をしたい」としてデータマッピング、処理記録・域外移転等への対応（SCC 締結）、管理体制・ルールの整備、システム上のデータ保護方針の策定を行ったが、そこで止まってしまっているのが現状で、継続的なマネジメントシステムの運用、ルールに従った取扱いの実施・データガバナンスまで行っている企業は少ない。顧客データベースから様々な部署がデータをコピーし独自に使用しているケースは多く見られるが、顧客からの削除依頼がコピーデータにまで反映されず各部門が引き続き顧客にアクセスしてしまえば、社会的に大きな批判を招く可能性が高い。また、セキュリティインシデントによりデータ漏えいが発生した場合に、EU 在住者データの有無や数をすぐに把握できる体制にもなっていない等、企業においてマネジメントシステムが機能していないことが大きな課題として顕在化してきている。

例えば、個人データの新たな取り扱いが発生する場合、それを事前に管理部門が把握し、必要な手当てをフィードバックし体制を整えてから実際の取り扱いを開始し、さらにそれをモニタリングするという一連のプロセスが予め整備されていないと、様々なところで新

たな個人情報の取扱いが発生してもその影響評価を行うこともできないまま野放しとなり、重大な法令違反・事故を引き起こすリスクを排除できない。

GDPR ではプライバシーバイデザインのプロセス整備を求めており、個人データ取扱いの事前把握は必須となる。さらに GDPR では DPIA も求めている。「自社はセンシティブ情報を扱っていないので DPIA は不要」としている企業を多く聞くが、GDPR の DPIA 要件のうち 2 つ該当するものがあれば DPIA を実施する必要がある。また、例え現在は該当するものがないとしても、近い将来取り扱う可能性は非常に高く、対応できる体制作りは必要である。

（参考）GDPRデータ保護影響評価要件

	データ保護影響評価の実施要否を判定するリスク要素（2つ以上該当でDPIA実施が必要）	センシティブデータの定義
情報種別	センシティブな個人データ、極めてプライバシー性の高い個人データを取り扱う場合	人種若しくは民族的素性、政治的思想、宗教的もしくは哲学的信条、または労働組合員資格に関する情報、および遺伝データ、自然人の一意な識別を目的とした生体データ(生体認証データ等)、健康に関するデータまたは自然人の性生活もしくは性的指向に関するデータ、有罪判決又は犯罪に関連する個人データ
	弱い立場にある個人のデータを取り扱う場合（子ども、従業員、患者、高齢者等）	
データ処理	個人データを用いて本人の評価またはスコアリングを行う場合	
	個人データに基づいて自動処理により契約内容を決定する場合	
	個人の体系的な監視を行う場合	
	個人データを大規模に取り扱う場合	
	異なる目的で取得した複数の個人情報データベースの照合または結合を行う場合	
	革新的技術を利用して個人情報を取り扱う場合（IoTやAIの利用等）	
	個人データの処理が本人の権利行使、サービス利用、契約締結などを妨げる場合	

KPMG

56

実際のビジネスでは、法令で定義された個人データの管理さえ行っていれば問題ないとはならない。企業における管理要件は、リスクベースで考える必要がある。法令要件だけで考えていると、マルチステークホルダーでビジネスプロセスを構築しようという発想にはなかなか繋がらない。本質的に何が大切なのかを考えながら、対策を講じていく必要がある。

世界各国の個人情報保護に関する法規制が次々と見直されていく中で、グループ全体の体制を整えるために、私たちは、まずグループ共通ポリシーを規定した上で、その下に各国固有の法令要件や拠点別に求められる対応（日本のマイナンバー対応や GDPR の EU 在住者データの扱い）を細則として設け、さらにその下でガイドラインや手順書を整理することを提案している。さらに、細則の中で共通化できるものは可能な限りグループポリシーに上げていくことが、現場の混乱をなくすためには重要となる。また、グループ全体で体制を整備するには、本社がリーダーシップを発揮し、リスク評価のグループ統一基準の作成や各国法規制の把握、拠点間の調整を行う役割を担うことで効率化が図れる。

まとめ

個人データの取扱いはますます高度化・複雑化し、各国の規制も強化が進む一方で、個人データの利活用は企業にとって死活的に重要となってくる。各国の法改正の都度パッチワーク的に対応を行うのではなく、抜本的にデジタル時代においてどのようなプライバシー保護策が必要なのか見直すことで、安心してデータ活用を推進できる管理体制が整備されると考える。

GDPR はとかく巨額な罰則金が注目されがちだが、プライバシーの問題は単に罰則金で済む話ではなく、営業停止や企業ブランドの毀損、消費者からの賠償請求等、これまでの経営が一気に傾く可能性もある最重要経営リスクの１つである。さらに、今後のイノベーションとプライバシーはセットで考える必要があるので、管理体制整備の役割は非常に重要なものとなってくる。