KPMG

プライバシー技術：What's next?

自動化時代における
データプライバシー技術の進化

OneTrust
PRIVACY, SECURITY & GOVERNANCE

はじめに

データ漏洩に伴う手痛い損害、終わりのないセキュリティ課題、オンラインサービスのパーソナライズ化、押しつけがましい広告戦術、消費者データの共用。昨今のビジネスにおける個人データの利活用やその保護策に対する消費者の懸念は、今や消費者データプライバシーの問題を重要な経営課題へと押し上げています。

消費者は、単にデータの保護に関心があるだけではなく、自らの個人データがどのように利用されるのかについて、より多くのコントロール権を要求しています。また、規制当局は、不適切なデータの収集や共有の慣習に対して目を光らせ、厳格な法規制を次々と成立させています。

KPMGの「Me, my life, my wallet（私、私の人生、私の財布）」調査によると、消費者の55%は、企業に対する最優先の期待事項としてデータ保護対策を挙げており、47%は、企業が自身の個人データの販売や共有をしないよう求める、と回答しています[1]。

また同時に、疑心暗鬼になっている消費者の間で、企業活動への信頼が失われつつあります。KPMGの「The new imperative for corporate data responsibility」レポートによると、調査対象となった消費者の68%は、企業が個人データの第三者提供を倫理的に行っているかどうかを疑っています。また、消費者の50%は、個人データの保護について企業を完全には信用していない、と回答しています[2]。

継続する消費者トレンドースマートフォンやソーシャルメディアの広範な普及、オンラインショッピングへの大規模なシフト、カスタマーエクスペリエンスのパーソナライズ化などーは、爆発的に多くの消費者データを生み出し、5GやAI、IoT（モノのインターネット）などの先進技術がそれらの共有や利活用を劇的に高度化させています。そして、それらによって複雑なデータセキュリティやプライバシー保護の問題が生じているのです。

広がり続ける現在のデータ空間を効果的に管理していくために、データプライバシー技術の実用化は急務となっています。本レポートでは、急速に変容するビジネス環境において、データプライバシー技術やその管理策がどのように活用されるのかという点について考察しています。

Sylvia Klasovec Kingsmill
Global Cyber Privacy Leader
KPMGインターナショナル

Kabir Barday氏
CEO
OneTrust

*本レポートは、2021年5月にグローバルで発行されたレポートを翻訳したものです。

目次

06 エグゼクティブサマリー

08 チェンジドライバー

12 プライバシー分野への技術の適用

16 変化する消費者プライバシー技術

20 プライバシー重視のソリューションの広がり

24 企業のためのプライバシー技術とは

30 今後の展望

34 KPMGによる支援

エグゼクティブサマリー

データプライバシーとセキュリティに対する消費者の懸念は、現在あらゆる場所で取り上げられるビジネス課題となっています。急速に進化する消費者向けのテクノロジーやアプリケーションの普及により、個人データの利活用に関する管理強化や透明性を求めるニーズは明白で、5GやIoTなど、革新的技術の進化を背景として、その状況はさらに複雑化しています。

オンライン追跡や同意のないデータ共有、ターゲティング広告、データ漏洩などに対する消費者の懸念や企業への不信に係る問題を背景として、世界中の国々が新たな個人情報保護法を相次いで施行し、規制当局は新たなグローバル規制に注目しています。企業は、膨大な数の規制変更に加え、次々に生まれる新たなテクノロジーや増大する脅威、消費者の関心の高まりなどにより、適切なデータの取扱いについて前例のないプレッシャーを受けています。

今日のデータ課題に対処するためには、新たな時代の大胆なデータ利活用やその管理に対応できるプライバシー技術の活用が必要です。企業は、競うようにデータプライバシープログラムや関連システム、ツールを開発し、強化しています。そして、新しいプライバシー基準を遵守し、急速に変化する視点と要求事項に対応しようとしています。

また、警戒心の強い消費者は、自身のデータの新たなコントロール権を行使するために、個人データ保管庫や権利行使のサービスプロバイダー、情報銀行などにも注目しつつあります。一方、プライバシー強化技術や次世代のプライバシーポータル、その他新たに生み出されるさまざまな機能は、企業が適切なデータ管理の仕組みへ切り替えていくことを後押ししています。そして、その過程で無視できないのは、信頼できるデータ倫理の枠組みの必要性でしょう。

最終的に、企業は完璧な「データ管理の仕組み」、つまり、プライバシー、セキュリティ、倫理面での懸念を効果的に低減でき、知見に基づく意思決定やイノベーション、収益拡大等の新たな機会をもたらしてくれるような、個人データ管理要素の正確な“組み合わせ“を考案しなければなりません。

「テクノロジーとそれに付随するデータログは、あまりにも多くの場面で私たちの生活の一部となっています。企業が信頼を獲得・維持できなければ、警戒心の強い消費者は重要な個人データの共有に躊躇し、顧客中心主義のデータドリブンなビジネスを展開することができなくなるでしょう」と、KPMGインターナショナルのグローバル・サイバー・プライバシーリーダーであるSylvia Klasovec Kingsmillは述べています。

「デジタル時代における“信頼”は、組織のブランド、製品、サービス、人材の質に対してだけでなく、データの利活用やその管理に対しても重要となります。そのための今後の課題として、企業は、価値を創造し成功へ導くために活用する顧客データを適切に保護していることについて、外部への証明が求められるでしょう。プライバシー技術は、企業がこの道のりを歩むことをサポートする大きな機会を提供します。そしてそれを正しく理解した企業は、その証明を行ううえで大きなアドバンテージを得ることができるのです。」

チェンジドライバー

何が自動化への道を加速させているのか？

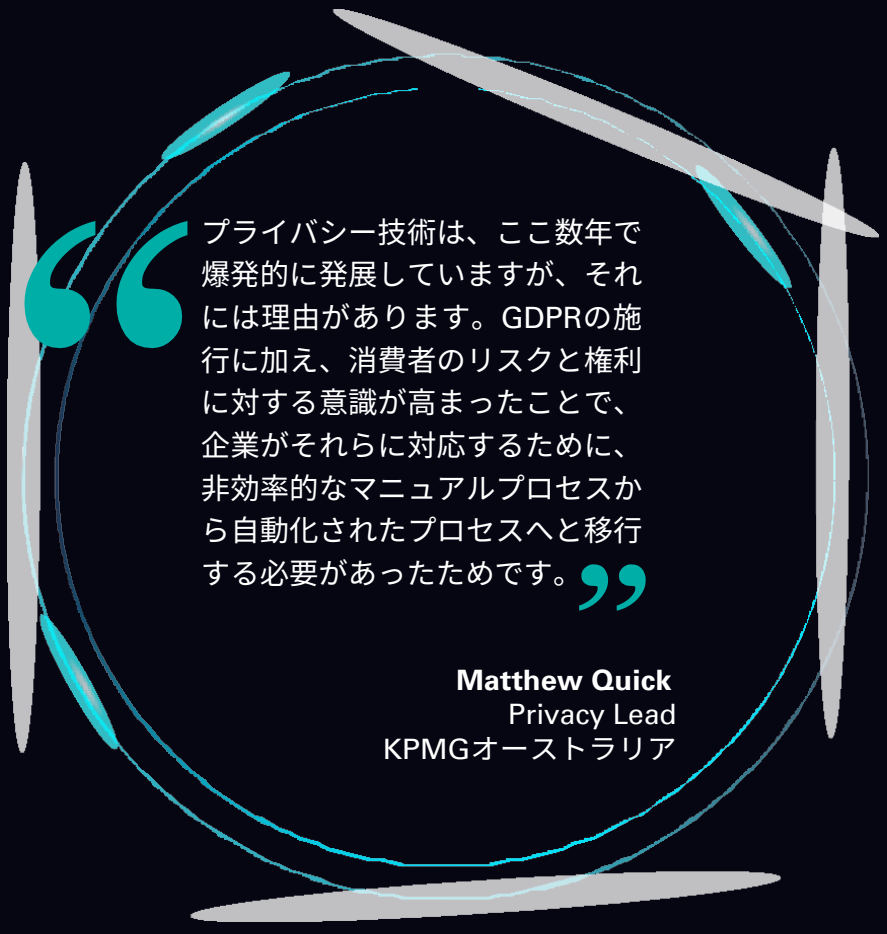
テクノロジーの進歩によりデータの収集や処理が広がるにつれ、消費者の懸念やプライバシー権に対する意識がビジネス市場や規制当局の間で注目されるようになり、企業はプライバシー保護の組織体制や業務プロセスを見直す必要に迫られています。プライバシー保護プログラムの新設または拡張、新たなプライバシー保護基準の遵守など、企業は個人情報保護に関する考え方の変化に対応するための戦略的なオペレーション変更を検討しています。

プライバシーチームに求められる業務量は急激に増加し、プライバシーエンジニアリングやデータ利活用に関する新しいスキルの需要が高まっていることで、プライバシーチームは今、岐路に立たされています。必要なデータのセキュリティと保護に関して、どうすれば効果的かつ効率的で一貫性があり、規模に見合ったタイムリーな対応ができるのでしょうか。

現在、100ヵ国以上の国で個人情報保護法が制定されていますが、グローバルな規制に加えて、オンラインでのトラッキングや広告、同意のないデータ共有、致命的なデータ侵害などに対する消費者の反発などもあり、すべての企業活動において、プライバシーコンプライアンスのための統合的アプローチの必要性が高まっています[3]。

テクノロジーだけでプライバシーやコンプライアンスの課題を解決できるわけではありませんが、企業が従業員や顧客、ステークホルダー、消費者市場と24時間365日対話するために、テクノロジーが重要な役割を果たしていることは確かです。

次のページの年表は、一般消費者のためのプライバシー保護対策の変遷を示しています。



プライバシー保護の進化

1361
イングランドの治安判事法が、「のぞき魔」や盗聴者を犯罪者として取り締まる[4]。

1792
米国議会が手紙のプライバシーを守るための法律を制定[5]。

1800年代
「封筒」が発明される。

1858
新聞社がElisabeth Félix氏の死に際の描画を掲載しようとしたことを契機に、フランスにおいて個人情報保護法が制定される[6]。

1888
Eastman Kodak社がスナップショット・フィルム・カメラを発明し、プライバシー侵害が懸念されるようになる[7]。

1890
米国の弁護士Samuel D. Warren氏とLouis Brandeis氏が、「プライバシーの権利」をHarvard Law Review誌に発表し、プライバシーが法的権利として認められるようになる。これは、晩餐会でのWarren氏の写真がゴシップ誌に掲載されたことが契機となった[8]。

1907
世界初の盗聴器「ディクトグラフ」が発明される[9]。

1928
米国最高裁が個人の電話の盗聴を違法と宣告[10]。

1948
世界人権宣言において、プライバシーの権利が確立される[11]。

1994
Netscape社が初めてオンライントラッキングを可能にするブラウザをリリース[12]。

1995
欧州連合（EU）が「データ保護指令」を採択[13]。

1997
SixDegrees.comの立ち上げによりソーシャルメディアが出現し、2002年にはLinkedIn、2004年にFacebook、2006年にTwitterが次々と登場。なお、「"知り合いの知り合い"といった関係をたどると、5人の仲介者を経て6人目で世界中の人々と間接的な知り合いになることができる」という発想をベースにしたSixDegreesは2001年に閉鎖[14]。

1999
Sun Microsystems社のCEOであるScott McNealy氏が、「プライバシーなんてものはないのだから諦めなさい」と公言[15]。

2000
米国とEUが、欧州市民の個人データを米国に移転できるようにする「セーフハーバー協定」に署名[16]。

2000
Ericsson社が、携帯電話、PDA、限定的なウェブ閲覧機能、タッチスクリーンを組み合わせた初のスマートフォンを発表[17]。

2008
App Storeが開設される。データドリブン型のモバイルアプリケーションの利用により、モバイルデバイスは非常に高性能な個人情報処理および共有デバイスへと変貌した[18]。

2010
Facebookがユーザープロフィールのデフォルト設定を「非公開」から「公開」に変更[19]。

2010
Facebook社（現：Meta Platforms社）のCEOであるMark Zuckerberg氏が、「プライバシーはもはや社会規範ではない」と公言[20]。

2011
ユーザー追跡機能が含まれる最新のスマートフォンが発表される[21]。

2012
Facebookユーザーの共有コンテンツが、週70億個にまで増加。米国の調査によると、利用者の70%は、データの取扱いについてソーシャルメディアを信用していない[22]。

2012
初めてモバイルインターネットよりもモバイルアプリケーションを利用するユーザーの方が多くなる。一方、 自分の周囲にいる女性を公開データに基づいて特定できるという「Girls Around Me」 のアプリケーションが配信停止となる[23]。

2012
New York Timesは、センサーの急増や新しいデータ形式の普及、ストレージ容量の増加などの流れのなかで、「ビッグデータの時代」を宣言[24]。

2013
WikiLeaksは、Edward Snowden氏が米国諜報機関による広範な監視を示す機密情報について暴露することを支援。国家安全保障と個人のプライバシーに関する世界的な議論を巻き起こす[25]。

2014
技術系出版書籍が、2014年を「ウェアラブルの年」と宣言。スマートウォッチとスマートリストバンドの販売台数は、それぞれ500万台と1,500万台に到達[26]。

2015
人類は1日で2.5百京バイトのデータを生成。これはDVD 6億2,500万枚分に相当する[27]。

2015
欧州司法裁判所は、欧州と米国の間で個人データの転送を認めるセーフハーバー協定が無効であると判決を下す[28]。

2015
IoTという言葉が生まれてから16年が経過。Amazon社がホームシステムの音声コントロールサービスを開始したことが、この年の画期的な出来事であった。そしてCisco社は、IoT機器の普及が150億台にのぼると推計[29]。

2016
アルゴリズムがデータを利用して将来の行動予測を行う「ダークパターン」 が登場[30]。

2016
EUが一般データ保護規則（GDPR）を制定。これは過去20年以上にわたるデータ保護規制の歴史において最大の変化であり、EU全体に適用される単一のルールセットで、より厳格な罰則を規定[31]。

2018
GDPRの施行後、EC（欧州委員会）は数十億ユーロの罰則金を科す[32]。

2019
多くの著名な企業が、GDPR違反で罰則金を科される[33]。

2020
COVID-19のパンデミックが世界中の日常生活と家計に影響を与える。

2020
Schrems IIに対する欧州司法裁判所（CJEU）の判決により、EU-US Privacy Shieldは無効とされる[34]。

2020
データ保護当局は、さらに多くの企業へGDPR違反の罰則金を科す。

2021
欧州連合理事会はePrivacy規則に合意し、欧州議会、欧州委員会との三者協議を開始[35]。

2021
バージニア州消費者データ保護法（CDPA）が成立。カリフォルニア州プライバシー権法（CPRA）に続き、米国で2つ目の州全体にわたるプライバシー法となる[36]。

2021
ドイツニーダーザクセン州のデータ保護委員会[37]やスペイン王国データ保護機関（AEPD[38]）により、企業は数千万ドル規模の罰則金を科せられるなど、罰金処分が続いている。

未来
テクノロジーはかつてない速さで消費者のプライバシーを浸食している。プライバシーは2050年までに完全に姿を消してしまうのか、それとも消費者が取り戻すのか？

プライバシー分野への技術の適用

プライバシー技術を活用して、プライバシーの全領域をカバーする

ビジネスにおいて、異なるシステムを統合して業務を自動化する強力な新技術やツールがますます活用されるなか、新時代のプライバシー意識の高まりは、企業にプライバシーシステムやプログラムのさらなる進化を求めています。

データセキュリティやプライバシー保護を強化する競争において、テクノロジーは手動プロセスに取って代わり、企業が世界各国のプライバシー規制を遵守するための強力な手助けとなっています。

次世代のプライバシー技術への移行が進むにつれ、プライバシー技術がおおむね3つの重要領域：「プロセスオーケストレーション」、「個人データ管理」、「ガバナンス、リスク管理およびコンプライアンス（GRC）」に整理できると考えられます。

> “プライバシー技術分野は、急速に成熟した産業へと発展しており、多くの企業においても、CPO（最高個人情報責任者）の抱える課題や関心の中核に位置づけられるものとなっています。この技術の適用を考える場合、サイロ化された閉じた視点ではなくエコシステムのレンズを通してアプローチすることが重要です。プライバシー自動化の技術とは、データの管理や保護、プライバシープログラム管理の効率化や費用対効果の向上など、さまざまな側面における補完技術を紡ぎ合わせるものと言えるでしょう。”

Orson Lucas
Privacy Lead
KPMG米国

プロセスオーケストレーション

プロセスオーケストレーションとは、オペレーションを改善し効率を向上させるために、プロセスを標準化することです。プロセスオーケストレーションには自動化も含まれ、これを活用することにより、企業は時間やコスト、リソースを低減しながら、首尾一貫した形でタスクやプロセスを完了させ、それらを継続的に改善していくことが可能となります。

これは、プライバシーチームが消費者や規制当局への義務を果たすうえで重要なことです。プライバシー技術のソリューションの場合、たとえば個人データへのアクセスに対する開示請求に対応する場合などにプロセスオーケストレーションが活用できます。手動のアプローチでは、応答に一貫性がなく対応が不十分となったり、必要以上に時間がかかり複雑な請求に対応できる専任のプロジェクトチームが必要になったりすることもありますが、ソリューションの活用によりこういった問題が解消できるでしょう。

プロセスオーケストレーションでは、このような請求を構造化された形式で整然と管理し、業務効率を高めてコストを低減できます。また、KPMGの提唱する“優れた顧客体験のための6つの柱（Six Pillars）にも適合できるのは大きな利点です[39]。6つの柱を理解し、それを実現する企業は、より良い成果を生み出し、急速に成長するとともに、株主価値を高めています。

個人データ管理

個人データの管理で重要なことは、データを効果的かつ安全に収集、保持、利用することで、企業はさまざまな方法でこれに取り組んでいます。
それは、支払い情報や配送伝票を扱う小売企業であっても、クライアントのためにセンシティブな契約情報を保持する企業であっても同様です。
そして、プライバシーに関する消費者の要求や期待に応えるためだけでなく、収集されたすべての個人データがどこに提供され、そのデータが何に使用されるのかについて把握する必要があります。

優れた顧客体験のための「Six Pillars：6つの柱」

1. パーソナライズ
さまざまなリクエストを送信できる自動化されたフォームを活用するとともに、データ主体が自身の個人データの利用状況を閲覧できるダッシュボードを表示する。

2. 誠実性
データ主体による開示請求への対応において、適切な期間内に適切な方法で回答するなど、誠実な姿勢を示す。

3. 期待の充足
リクエスト受付後はすぐにデータ主体へ応答し、常に最新情報の提供に努める。そして明瞭な回答を行うことにより、顧客の期待に応え、さらに上回る。

4. 問題解決力
データ主体の要求に応えることに注力し、今後取り得る選択肢を提示する。

5. 利便性
リクエストへの応答に自動化プロセスを導入し、データ主体への対応に要する時間と労力を最小限に抑える。

6. 親密性
共感を示し、データ主体の要求を理解したうえで優先事項として扱う。

データの保管・保持や利用を規制するプライバシー法令への対応のためにも、データマッピングとデータの管理は特に重要です。これは、データの共有やローカリゼーション、または削除に関するコンプライアンスの課題にも関係します。
プライバシー技術のソリューションは、個人データの管理や記録作成を、スピード、正確性、効率性において新たなレベルまで高めることができます。データ検出の自動化を提供するソリューションは、個人データの所在の特定や、消費者要求への効果的な対応を可能とします。また、暗号化、マスキング、アクセス制御の自動化による追加的なデータ保護要件の充足といった点でも、プライバシー技術のソリューションを適用できるでしょう。

GRC

ガバナンス、リスク管理、およびコンプライアンス（GRC）の業務は、広範な責任範囲をカバーし、さまざまな形態で行われています。効果的なGRCの中心には、連結されたデータモデルがあります。それは、プライバシー関連リスクやコンプライアンスに係る統制を、レピュテーションリスクや法令遵守といった全社レベルでのリスク管理に結び付けます。

賢明な企業はますますGRCに注目し、さらに広く捉え、顧客視点をも取り入れるようになっており、結果として高い信頼の獲得につなげています。現在、すべての防御ラインやリスク種別にまたがるリスクの統合的な視点を得るために、統合GRCまたは統合リスク管理へと向かう流れが生まれています。リスク種別には、テクノロジーや業務運営、プライバシー等が含まれます。GRCテクノロジーの観点からは、「リスクエコシステム」が重要なトレンドとなっています。

プライバシー強化のために、今後プロセスオーケストレーションとGRC管理プロセスが最高レベルのプライバシー技術と統合され、包括的なプライバシーリスク管理が可能になると考えられます。近い将来には、リアルタイムの洞察を生み出すデータドリブン型GRCが標準となり、それらがプライバシーリスクの把握や管理の方法を変えていくでしょう。

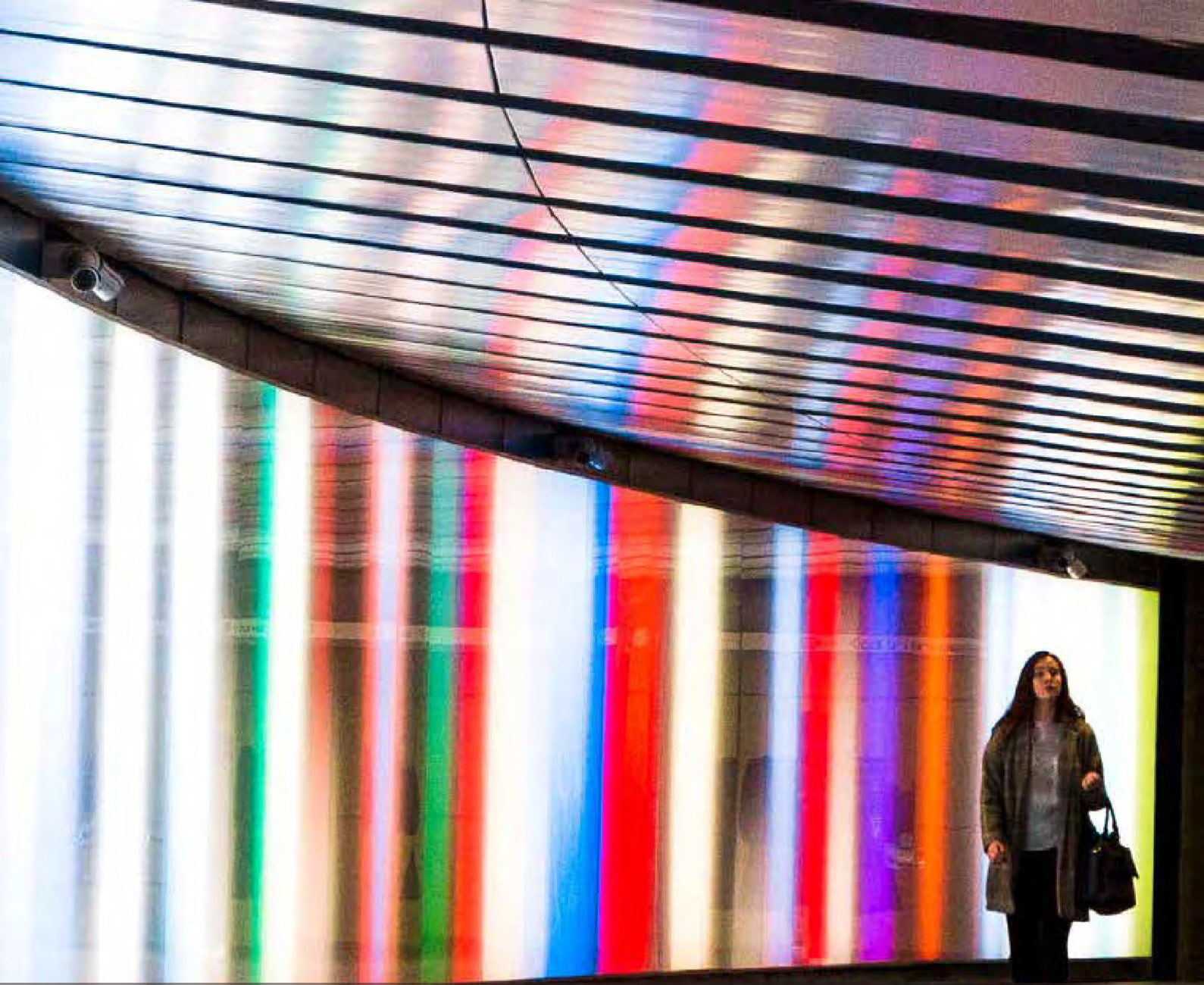
> “プライバシー技術は、プライバシーフレームワークや関連統制の導入に、自動化、拡張性、革新性をもたらします。大規模なプライバシー変革プログラムの成功や関連コストの削減、リードタイムの短縮に不可欠なのは、プライバシーの専門家が、ありふれた運用タスクではなく変化を促進することに集中できるようなプライバシー関連プロセスを確立することです。”

Maliha Rashid
Privacy Lead
KPMGローワーガルフ

す。

変化する消費者プライバシー技術

消費者向けテクノロジーが私たちの生活に与え続ける影響



デジタル技術を駆使して家事を自動化するスマートホームから、私たちの健康状態をモニターする「賢い」ウェアラブルまで、消費者向けテクノロジーは私たちのライフスタイルに浸透し、その形を変え続けています。今日の発展の中心にあるのは、無限に流れる個人データです。そしてそれは、消費者プライバシーを脅かす潜在的な脅威を数多く抱え込んでいます。本章では、消費者向けテクノロジーを取り巻く環境がどのように変化しているかを解説します。

> “アフターコロナにおいて、世界的に消費者のオンラインへのシフトが進んだことで、消費者向けビジネスでは自動化が新たな流れとなっています。消費者向けデバイスやアプリケーションのエコシステムに素早く適応可能な市民開発者も増加しているなか、幸いなことに、自動化、AI、分析技術の活用やそれらの既存プラットフォームとの統合は以前より容易になっており、ビジネスが求めるペースでプライバシーバイデザインを取り込むことができるようになってきています。”

Natalie Semmes
Head of Intelligent Automation
KPMG英国

IoT、5G、エッジコンピューティング

IoTが急速に普及したことにより、プライバシーの課題も増加しています[40]。

これらの機器は、私たちのあらゆるニーズや欲求に対応できる、膨大な数の新しいサービスや顧客体験を生み出せる可能性を秘めており、そこで処理されるデータ量も飛躍的に増加しています。今後、IoTの持続的な成長の鍵となるのは、5G技術の順調な展開と、エッジコンピューティングの継続的な開発です。5Gは、高速化、低遅延化、帯域幅の拡大を実現し、これにより数十億台のコネクテッドデバイスがこれまでにない大量のデータを送信できるようになります。エッジコンピューティングは、データソースの近くでのデータ処理を可能にし、転送しなければならないデータ量を削減できます。

このような技術進歩は、ビジネスの相互接続に関して、スピードや拡張性、効率性を劇的に向上させるものと期待されていますが、その一方で、テクノロジープロバイダーはますます多くのデータポイントで豊富なデジタルフットプリントを収集できるようになるため、プライバシーに関する新たな懸念も生じます。

もしプライバシー保護やセキュリティの対策が追いつかなければ、個人データの流出はほぼ避けられず、私たちの個人的な行動習慣はますます露見してしまうでしょう。

> 5Gやエッジコンピューティングは、次の産業革命を実現するプラットフォームとなります。これからは、デジタル経済を難なく進む野心的なビジョンと破壊的モデルを持つ企業が成功者となり、驚異的な収益や顧客成長率、市場シェアの目標を何度も達成するでしょう。

Alex Holt
Global Head of Telecoms & Media
KPMG米国

人工知能（AI）

AIは進化し続けており、プライバシーを脅かしながら個人データの利用能力を高めています。
個人データを利用して洞察を得ようとすると、個人データが本人の予期しない方法、または無許可で使用されたり、本人の利益を損なうような結果が生成されたりと、プライバシーに対する本人の期待に反する可能性があります。
AI利用に関する懸念の例としては、プライバシーの侵害とみなされる可能性のある顔認証データの利用ケースや、センシティブではない形式のデータからセンシティブな情報を推定または予測するAIおよび機械学習アルゴリズムの利用などが含まれます。

また、アルゴリズムに含まれるバイアスや、テクノロジーがシステムによる差別を不用意に増幅させてしまう可能性、さらには、同意や選択、自動化された意思決定に付帯するプライバシー上の課題などについても、激しい議論が交わされています。

AIの取組みが機械学習から深層学習へと移行し、人工的なニューラルネットワークが自ら学習してインテリジェントな判断を下すようになるにつれ、AI主導のデジタルアシスタントなど、企業が消費者と対話する際にもAIが大きな役割を果たすようになってきました[41]。

AIや機械学習の能力が進歩するにつれ、企業は、ビジネス上の洞察や意思決定の自動化を促進するために、データをどのように使用しているのかについて、消費者へ情報を提供する必要があることは明らかです。

仮想現実（VR）と拡張現実（AR）

仮想現実（VR）、拡張現実（AR）、複合現実（MR）は、現実世界とデジタル世界の境界を曖昧にしています。MRは、完全な没入型のVR体験と、デジタルで拡張されたAR体験の間に位置し、現実体験とデジタル体験を組み合わせたものです。

これらの技術の可能性は、多くの人々から注目されています。非営利団体“Charity: Water”は、VR技術を活用することで、メトロポリタン美術館に集まった400人をエチオピアに連れていき[42]、13歳のSelamという少女が毎日家族に水を届けるまでの長い道のりを伝えました[43]。また、ゲームの世界では、長期にわたり「ポケモンGO」がARの力を示す好例として取り上げられています。

新型コロナウイルス感染症（COVID-19）が職場環境を変えていくなかで、仮想的なインタラクションを提供し、顧客体験を向上させるシステムに注目が集まっています。しかしながら、これらのテクノロジーの中心には、生体データの収集や消費者向けアプリケーションからの常時データ収集も含まれます。トラッキングセンサーを介して収集されたデータは、より信憑性のあるディープフェイクを作成するために使用される可能性があり、また、アイトラッキングの改善は、ユーザーエクスペリエンスの向上に役立てられると同時に、ターゲット広告とのインタラクション状況を広告主が正確に測定できる機会を提供します。このようなテクノロジーの開発により、プライバシーの懸念がさらに高まると考えられます。

新しいVRやARシステムの市場投入が急がれるなか、適切なプライバシーへの配慮についても見落としてはなりません。

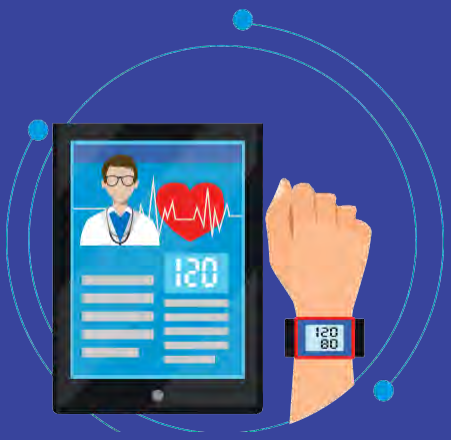
ソーシャルネットワーキング、コラボレーションとテクノロジー

ソーシャルメディアユーザーのプライバシーに関する懸念は、近年急増しています。度重なるデータ漏洩や、プロフィールデータの悪用の可能性、セキュリティ上の問題などにより、ユーザーはソーシャルメディアとの関係やデータの安全性について再考するようになりました。

プライバシーへの関心は衰えることなく、結果として消費者のプライバシー保護技術の採用も爆発的に増えています[44]。しかし同時に、過去12ヵ月間にソーシャルメディアのプライバシー設定を更新した消費者はわずか3人に1人で、より強固なパスワードの設定を行った消費者は24%にすぎませんでした[45]。一方で、世界的なパンデミックによるリモートワークやオンラインでのバーチャルミーティングの普及は、セキュリティやプライバシーのさらなる課題をはらんでいます。

消費者は、ソーシャルメディアサイトやコラボレーション技術に関連するプライバシーの影響についてますます懸念を深めており、より安全なシステムの登場が期待されています。

ヘルスケアテクノロジー



最先端の技術開発は、長らく医療業界において先導され、患者への対処に適用されてきました。1970年代にはIT活用による患者の電子カルテ作成が行われ、2000年代にはパーソナルデジタルアシスタント（PDA）が日々の臨床に活用されるようになりました。そして現在では、VRを利用した3Dモデルの作成により、外科医が手術前の訓練を行えるようにもなっています。

近年では、家庭用医療機器の開発にもIoTの利用が増えています。たとえば、Medtronic社がFitbit社と提携し、継続的な血糖値モニターのデータとFitbitアクティビティトラッカーで収集されるデータを統合する試みなどが行われています[46]。今後、5Gによる接続性の向上により、健康観察機能はさらに向上し、医療機関による迅速な対応が可能になるでしょう。

しかしながら、このような進歩は、センシティブな個人データの問題も生み出します。Kantar社の調査によると、今日の医療テクノロジーが適切なデータセキュリティを提供していると考えている消費者は、わずか38%にとどまっています[47]。

プライバシー重視のソリューションの広がり

プライバシー技術はどのように進化しているか

消費者向けテクノロジーが進化するにつれ、消費者が自身のデータやプライバシーを管理できるようにするプライバシー中心のソリューションも進化しています。

パーソナルデータストアとデータプライバシー

パーソナルデータストアは、消費者が個人データの安全管理を行うための一元化された場所を提供します。一般的に、このソリューションでは個人が自身の個人データの台帳を作成・管理し、それらのデータをどのように共有するか選択できるようにします。

しかし、これらのソリューションの多くは、まだ主流になっていません。個人情報を一元管理することで、データの管理が容易になり、単一の正しい情報源として機能することができる一方、万が一そのコピーが盗まれた場合には、個人のプライバシーへの影響が甚大なものとなる可能性もあります。

同時に、より多くのデータのコントロール権限を求める消費者の要望は、パーソナルデータストアの開発と導入の動機付けとなるかもしれません。また、パーソナライズされたダッシュボードから得られる洞察に魅力を感じる人も多いでしょう。

データ自体もまた、企業にとって魅力的なものとなります。正確性の高い「ゼロパーティデータ」（個人が意図的に作成し、最新の状態を維持しているデータ）へのアクセスが可能となるからです。しかし、多数の消費者が利用しない限り、企業が既存のデータ収集プロセスを毀損してまでも導入するというメリットは、なかなか見出せないでしょう。

情報銀行

パーソナルデータストアが実現する個人データ集中管理の原理は、情報銀行にも見られます。The Open Data Instituteは、これを「独立したデータ信託を行う法的構造」と定義しており、個人が自身の個人データの管理を受託者に委ね、受託者はその個人に代わって、誰がその個人データにアクセスし、どのような目的で使用できるかを決定します[48]。

もし情報銀行から提供される個人データを使用している企業がプライバシーに関する要求事項を遵守していない場合、当該企業のデータへのアクセスは取り消される可能性があります。また、情報銀行は、相互運用性を維持する観点からもデータのメンテナンスを重視し、また、ユーザーである個人が自身のデータの使用状況について十分理解していることや、その使用に対する同意が行われていることについて確認を求めるでしょう。

情報銀行の開発はまだ始まったばかりで、いくつかの克服すべき課題も存在します。たとえば、開発に関する国際標準の必要性や関連法令の整備などもその1つです。しかし、ジョンズ・ホプキンス大学が医療研究のために情報銀行を開発した例などは、その大きな可能性を示唆しています[49]。欧州委員会の「A European Strategy for Data（欧州データ戦略）」が示すように、個人が自身の権利行使を容易にする手段として、今後情報銀行のさらなる調査研究が必要になるものと考えられます[50]。

プライバシー強化技術の開発と普及が広がることで、信託に対する不信を低減し、より多くの企業が参加できるように促す複合的なアプローチにより、情報銀行の成長をさらに後押しできるかもしれません。

権利行使のサービスプロバイダー

EU一般データ保護規則（GDPR）やその他世界各国のプライバシー規制において、データ主体の権利は明確に整理され、個人のためのいくつかの権利は法律上に組み込まれました。同時に、データ漏洩や罰金の公表数も増えたことで、消費者のデータプライバシーへの関心はますます高まっています。

そのため、データ主体としての権利をどのように行使するかについて、消費者も意識し始めています。これを受け、データライツアズアサービス（権利行使のサービスプロバイダー）の業界が生まれ、個人によるデータ主体としての権利行使を自動化したり、デジタルフットプリントを少なくしたり、検索エンジンやその他データ集積企業の保有する個人情報の削除を要求したり、eメールのIDをオンラインで隠したりすることが可能となってきています。

新たなテクノロジーが私たちの生活に浸透していくなかで、権利行使のサービスプロバイダーは、消費者が効率的かつ自動化された方法で権利行使できる機会を提供します。

プライバシー強化ブラウザ

ブラウザは、長期にわたりプライバシー権をめぐる争いの場となっており、多くのブラウザ関連サービスがプライバシー主唱者と対峙してきました。その間、消費者がプライバシー強化ブラウザを採用したことで、消費者もこの争いに参加していることがわかります。

適切な設定がなされていない場合、ほとんどのブラウザは通常、インターネットを閲覧する際に、閲覧履歴、ログイン認証情報、クッキーやトラッキングメカニズムによって収集されるデータ、オートフィルのための情報など膨大な量の個人データを収集します。また、設定を行うためには、一般的に消費者の能動的なアクションが必要となります。

このような個人データを、多数の第三者へ共有することが可能となるサードパーティのクッキーについては、いくつかの大手ブラウザメーカーがその仕組みを廃止または改善すると発表しています。しかし、オンラインでの消費者行動に関するデータを自身のデバイス上に保持し、ウェブサイトに埋め込まれたトラッカーからブロックするなど、大手ブラウザメーカーがいくつかの解決策を提案している一方、プライバシー強化ブラウザは対策に後れを取っています。

グローバルプライバシーコントロール

2009年に提案された「Do Not Track」の仕組みは、ユーザーがウェブサイトによるトラッキングを拒否するためのシグナルとして機能するよう意図されていました。しかし、広く普及しなかったため、個人がブラウザで「Do Not Track」機能を有効にしていても、そのシグナルが守られるという保証はありませんでした。そのため、W3C（World Wide Web Consortium）は2019年1月に「Do Not Track」のワーキンググループを解散しました[51]。

「Do Not Track」機能廃止の後を継ぐグローバルプライバシーコントロール（GPC）は、参加企業のウェブサイトにDo Not Sell（またはDo Not Share）のシグナルを送信するよう設計された新しいブラウザメカニズムです。GPCは、消費者が第三者であるデータブローカーとのデータ共有を望まない場合にシグナルを送ることも目的としています。今後ますます多くのIT企業がこの仕組みに参加すると考えられます[52]。

> “プライバシー管理にはテクノロジーの活用が必須です。テクノロジーは、データの分類やプライバシー影響評価（PIA）、権利対応といったシンプルな機能だけでなく、匿名化や暗号化、データ削除などのより高度な手段に至るまで、情報のライフサイクル全体を通して、プライバシーに関する義務や要件の管理を容易にします。
>
> デジタルの世界では、これまで以上にプライバシーが重要となっています。欧州データ戦略によると、近年はAIやアナリティクスにおけるビッグデータの利用に対する個人データ処理の保護や顧客信頼を高める対策は、通常慣習になっていると言われています。このプロセスにおいて、成熟したプライバシープロセスの導入を可能にするテクノロジーソリューションが役に立つでしょう。”

Javier Aznar Garcia
Privacy Lead
KPMGスペイン

企業のための プライバシー技術とは

エンタープライズテクノロジーが進化する必要性

消費者向けテクノロジーが急速に進化し、それに合わせて消費者プライバシー技術も発展するなかで、企業もプライバシー技術を取り巻く環境変化に対応していくことが重要です。

規制による技術革新の要因

データ保護指令95/46/ECと同様に、GDPRは世界的なプライバシー規制の基盤を作り、企業は自社のプライバシーコンプライアンス状況について再評価を迫られ、より高い基準へ移行することを余儀なくされました。

しかしこれは規制の変化の始まりにすぎず、中国、ブラジル、タイ、インドなど、多くの国々もGDPRに追随し、規制の制定に動いています。

プライバシー規制の強化はメリットをもたらす一方で、潜在的な規制変更の数が大きく増えると、企業はそれらの把握、理解、要求事項の充足のために重い負担を強いられることとなるでしょう。

つぎはぎだらけの規制によってもたらされるハードルは、プライバシー技術を用いて対処するしかありません。賢明な企業は、クロスチャネルのプライバシーコンプライアンス戦略とその実装のために、先進的なテクノロジーを活用するでしょう。この技術は、さまざまな種類のテクノロジーを統合プラットフォーム上に集約し、効率化された1つのプライバシー管理システムとすることができます。

負債としてのデータから価値創出へ

多くの組織では、適切に管理されていないデータは負債とみなしますが、プライバシー要件に適切に対処できれば、組織はプライバシー保護の義務を果たしつつ、データから価値を生み出すことができるのです。

消費者は、自身の個人データについてコントロール権を求めています。新しいプライバシー規制において、同意の管理は企業にとって課題となっていますが、これは、複数のチャネルにわたってパーソナライズされたユニークな顧客体験の機会を生み出すことにも関連するものです。マーケティングチームは、テクノロジーソリューションにより複数のシステムにかかわる単一の情報源を作成し、さまざまな収集ポイントでの同意を一元管理することができます。

顧客データの使用に関して透明性の高いアプローチを取ることは、信頼の醸成につながります。企業は、さまざまなチャネルから顧客の要望に関する情報を収集して同期し、オプトインやマーケティングの成果を向上させることもできるでしょう。また、マーケティングとセールスとの横断で顧客の要望情報を同期させ、既存のマーケティングテクノロジーにプライバシーを組み込むことにより、マーケティングコンプライアンスの自動化を図ることも可能です。

最終的に、プライバシー問題を擁護するのはプライバシー専門家だけではありません。企業も消費者を保護し、データ管理を通じて顧客のエンゲージメントや嗜好を優先順位付けし、顧客のプライバシージャーニーを統合してポジティブな体験を作り出すことが必要となります。

個人の識別可能性とデータの使いやすさのバランス

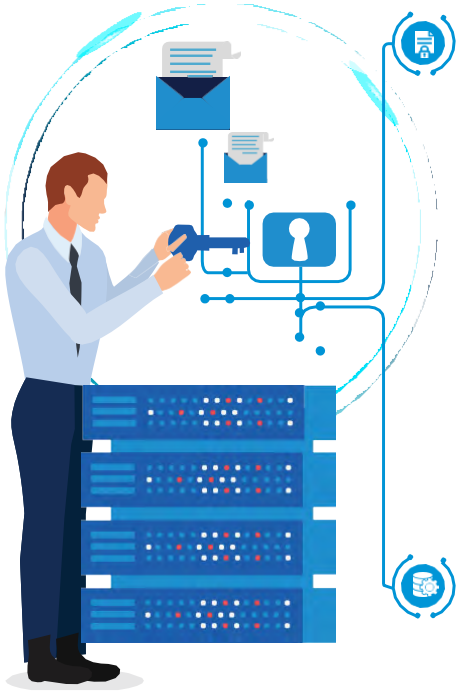
個人の識別可能性とデータの使いやすさのバランスをとることは、企業にとって長年の懸案でした。GDPRなどの規制では、データ保護の原則が匿名情報には適用されないとしていますが、企業は、匿名化により個人を再識別できる可能性が本当になくなっているかを確認しなければなりません。

> 市場における大きなトレンドは「信頼」の重要性です。信頼は今日、企業が競争し、互いに差異化を図るうえで重要な要素となっています。現代の組織、消費者、従業員は、自身の価値観に沿って買い物し、働き、かかわりを持ちたいと考えています。ブランドの信頼性は、今や製品やサービスと同等か、それ以上に重要になってきています。

Kabir Barday氏
CEO
OneTrust

単にデータセットから識別子を削除するだけでは十分ではありません。実際、いわゆる匿名化されたデータセットの公開後に再識別が行われてしまった例が広く知られており、規制当局（英国個人情報保護監督機関：ICOなど[53]）のガイダンスでも、この点に注意するよう指摘しています。

では、プライバシーを守りながら、個人情報を含む大規模なデータセットを共有する必要がある場合、企業はどのようにすればよいのでしょうか。有用なアプローチには以下が挙げられます。



差分プライバシー：

厳密には技術ではありませんが、これはデータを共有する際にプライバシーリスクを管理しようとするものです。データ分析の結果を見たときに、各個人データが元のデータセットに含まれていたものであるかどうか判断できないようにするというのが、この技術の中核にある考え方です。差分プライバシーは、データセットの中に“統計的ノイズ”層を加え、プライバシーを維持しながらも、各集団のパターンについて読み取れるようにします。また、プライバシーをリスクの累積という観点で定量化し、理解できるようにするものでもあり、「プライバシー予算」を設定して、それを超えるクエリーはそのデータセット内の個人の特定につながる、という考え方をします。

合成データ：

合成データの作成では、機械学習を用いて、個人データを含まない新たなデータセットを作成します。
新たなデータセットは（数学的および統計的な点で）個人データを含む元のデータセットとある程度の類似性を持つものとなります。合成データ作成の目的は、より広い範囲に共有できるデータセットを作ることです。

これらはデータ共有の際のプライバシーリスクを低減させますが、いずれも単独ではリスクを完全に排除することはできません。したがって、これらの手法を採用している企業においても、個人データ漏洩の可能性は継続的に評価すべきです。

AIなどを活用した次世代の自動化

AIは、プライバシー技術の未来において一定の役割を担います。実際、AIはすべてのオペレーションのベースでもあり、非倫理的なデータの取扱いを防ぐバリアともなります。

まず、AIはプライバシー保護の自動化を強化するために使用することができます。ベンダー管理から、クッキーや同意の監視、データの管理まで、AIはプライバシーコンプライアンスツール内で動作し、倫理的な境界線の中で人間のタスクをより迅速かつ正確に完了させます。また、より効果的なデータディスカバリーをサポートし、データの分類やリスクの特定に加え、特定されたコンテキストに基づいて適切な次のステップを提案するために使用することもできるでしょう。

しかし、AIを導入する際には、倫理的かつ安全な方法を確保しなければなりません。AIや機械学習システムは、既存のデータセットを分析することで動作しますが、たとえば、もし推論の元になったデータがより広範な集団の特性を正確に反映できていなければ、偏見や差別が助長されたり、増幅されたりする可能性も出てきます。また、開発者の中にある偏見が、アルゴリズムに反映されることもあり得ます。

次世代のプライバシーポータル

新しいテクノロジーがライフスタイルに影響を与え続けるなか、消費者は、企業もプライバシーに関する透明性を高めるためのツールを拡充させていくものと期待するでしょう。プライバシーダッシュボード、あるいはプライバシー設定の集中管理ツールは、個人がプライバシーに関するプリファレンスを一箇所で管理できるようにするものです。規制当局（ICOなど[54]）もダッシュボードを使用するメリットについて強調しており、データ収集が行われる各タッチポイントとリンクできるよう示唆しています。

消費者は、自身の個人データがどのように使用されているのかを理解したいときや、データ主体としての権利を行使したいときに何を期待するでしょうか。現在のツールやダッシュボードにおいても、個人は自身に関して収集されている個人データを理解し、何らかの形式で情報の更新や削除などのコントロールを行うことができるかもしれません。しかし、その多くは静的なもので読み取り専用の抽出データを提供するのみであり、リアルタイムベースで個人データを詳細に修正・削除できるものとはなっていません。

今後、パーソナルデータストアやデータプライバシー保管庫の利用が増えれば、消費者による個人データの管理は、組織ごとのアプローチから消費者が管理する保管庫へと一元化されるようになるかもしれません。次世代のプライバシーポータルでは、消費者が各企業で使用されている個人データのフィールドを正確に把握し、データが共有されることで目に見える形のダッシュボードが提供され、データ使用に対する強化されたコントロール手段が提供されるでしょう。

プライバシー拡張技術（PETs）

PETsは、プライバシー技術の将来に変化をもたらすもので、個人データの使用を最小限に抑えたり、データの安全性を最大限に高めたりするとともに、個人が自らプライバシー権を保護できるような仕組みなどを実現するでしょう。PETsの利点は、基礎となる個人データを保護しながらもデータ分析を可能にすることです。PETsの一般的な例は以下の通りです。

準同型暗号化（Homomorphic Encryption）：暗号化は、長らく個人情報を保護するための手段として利用されてきました。しかしながら、必要なデータにアクセスする際に、復号化されたデータについて安全に保存・処理しなければならず、リスクが発生します。準同型暗号化は、データの復号化を不要とするものであり、まるでプレーンテキストを扱っているように、暗号化されたままデータの計算処理などが可能になるという技術です。準同型暗号には、PHE（部分準同型暗号）、SHE（Somewhat準同型暗号）、FHE（完全準同型暗号）などの種類があり、それぞれ実行可能な計算範囲が異なります。

セキュアマルチパーティ計算（SMPC）：SMPCは、暗号のサブフィールドの1つで、異なる当事者が所有する複数の暗号化されたデータソースに対して、各当事者の保有する入力データの内容を明らかにすることなく、データの共同解析を実現しようとするものです。

しかしながら、PETsはまだ誕生間もない分野で、コストや導入の複雑さなどの障壁があり、その状況は日々変化しています。

データアクセス制御

企業は、取り扱うセンシティブなデータの急増に伴い、急速に進化する倫理的・法的なプライバシー保護義務への対応を求められるなど、増え続ける課題に直面しています。単にウェブサイトへアクセスするだけでeメールアドレスや位置情報などの個人データが生成され、消費者の理解や同意のないままにデータ収集や保存が行われるということも頻繁に起きています。

ここ15年ほどの間、ロールベースアクセス制御（RBAC）が、個人データへのアクセスを管理するための好まれる手法でした。これは、個人ごとにアクセス権を設定する手法に代わって、組織内でのユーザーの役割に基づいてアクセス権限を管理するというものです。この手法では、どのユーザーがどの役割に割り当てられていて、各役割の職務遂行にどのようなアクセス権限が必要とされるかというパラメータを、管理者が暗黙的に事前決定しておく必要があるため、静的なアクセス制御と言われることもあります。しかし、データアクセス制御に求められる要件はますます複雑化しており、特に規制の厳しい業界やグローバルな組織においては、ユーザーの役割といった単一の属性だけで制御することは難しくなってきています。

このような状況を踏まえ、多面的で動的なアクセス制御モデルが提案されており、それらはプライバシー保護を重要な要素として含んだものとなっています。これらのデータアクセス制御モデルでは、どのようなアクセス権限を付与するかという点において、使用目的の概念が重要となり、指定されたデータ要素へのアクセスの目的に沿って、意図された個人データ利用を特定します。

さらに、これは利用目的に係るコンプライアンス確認や明示的なアクセス禁止をサポートすることができます。管理者は、個人データへアクセスする目的がデータの使用目的に合致しているかを確認し、合致しない場合はデータ使用を禁止することができます。たとえば、病院の受付担当者は患者の名前と連絡先しか見ることができませんが、医師や看護師は完全な患者の記録にアクセスすることができます。この例では、放射線技師は、完了したX線撮影結果と関連記録へアクセスできる一方で、その役割の範囲外にある患者の特定医療記録にはアクセスできないようにするのが適切かもしれません。

これらはすべて、企業が設定した方針やコンプライアンスルールセットとメタデータに基づいて、リアルタイムで実行させることが可能です。また、管理者は、システムやデータストアごとに個別の役割を設定する必要がありません。この動的で多面的なアプローチにより、ロールベースアクセス制御と比べ、より効果的にリアルタイムでの変更に対処でき、課題を軽減することが可能となります。

では、データ倫理の問題は？

顧客体験や洞察力を高めるために、高度化する技術を次々に導入し続けることは、際限のないデータ収集を必要とすることにつながるでしょう。その結果、個人データの倫理的な収集、処理、管理に関する違反が発生する可能性が高まります。

技術の進歩に規制が常に追いついているわけではないため、企業は、すべてのデータ主体にとって公正で信頼できる結果を維持するためのデータ倫理フレームワークを組み込む必要があります。データ倫理フレームワークは、自動化された意思決定をデータ主体の権利に配慮したものとし、データ主体に対して説明できる公正な意思決定をサポートし、イノベーションが安全で信頼できる方法により行われることを保証することで、企業が消費者と従業員の信頼を維持するのに役立ちます。

プライバシー技術の将来においては、倫理が特に重要な意味を持つこととなるでしょう。「プライバシーバイデザイン」の適切な計画を組み込み、社会的影響を広く考慮する倫理的原則に従うことが求められるはずです。この点を正しく理解できていないと、破壊的テクノロジーがもたらす機会を活かしながらも効果的なデータ管理の仕組みを実現することは困難となります。

> 企業は、顧客からの信頼を獲得し、プライバシーに関するルールや法規制を遵守するために常に努力しています。信頼され、安全で、法規制を遵守した製品やサービスを提供するという点において、継続的にコンプライアンスを実証していくために、俊敏性、機動性を備え、ユーザーフレンドリーでプライバシー関連要求に効果的に対応できるプライバシー技術を活用することが重要です。

Tom Hyland
Privacy Lead
KPMGアイルランド

今後の展望

プライバシー技術のソリューションを選択するうえでの重要な検討事項

「今」を評価し、要件を特定する

プライバシー技術のソリューションを真剣に検討する前に、そのソリューションが対応しなければならない具体的なニーズを把握しておく必要があります。そして、プライバシー、コンプライアンス、法務の各チームと組織の義務について話し合い、現在自社がどのように多様なニーズに応えているのかを評価します。自動化できる手動プロセスを検討し、現在および将来的にソリューションが提供すべき事項を明確にします。

また、技術仕様も考慮してください。プロセスの早い段階で技術スタッフを参加させることで、どのソリューションが実行可能なオプションであるかをより理解することができます。この意見は、ほかの部門やチームがプライバシー技術のソリューションに何を望むかを示すことにもなり、それらを統合して組織全体での活用を促進することにもつなげられます。

プライバシー技術のソリューションで求められるもの

企業におけるデータの将来は、プライバシー技術にも依存するようになるため、ソリューションを選択する際には、慎重かつ入念な検討を行わなければなりません。プライバシー技術のベンダーによる営業（場合によっては誇張された宣伝）は、企業がプライバシーに関するベストプラクティスの競争優位性を認識するにつれて、増加していくでしょう。

ほかの新しいソリューションと同様に、プライバシー、セキュリティ、ベストプラクティスの要件を完全に満たすことのできる必須機能と技術仕様を理解してください。そして何よりも、そのソリューションは、テクノロジーや規制の環境変化のなかで組織とともに成長できるものでなければなりません。ソリューションに求められる特性としては、使いやすさ、利用可能な製品やサービスの組み合わせ、長期的な持続可能性などが挙げられます。

使いやすさ

ますます多くの組織が社内にプライバシーチームを設置するようになっているため、プライバシー技術のソリューションは、既存のプライバシーやコンプライアンスのプロセス上で容易に構築できるようになっています。ソリューションの導入や日常的な使用が困難であるほど、その有用性は低くなります。ソフトウェアの実装にフォーカスするのではなく、コンプライアンスの実現に重点を置きましょう。

> “プライバシー技術は、個人が自身のプライバシーを強化できるようにする技術にほかなりません。これらのソリューションを提供することは、データドリブン型組織モデルの基本です。企業は、信用と信頼を取り戻す必要があり、関連規制における透明性の要件とは、データドリブン型のサービスの付加価値を示すことと同じであると解釈します。
>
> カスタマージャーニーに明確な焦点を当て、個人データの処理をレビューすべきです。その対象には、データを収集するすべてのインタフェースや“センサー”およびデータに基づいて提供される付加価値を含みます。もし個人データが組織モデルの一部となっている場合は、その個人を自社の長期的パートナーとして捉えましょう。
>
> 今こそ、プライバシー管理をデジタル化し、顧客とその他のステークホルダーを含むユーザーの視点に立った柔軟なものとする時です。”

Michael Falk
Privacy Lead
KPMGドイツ

> “日本では、個人所有のデバイスから得られるIoTデータの市場取引やマネタイズが、さまざまな組織コミュニティで重要な関心事となっています。私たちは、プライバシー技術がこのリスクを管理する鍵になると考えています。”

大洞 健治郎
Privacy Lead
KPMGジャパン

ソリューションは、たとえば、手動でのユーザー割当タスクを自動化されたAPIワークフローに統合するというように、既存のビジネスワークフローをソリューションのワークフローに統合するといったシンプルなものであるべきです。

どのようなソリューションであっても、求めるメリットを享受するためには、膨大な量のアーキテクチャー、プロセスの再設計および設定調整が必要になります。これは、テクノロジーソリューションの購入に係るコストの何倍にもなることがあります。

利用可能な製品とサービスの組み合わせ

もう1つの考慮すべき点は、ソリューションのサービスと製品の組み合わせについてです。まず、1つのプラットフォーム上ですべてのニーズをカバーできるかどうかを判断します。カバーできる場合は、1つのプラットフォーム上でチーム間のコラボレーションが可能になり、プライバシー管理がシンプルになります。これが常に更新されるサービスと製品の組み合わせで実現できると、組織も成長できるでしょう。

プライバシー技術は、なるべく細かくモジュール化されていると望ましく、特に小規模な組織が最重要な機能を提供するために有用となります。プライバシーに関する規制の中には、規模に応じた基準値が設けられているものもあります。モジュール式のプライバシー技術のソリューションを使用すれば、必要に応じて新しいモジュールを追加することができます。モジュール性と変化する規制に対応するサービスの組み合わせは、非常に重要なものとなります。

長期的な持続可能性

最後に、プライバシー技術のソリューションに長期的な持続可能性があるかどうかを確認したうえで、組織再編、合併／買収、企業の成長、テクノロジー環境の変化、プライバシー規制の変更などの一般的なシナリオに対応できるものを選択します。これにより企業は、プライバシーに関する義務を果たしながら、顧客のニーズにも応えることが可能となり、常に時代の先を行くことができるでしょう。

> 自社に合ったソフトウェアソリューションを選ぶのは難しいことです。特に、多くの場合、この選択はあなただけに関連するというわけではないからです。これらのソフトウェアの使用は、あなたの業務の延長線上にあるため、そのソフトウェアが業務にうまく重なり合っているかについて、十分確認するようにしてください。

Andrew Clearwater氏
CPO
OneTrust

> プライバシー技術はもはや、何を構築して、それをどのように現行業務へ組み込むかという、後追いの検討ではなくなりました。プライバシーは、企業の重要なインフラの一部となりつつあるため、間違った企業や技術スタックへの投資、あるいはビジネスにプライバシーを組み込まずに後でそれを考えようという選択は、取り返しのつかないものとなるでしょう。

Blake Brannon氏
CTO
OneTrust

KPMGによる支援

KPMGは、サイバーセキュリティの専門家で構成されるグローバルな組織が、リスクを多面的に捉えながら、企業のプライバシーに関する課題解決をサポートしています。精度、品質、客観性に対する揺るぎないコミットメントに基づき、私たちは企業のすべての事業活動に防御と信頼を組み込み、技術面の対策だけでなく、セキュリティ文化を構築することについても支援します。

企業がプライバシーとサイバーセキュリティの分野でどのような状況に置かれているかにかかわらず、役員室からデータセンターに至るまで、切れ目のない横断的な専門的知見を提供します。プライバシーに関する方針を評価し、ビジネス上の優先事項に合わせて調整を行うだけでなく、先進的なソリューションの開発や実装、進行中のリスクの監視、インシデントへの効果的な対応も支援します。組織全体にプライバシーのコンプライアンスを浸透させ、将来を見通しながら迅速に行動し、安全で信頼性の高いテクノロジーを取り込むことで、企業の優位性獲得に役立ちます。

KPMGは、深い技術的専門知識、強力なビジネス洞察力、規制対応に詳しいクリエイティブな専門家を組み合わせることで、企業が顧客、従業員、ベンダーの期待に応えながら、個人情報を活用して価値を創造し、収益を増加させることをサポートします。

ともに信頼できるデジタルの世界を作り、可能性の限界に挑戦していきましょう。

OneTrust

OneTrustは、2020年のInc.500で最も急速に成長している企業に選定され、オペレーションに信頼を組み込むというエンタープライズプラットフォームのカテゴリーを定義しています。OneTrustは9,000社以上の顧客（Fortune 500企業の半数を含む）に利用されており、信頼を競争上の差別化要因とするとともに、プライバシー、セキュリティ、データガバナンス、GRC、サードパーティリスク、倫理とコンプライアンス、ESGプログラム全体にわたる、一元的で柔軟なワークフローの実装をサポートしています。

OneTrustのプラットフォームは150の特許に支えられ、AIとロボットによる自動化エンジンOneTrust Athena™を搭載しています。OneTrustが提供する製品には、以下が挙げられます。

- OneTrust Privacy Management Software
- OneTrust DataDiscovery™　AIによるデータ検出と自動分類
- OneTrust Data Governance™　データインテリジェンスソフトウェア
- OneTrust Vendorpedia™　サードパーティリスクに関する情報交換
- OneTrust GRC　統合リスク管理
- OneTrust Ethics　倫理・コンプライアンスソフトウェア
- OneTrust PreferenceChoice™　同意およびプリファレンス管理
- OneTrust ESG　環境・社会・ガバナンスソフトウェア
- OneTrust DataGuidance™　規制調査

IDC Worldwide Data Privacy Management Software Market Shares Report, 2020によると、「OneTrustは市場を完全にリードしており、減速や停止の兆候は見られない」と評されています。

また、OneTrustは、Insight Partners, Coatue, TCV, SoftBank Vision Fund 2, Franklin Templetonから53億米ドルの評価額で合計9億2千万米ドルの資金を調達しています。

急成長を続けるOneTrustのチームは従業員2,000人を擁しており、アトランタとロンドンに本社を置くとともに、その他のオフィスをベンガルール、メルボルン、デンバー、シアトル、サンフランシスコ、ニューヨーク、サンパウロ、ミュンヘン、パリ、香港（SAR）、バンコクにも構えています。

詳細については、OneTrust.comをご覧いただくか、LinkedIn, Twitter, YouTubeへアクセスしてください。

参照

1 KPMG's Me my life my wallet, 2021.

2 KPMG's The New Imperative for Corporate Data Responsibility, 2020.

3 OneTrust Data Guidance, 2021, https://platform.dataguidance.com/

4 Justices of the Peace Act, 1361 (Eng.), 34 Edw. 3, c. 1.

5 Second Congress. Sess. 1, Chapter 7, 1792.

6 Félix v. O'Connell, Trib. Civ de la Seine, 16 juin 1858.

7 Mia Fineman, "Kodak and the Rise of Amateur Photography," metmuseum.org, October 2004.

8 The Right to Privacy, Samuel D. Warren; Louis D. Brandeis, Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220.

9 K.M Turner & W.F.H. Germer, Telephone Dictating Machine or Apparatus, Patent No. 843,186, Patented Feb, 5, 1907.

10 Olmstead v. United States, 277 U.S. 438, 1928.

11 United Nations Declaration of Human Rights (UDHR), Article 12, 1948.

12 "Netscape 1.0 Released," thisdayintechhistory.com, 2015.

13 The History of the General Data Protection Regulation, European Data Protection Supervisor.

14 SixDegrees.com, wikipedia.org, 2021.

15 Polly Sprenger, "Sun on Privacy: 'Get Over It'," Wired.com, January 26,1999.

16 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council, August 25, 2000.

17 Adam Pothitos, "The History of the Smartphone," Mobile Industry Review, October 31, 2016.

18 The App Store turns 10, Apple Newsroom, July 5, 2018.

19 Sarah Perez, "The 3 Facebook Settings Every User Should Check Now," The New York Times, January 20, 2010.

20 Bobbie Johnson, "Privacy no longer a social norm, says Facebook founder," The Gaurdian, January 11, 2010.

21 Charles Arthur, "iPhone keeps record of everywhere you go," The Guardian, April 20, 2011.

22 Emil Protalinski, "70% don't trust Facebook with their personal information," ZDNet.com, May 9, 2012.

23 "Girls Around Me app 'like looking in the window': developer," securitybrief.co.nz, April 2, 2012.

24 Steve Lohr, "The Age of Big Data," The New York Times, Feb. 11, 2012.

25 Becky Branford, "Snowden affair puts Wikileaks back into spotlight," BBC News, June 28, 2013.

26 Joe Svetlik, "2014: Wearable tech review of the year," Wearable.com, December 22, 2014.

27 James Connington, "It's time to make sure research is understandable to all," The Telegraph, July 27, 2015.

28 Samuel Gibbs, "What is 'safe harbour' and why did the EUCJ just declare it invalid?" The Guardian, October 6, 2015.

29 “Internet of Things Will Deliver $1.9 Trillion Boost To Supply Chain And Logistics Operations,” Cisco Newsroom, April 15, 2015.
30 Natasha Singer, “When Websites Won’t Take No for an Answer,” The New York Times, May 14, 2016.
31 “Data protection in the EU,” ec.europa.eu, 2021.
32 GDPR Enforcement Tracker, enforcementtracker.com, 2021.
33 “Provvedimento correttivo e sanzionatorio nei confronti di Eni Gas e luce S.p.A.,” gpdp.it, December 11, 2019.
34 Court of Justice of the European Union, Press Release No 91/20, July 16, 2020.
35 “Confidentiality of electronic communications: Council agrees its position on ePrivacy rules,” Press release: European Council of the European Union, February 10, 2021.
36 Sarah Rippy, “Virginia passes the Consumer Data Protection Act,” iapp.org, 2021.
37 LfD Niedersachsen verhängt Bußgeld über 10,4 Millionen Euro gegen notebooksbilliger.de, lfd.niedersachsen.de, January 8, 2021.
38 “Resolución De Procedimiento Sancionador,” Procedimiento Nº: PS/00477/2019, www.aepd.es.
39 KPMG’s Six Pillars, https://home.kpmg/xx/en/home/insights/2020/01/six-pillars.html.
40 Knud Lasse Lueth, “State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time,” iot-analytics.com, November 19, 2020.
41 KPMG’s COVID-19 and the future of digital assistants, kpmg.us, 2020.
42 Charity: Water, The Source, 2015, https://www.with.in/watch/the-source/
43 J. Volpe, “The 21st-century charity that puts Google and VR to good use,” engadget.com, March 3, 2016.
44 Queenie Wong, “Why WhatsApp users are pushing family members to Signal,” cnet.com, Feb. 5, 2021.
45 KPMG’s Me my life my wallet, 2021.
46 Press release : Medtronic and Fitbit Partner to Integrate Health and Activity Data Into New CGM Solution for Simplified Type 2 Diabetes Management, Medtronic Newsroom, December 7, 2016.
47 Jessica Davis, “Consumer Adoption of Health Tech Slowed by Privacy, Security Concerns,” healthitsecurity.com, January 7, 2020.
48 Jack Hardinges, “Data trusts in 2020,” theodi.org, March 17, 2020.
49 Data Trust, ictr.johnshopkins.edu, 2021.
50 A European strategy for data, ec.europa.eu, February 2020.
51 WG closed, github.com, January 2019.
52 GPC Privacy Browser Signal Now Used by Millions and Honored By Major Publishers, Global Privacy Control, January 28, 2021.
53 What is personal data? ico.org.uk, 2021.
54 How can dashboards help? ico.org.uk, 2021.

謝辞

本レポートの企画、分析、執筆、作成にあたり、知識と知見を惜しみなく提供してくださった方々に心より感謝申し上げます。

お問合せ先

KPMGコンサルティング株式会社
T : 03-3548-5111
E : kc@jp.kpmg.com

home.kpmg/jp/kc

本レポートで紹介するサービスは、公認会計士法、独立性規則および利益相反等の観点から、提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。
詳しくはKPMGコンサルティング株式会社までお問い合わせください。

home.kpmg/jp/socialmedia

本冊子は、KPMGインターナショナルが2021年5月に発行した「Privacy technology: What's next? - The evolution of data-privacy technology in the age of automation」を、KPMGインターナショナルの許可を得て翻訳したものです。翻訳と英語原文間に齟齬がある場合は、当該英語原文が優先するものとします。

Publication number: 137417-G | Publication date: May 2021