KPMG

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

目次

まえがき

企業はかつてないほど自社の顧客について把握しています。おそらくあなたの会社は、この24時間に顧客がどの食料品店で買い物をするか、休日はどこに出かけるか、昨夜どの店で食事をしたか、今朝はどうやって仕事に行ったかなど、10年前や20年前には考えられなかったほど多くの顧客情報を収集しているでしょう。

我々は消費者として、こうした生活とITとの密接さから恩恵を受けています。健康アプリで歩数を数えたり、メッセージアプリでビーチから写真を送信したりすることができます。また車に搭載されたテレマティックス（移動体と携帯電話などの通信システムを複合して提供されるサービス）技術は、自動車保険料の引き下げに役立っています。

コンピューター上であれ、スマートフォン上であれ、コネクテッド・カー（インターネットとの接続によりサービスを受ける機能を有した自動車）であれ、こうしたテクノロジーを利用する際は、往々にして「生活をより便利に、より豊かに、そして時にはより低コストに変えるサービスまたは製品と引き換えに個人情報を提供する」ことが前提となっています。

こうしたトレードオフの関係はデータ社会の根幹を成していますが、それにも限界があります。人々は企業が自分の情報を収集、利用、保持、開示し、あるいは、売買さえしていることについて、ますます意識するようになってきており、「身近で役立つ」存在が境界線を越え、「不快でプライバシーを侵害する」存在にいつ変わるのか？という不安を募らせています。

KPMGは、世界24ヵ国の約7,000人を対象に質問を行い、個人データの使用の際に、人々が快適または不快と考える境界線がどこにあるのかについて調査しました。

本レポートは、企業にとって、この「境界線」を踏んでしまったり、踏み超えたりしないための手引きとなるでしょう。

当然ながら、どこにその「境界線」があるかについては、個人によって大きく異なります。ある人にとって「許容できない」ものが、別の人にとっては「容認できる」という場合もあります。性別、年齢、資産状況、国籍、教育水準は、いずれも状況を変える要因となり得ます。しかもそれは思いもよらない方向に変わることが多いのです。

たとえば、回答者の半数以上は、性別、教育水準または民族をインターネット上で公開されることには抵抗がないものの、自分の所得、現在地、病歴、住所を公開されることに抵抗がないとの回答は、20%を下回りました。

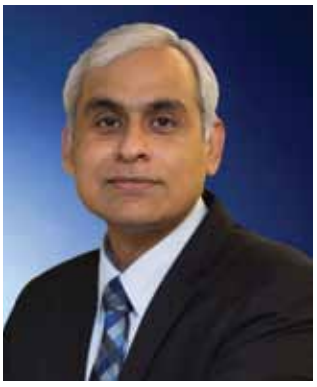
インドやマレーシアといったアジア諸国は、スカンジナビア諸国よりもパーソナライズド広告という考えを受け入れているようです。またインドの消費者と比べ、日本の消費者は個人データを扱う企業への信頼度がはるかに低い反面、個人データを守るために防衛策を実施する確率は最も低いという結果が出ています。

このビッグデータ時代にあって、何が私的で何が公的なのかというモラルや法律上の問題について、社会の取組みはまだ始まったばかりです。これは、企業が無視しても構わない哲学的な論争などではありません。規則に違反したり、消費者の態度を読み違えたりすれば、EUや米国といった主要市場では多額の罰金を科されるおそれがあることに加え、消費者からの信頼を失ったり、プライバシーを侵害されたと感じた消費者が大挙して離れてしまう可能性もあります。株価や収益、そして一部の企業にとっては事業の存続さえもが、プライバシー問題に対して、より知的で洗練されたアプローチを取れるかどうかによって左右されるでしょう。

モラルや法律という観点から見て、自社が顧客情報を適切に扱っているかを自問する企業はごくわずかです。今こそ自問すべき時が来ています。

Mark Thompson
Global Privacy Lead
KPMG International

Greg Bell
Global Cyber Security Co-leader
KPMG International



Akhilesh Tuteja
Global Cyber Security Co-leader
KPMG International

消費者はどこに境界線を引くのか?

「容認できる」が「許容できない」に変わるのはどのような時でしょうか?「便利だ」という評価が「プライバシーの侵害だ」という評価に変わるのはいつなのでしょうか? 消費者と企業の間の信頼関係を構築・維持するためには、消費者が個人データを利用されることに、どの程度敏感であるかについて理解することが極めて重要です。

調査結果に基づく考察：

半数以上の回答者が、性別、教育水準および民族に関する個人データをインターネットで公開することに抵抗はないと答えました。

<20%

インターネットの検索履歴、所得、現在地、住所、病歴に関する情報を開示することに抵抗がないと答えた人は、全体の**20%未満**でした。

55%

55%の回答者が、プライバシーに関する懸念を理由にインターネットでは買い物をしないことを決めたと答えました。

ほとんどの国の回答者が、**プライバシーに関する管理策を実施すること**は利便性よりも重要だと答えました。

ソーシャルメディア、ゲームおよびエンターテインメント業界の企業は、必要以上に多くの個人データを求める傾向にあります。

本調査では、1箇所を除く他のすべての市場で、回答者の**75%**以上がオンラインショッピングのデータを第三者に売られることは不快だと答えました。

>2/3

3分の2以上の回答者は、個人データを利用するスマートフォンアプリやタブレット用アプリは不快に感じています。

回答者の半数は、既にインターネットブラウザのクッキーを削除したり、ソーシャルメディアのプライバシー設定を管理しています。

約**3分の1**の回答者は、ウェブ閲覧の際にシークレットモードまたは「追跡を許可しない」モードを利用しています。

個人データを保護するために暗号化機能を利用していると答えた回答者は、**25%**でした。

50%

無料または割引価格で製品を手に入れられるなら、プライバシー保護のレベルが低くてもよいと答えた回答者は、約**半分**だけでした。

回答者の所得は、プライバシー保護のレベルの低さを受け入れるか否かについて、**大きな影響を及ぼしていない**と考えられます。

回答者の教育水準は、プライバシーに対する考え方や何を不快または受け入れ可能と考えるかについて**影響を及ぼさない**ことがわかりました。

出所：Crossing the line: Staying on the right side of consumer privacy, KPMG International, 2016

大量データの収集によって顧客が離れていく危険性

多くの企業は、消費者が許容するプライバシーの境界線が、生活の領域によって異なることをまだ認識していません。多くの場合、消費者はいつ、どこで企業と関わるかに応じて、その関わり方を区別しています。企業が、消費者が快適と感じる境界線を踏み越えてしまい、生活のよりプライベートな領域に侵入した場合、消費者は苛立ち、最終的にはその企業ブランドに背を向けるおそれがあります。

プライバシーに敏感であることは明白

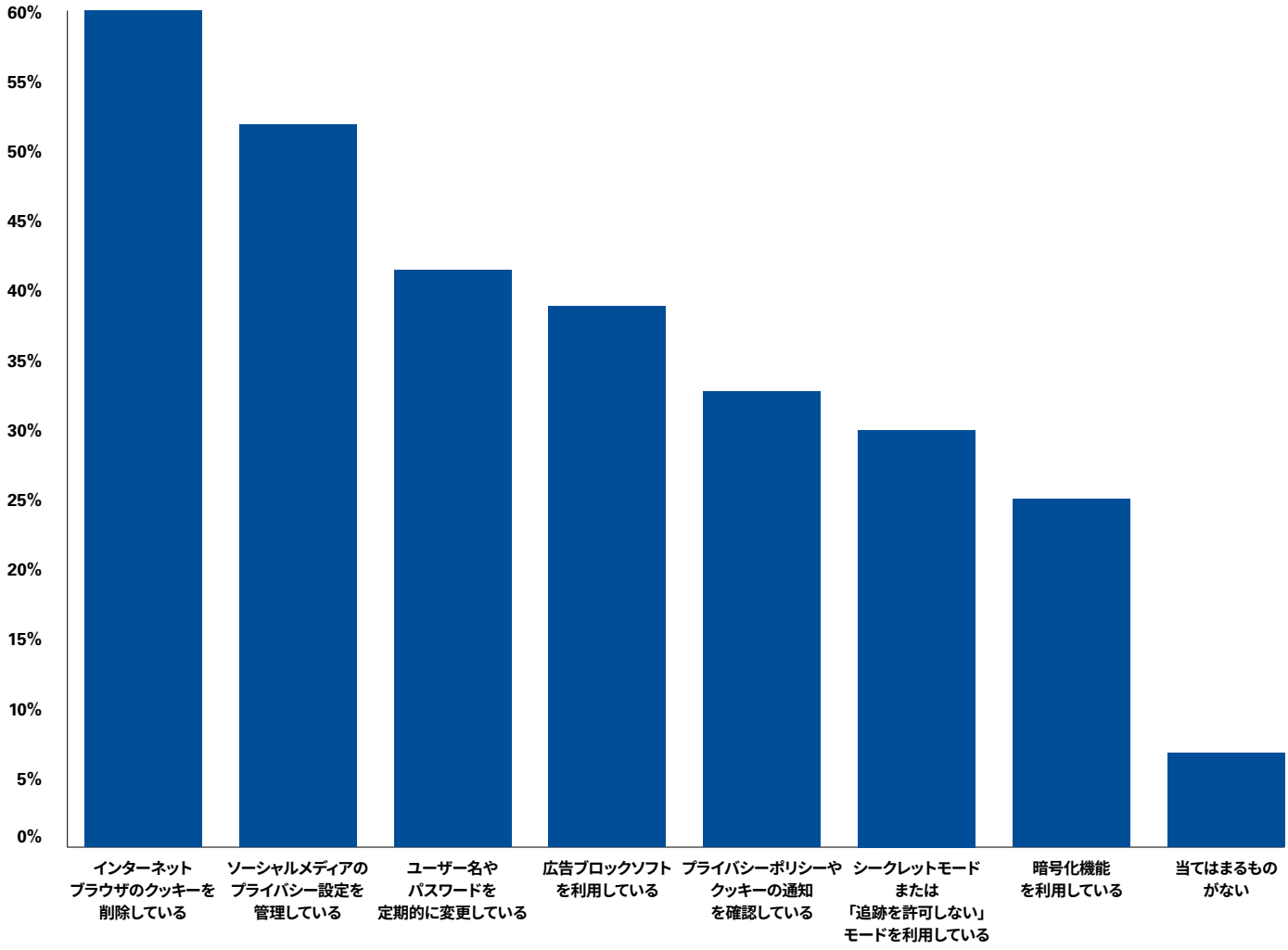
企業は四六時中、消費者から個人データを収集しようとしていますが、消費者はそれを不快に感じています。根本的に、消費者が期待するプライバシーに関する境界線は、自宅、職場、公共の場所でそれぞれ異なり、自分のプライバシーに対するコントロールを第三者の手に明け渡すことには消極的です。

さらに世界中の消費者のうち、企業が個人データの取扱いや利用方法について、完全にコントロールできていると考えている回答者はわずか10%でした。スペインでは55%の回答者がまったくコントロールできていないと答え、個人データのコントロールに対する懸念が一番少なかったマレーシアでさえ、企業による個人データの取扱いや利用方法を十分または完全にコントロールできていると答えた回答者は31%に留まりました。

したがって、無差別的な個人データの収集は、消費者を遠ざけてしまう危険性があります。また、消費者が不快だと感じれば感じるほど、インターネット上で個人データを保護するための行動を取る可能性も高くなります。世界的に見て、調査回答者の半数が既にインターネットブラウザのクッキーを削除したり、ソーシャルメディアのプライバシー設定を管理したりしています。またほぼ3分の1（30%）の回答者はシークレットモードまたは「追跡を許可しない」モードを利用し、25%の回答者は暗号化を利用しています（図1参照）。

「約20%の回答者が、企業による個人データの取扱いや利用方法について、非常に懸念を抱いています」

図1：消費者が個人データを保護するために普段用いている防衛策



出所：Crossing the line: Staying on the right side of consumer privacy, KPMG International, 2016

公的な領域と私的な領域

消費者は自身の家庭生活に関する情報を提供することに関して、本能的に慎重になっています。たとえば米国の複数のエネルギー関連・水道関連企業が、スマートメーターを居住用ビルに取り付けようとした際に、住人からの抵抗に遭っています[1]。本調査によって、43%の回答者が、公益企業が取得した情報を利用して、住人の数や特定の時間帯における住人の行動を推測することが可能になるのであれば、スマートメーターを自宅に取り付けることは不安だと感じていることが明らかになりました。

1. http://bv.com/docs/articles/the-opt-out-challenge.pdf

消費者は誰を信用しているのか?

最も信頼している

41% 銀行

39% 医療機関

36% 司法当局

33% 地方自治体

23% 公益企業

最も信頼していない

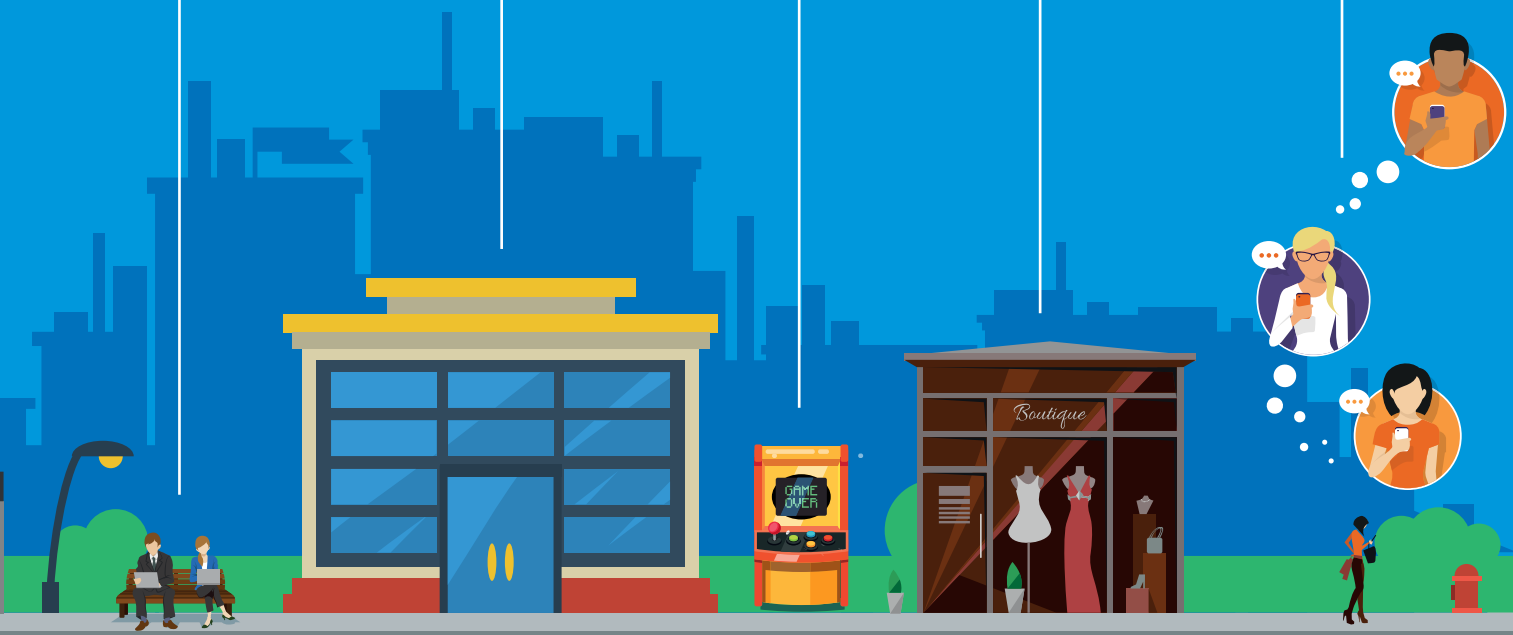
21%
テクノロジー企業

17%
スーパーマーケット

14%
ゲーム企業

14%
小売企業

13%
ソーシャルメディア



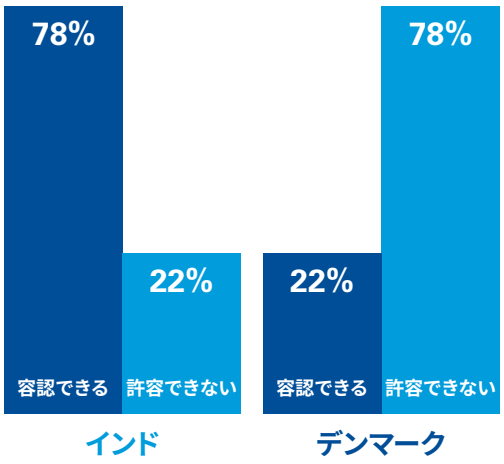
出所：Crossing the line: Staying on the right side of consumer privacy, KPMG International, 2016

本調査から浮かび上がる最も重要な教訓は、プライバシーに対する考え方は、対象となるデータや利用方法だけではなく、消費者の考え方や場所によっても異なるということです。たとえばパーソナライズド広告を「許容できない」と感じる回答者は78%であったのに対し、テレビを割引価格で手に入れられるのであれば、テレビ視聴をモニタリングされても構わないと答えた回答者は46%にのぼりました。また別の例を挙げれば、政府機関がテロと戦うために個人データを収集するのは構わないと答えた回答者は49%だったのに対し、インターネット小売業者が個人データを第三者に売っても構わないと答えた回答者は18%でした。

同様に、プライバシーに対する考え方には地域によって大きな違いが見られました。インドでは回答者の78%が、タクシー会社が地理位置情報を利用して顧客にサービスを提供することを「容認できる」と答えていたのに対し、デンマークではその割合はわずか22%でした（図2参照）。また、中国では60%の人がパーソナライズド広告を容認できると考えていたのに対し、日本では88%が許容できないと回答しました（図3参照）。

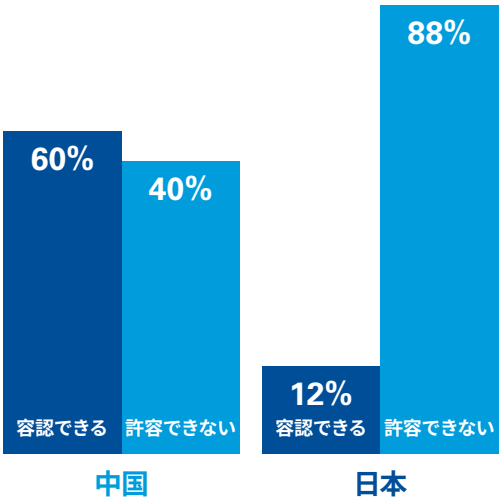
これらの結果は、個人データに関して経済の二重化が生じる可能性があることを示しています。個人データを提供することに異論のない（または選択の余地がない）消費者がいる一方で、より用心深い消費者は、個人データを守るために何らかの対策をしたり、出費をしたりする可能性があります。これは広告会社にとっても、企業にとっても好ましくない傾向です。企業が製品の開発とマーケティングを効果的に行うときに、顧客に関する個人データに依存して実施していることがその理由です。そのため、消費者が引き続き個人データを自由に提供してくれるようにするためには、企業が消費者の個人データについて適切な利用方法を学ぶことがますます重要となってきます。

図2：タクシー会社が地理位置情報を利用することをどう思いますか



出所：Crossing the line: Staying on the right side of consumer privacy, KPMG International, 2016

図3：パーソナライズド広告をどう思いますか



出所：Crossing the line: Staying on the right side of consumer privacy, KPMG International, 2016

エグゼクティブのための考察：信頼に対するリスク

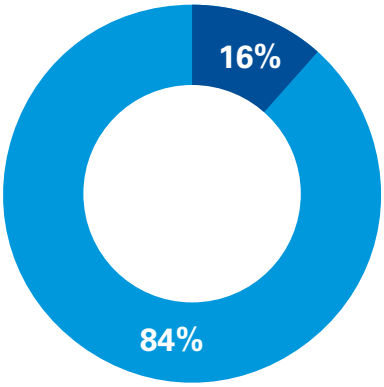
Mark Thompson
Global Privacy Lead
KPMG International

「企業が消費者の信頼を維持したいのであれば、消費者がよりセンシティブに考える領域の個人データを収集する際には、今までよりもかなり慎重に行動する必要があります。一部の人はサービスと引き換えに個人データを提供することについて、今でも妥当な対価と考えているかもしれませんが、個人データを守ることに一層の努力をする人もいるでしょう。

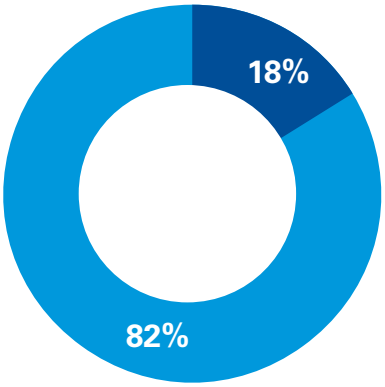
企業が個人データを収集することについて説得力のある理由を提示しない限りは、消費者は（可能であれば）次第に個人データを出し惜しみするようになるでしょう。その場合、個人データの処理において、プライバシーの意識に格差が生じる可能性があります。自分のプライバシーを気にする人々は、プライバシーを保護するためのさまざまな方法に投資することで、プライバシーを守ろうとするでしょう。事実、今回の調査が示すように、多くの人々は既にインターネット上でのプライバシーを守るために一歩進んだ対策を講じています。」

現状を把握する

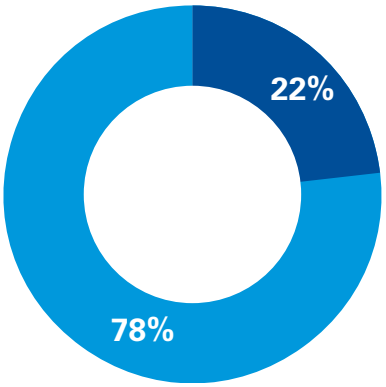
消費者が何を「容認できる」または「許容できない」と考えるかを理解する



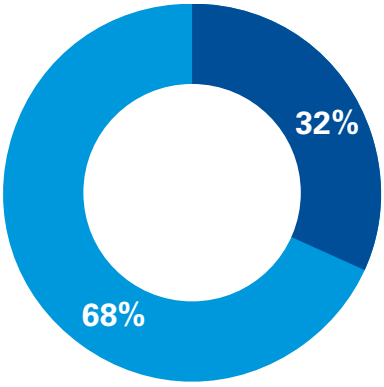
連絡先や写真、ウェブ閲覧履歴にアクセスできる、スマートフォンやタブレット用のナビゲーション、チャット、ニュースアプリ



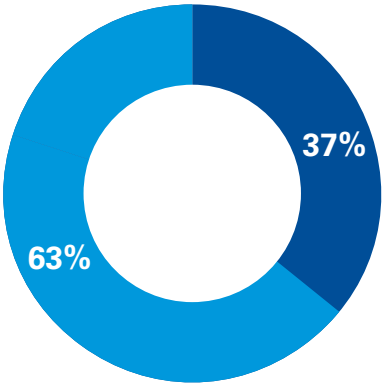
価格の割引や対応の迅速性、利便性、豊富な品揃え、商品の配達といったサービスを提供する一方で、第三者に顧客データを販売するインターネット小売業者



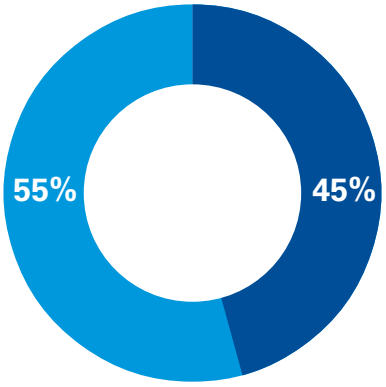
名前で呼びかけたり、朝食は美味しかったかと尋ねたり、お気に入りのシリアルの宣伝をするパーソナライズド広告



パリを訪れる計画を友人にメールしたところ、翌日パリのホテルやレストラン、周辺への小旅行のインターネット広告が表示されること



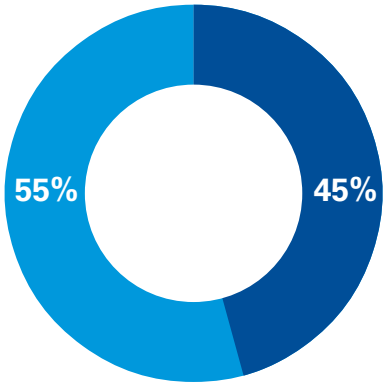
電車から降りた瞬間に自動的にサービスを提供できるようにするために、消費者の地理位置情報を購入しているタクシー会社



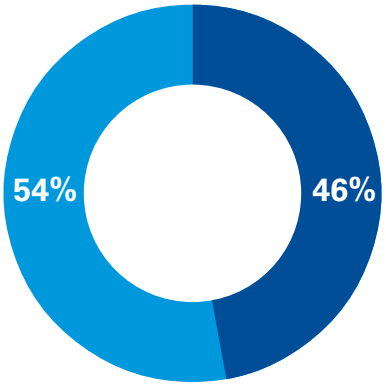
健康状態をモニタリングし、あなたとあなたの勤務先に向けて月次報告書を作成する無料の健康状態追跡管理装置

容認できる

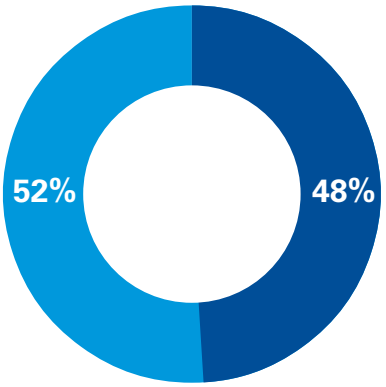
許容できない



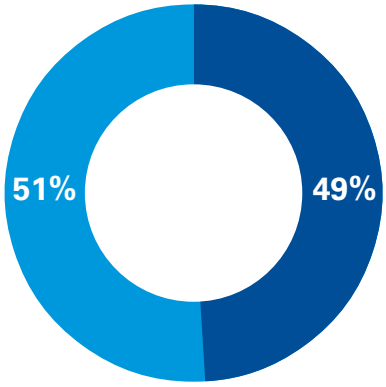
保険料を引き下げるが、危険な運転をしていたら警察に通報する権利を保険会社に与えるテレマティックス装置



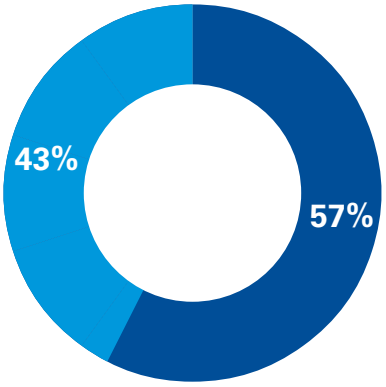
視聴習慣のモニタリングを許可することを条件に割引価格で販売されている新型テレビ



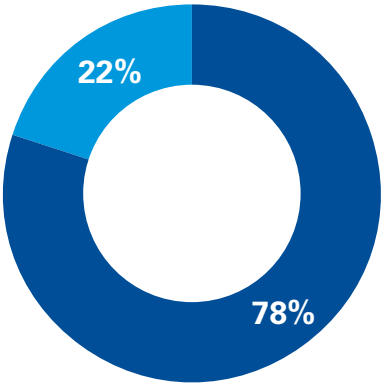
テクノロジー企業に、いつ・なぜ・どのようにして利用されるかについての追跡を許可することを条件に、無料で提供されているタブレットPC



司法当局によるテロ防止活動を支援するため、eメールやテキストメッセージおよびウェブ閲覧履歴の収集を許可すること



契約事業者が住人の数、食事や就寝の時間、使用している電化製品を推測することが可能となる、エネルギーのスマートメーター



救急サービス会社が、自分の車を追跡することが可能になるテレマティックス装置

反発に注意：消費者はいずれ対価を要求するようになるだろう

消費者は日々、無料の通信サービスや簡単に手に入る知識、無数のエンターテインメントコンテンツ、そしてかつてないほどの利便性と引き換えに、企業に個人データを提供することには同意を示しています。消費者が公平な対価を受け取っていると考えている限り、その同意は成立します。

しかしある特定の消費者層、たとえば個人データを利用されることを不快に思う人々が、十分な対価を与えられていないと考え始めたとしたらどうなるでしょうか？ または個人データがどれだけ利用されているかについて、より明確に自覚し始めたらどうなるでしょうか？ シークレットモードでのウェブ閲覧や広告のブロック、クッキーの削除を行っている人が増えていることは、多くの人々にとってこの問題がますます重要性を帯びている兆しと考えられます。

本調査から、世界の消費者の60%が、既にインターネットブラウザのクッキーを削除し、また52%の消費者がソーシャルメディアのプライバシー設定を管理していることがわかりました。

これらの割合を国ごとに見てみると、個人データを守るためにソーシャルメディアのプライバシー設定を管理したり、定期的にユーザー名とパスワードを変更したりする人の割合が最も高かったのはインドでした。

対照的に日本の回答者は、個人データを守るために防衛策を取る確率が最も低い傾向にありました。

プライバシー問題に関する意識の高まりに伴い、企業が個人データの売買を通じてどのような金銭的利益を得ているかについて消費者が認識した場合、企業は消費者からの反発に見舞われる可能性があります。

大手検索エンジンやソーシャルメディアプラットフォームにおけるビジネスモデルは、消費者のデータを販売することで成り立っています。経済協力開発機構（OECD）の推計によれば、Facebookにとって欧州の消費者1人当たりの個人データの価値は年間5米ドルに過ぎませんが、米国人の場合は10米ドル近く[2]に跳ね上がります。2014年にデータクープという新興データブローカーが月8米ドルの支払いで個人データを渡さなくて済むというサービスを提供した[3]という事実は、消費者が個人データを第三者企業から買い戻さなければならないという、倫理的に問題のある状況が訪れる前触れとも言えます。

消費者がインターネット上で取った行動や買物履歴、通信内容をモニタリングすれば、個人データが生成されます。データを収集する側は、消費者がいったん個人データを共有すれば、個人データはもはや消費者自身のものではなくなると主張するかもしれません。

たとえば英国の国営保健サービスは、蓄積された個人データを収益化する方法を既に模索しています。この活動を支持する人々は、たとえデジタル保健サービスへのアップグレードに費用がかかったとしても効率が高まり、匿名化した保健データベースへのアクセスを企業に対して有料で許可することによって、費用の回収が可能だと主張しています。

2. OECD (2013), "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", OECD Digital Economy Papers, No. 220, OECD Publishing. http://dx.doi.org/ 10.1787/5k486qtxldmq-en
3. How much is your personal data worth? | News | The Guardian

データブローカー：あなたが私を知れば、私もあなたを知る

データブローカー（消費者情報の収集・販売事業者）は、あなたの大切な人や両親、そして、もしかしたらあなた自身よりもあなたのことをよく知っているかもしれません。

データブローカーは世界約数十億人の情報を収集し、販売しています。データブローカーはあなたのeメールアドレスや電話番号、数ヵ月前からのインターネット検索履歴、購入動向、そして性的嗜好さえ知っているかもしれないのです。

ある大手のデータブローカーは、全世界の7億人の消費者と、米国のほぼすべての消費者に関する3,000以上の「傾向」についての情報を持っていると話しています。

利益の共有

消費者にとって、個人データが生みだす利益を共有するための、より公正なモデルは、自分の個人データを販売する企業との間で正式な利益共有契約を結ぶことです。企業にとってのもう1つの選択肢は、消費者が提供する個人データによって製品価格を変更することでしょう。これは既に、テレマティックス装置でドライバーの運転習慣をモニタリングする代わりに、そのドライバーの自動車保険料を引き下げるという形で、ある程度実現しています。事実として、回答者の45%が、たとえ警察に通報されるおそれがあるとしても、保険料が安くなるなら保険会社に運転習慣をモニタリングされても構わないと答えています。またブラジル、中国およびロシアでは、そのために運転習慣をモニタリングされることを受け入れると答えた回答者が64%と半数を上回りました（図4参照）。

次に登場するのが、健康状態をモニタリングする装置を装着する代わりに健康保険料を安くできるという、類似の取り決めだったとしても不思議ではありません。

本調査において、健康状態をモニタリングし、健康的なライフスタイルを維持するための月次報告書を作成する最新の健康状態追跡管理装置を勤務先から渡されたらどうするかと尋ねたところ、ブラジルの回答者の76%とインドの回答者の85%がそれを受け入れると答えました。しかしこれを受け入れられると考える北欧の回答者は少ない傾向にありました。

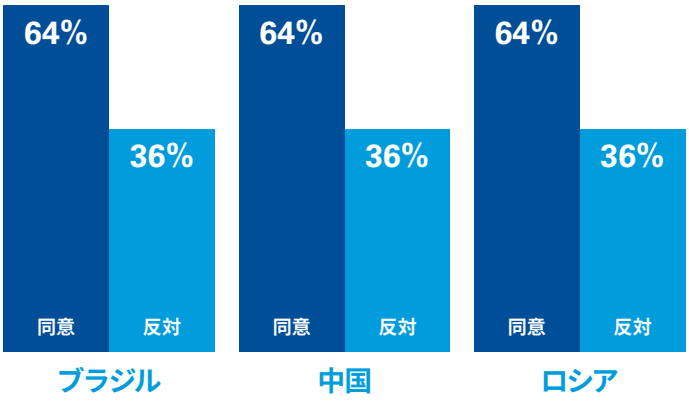
こうした二重価格モデルは、インターネットに接続された他のデバイスにも広がる可能性があります。消費者が何を視聴しているかを追跡するテレビが100米ドル、追跡機能のない同型のテレビが500米ドルで販売されることはあり得ます。IoT（モノのインターネット）に対応した「モノ」（インターネットに接続されたデバイス群）は2020年までに200億以上に増加すると推定され、特に消費財メーカーにとっては考慮すべきテーマとなっています[4]。

今後のデジタル化社会においては、消費者が個人データの共有にどの程度意欲的かという問題が極めて重要となります。本調査では、半数をかなり上回る国々において、回答者の60%～87%がプライバシーに対するコントロールは利便性よりも重要だと答えており、また、55%の回答者が、プライバシーに関する懸念を理由にインターネットでは買い物をしないことを決めたと答えました。インターネットで買い物をした場合に、個人データの取扱いについて懸念する人の割合が最も高かったのはマレーシア（74%）、フィンランド（72%）およびシンガポール（70%）でした（図5参照）。

しかし、消費者が自分の個人データに対するコントロールを取り戻そうとしても、既に手遅れかもしれません。一部の個人データは既に広範囲に拡散されてしまっており、完全なコントロールを取り戻すことは実質的に不可能です。インターネットの普及が加速していることを踏まえると、消費者が気づかないうちに、もっと多くの個人データが共有されていると考えた方がよいでしょう。

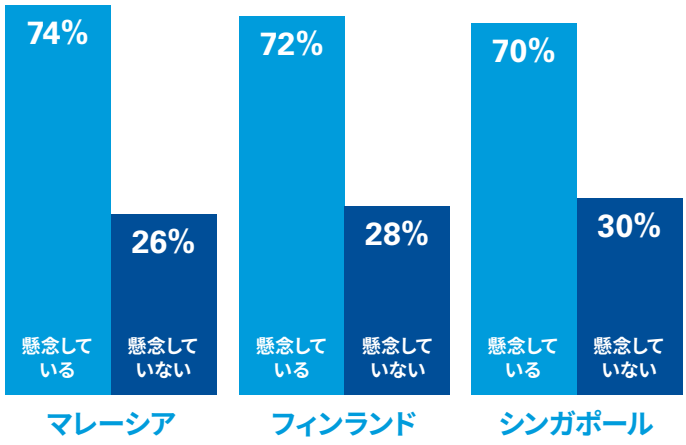
長い目で見ると、企業はいずれ個人データの共有について、より明確なボーダーラインを設け、個人データの価値を率直に認めざるを得なくなるでしょう。それまでの間は、迫り来る消費者からの反発をいかに管理し、最小限に抑えられるかが焦点となると考えられます。

図4：自動車の運転をモニタリングされることに同意しますか



出所：Crossing the line: Staying on the right side of consumer privacy, KPMG International, 2016

図5：オンラインショッピングにおけるプライバシーの取扱いについて懸念していますか



出所：Crossing the line: Staying on the right side of consumer privacy, KPMG International, 2016

4. http://www.gartner.com/newsroom/id/3165317

エグゼクティブのための考察：個人データを販売する業者に「赤信号」を付与する

Greg Bell
Global Cyber Security Co-leader
KPMG International

「販売価格に差をつけるということは、少なくともその企業は個人データを収集していることを率直に認めていることになります。消費者は現在、長々とした複雑な利用条件を読んでサービスを利用するかどうかを選択しなければなりませんが、本当にその条件を読んでいる人はほとんどいません。

考えられるもう1つの解決策は、シンプル、かつ、規則によって管理された信号システムです。個人データのすべてを販売するウェブサイトには赤信号、詳細な個人データの一部を販売するウェブサイトには黄信号、消費者が個人データを完全にコントロールできるウェブサイトには青信号を付与するのです。そうすることで消費者は、個人データに対する公正な対価が得られるのか、情報を得た上で判断することができます。

透明性とコントロールを高めることによって、消費者がより率直に個人データを共有することを示す兆しは、早くも見え始めています。イタリア北部にあるトレントという町で、その町に住む数百世帯が参加するオープンデータシェアリングシステムの利用実験が行われましたが、その実験において参加者の情報は安全な方法で保存され、情報にアクセスできる人をコントロールすることも可能でした。そのため、参加した世帯はこのシステムを信頼することができ、最終的には実験当初よりもはるかに多くの情報を共有するようになりました[5]。」

5. 'With Big Data Comes Big Responsibility', Harvard Business Review, 2014年11月

消費者がプライバシーを重視しているのであれば、なぜ個人データを提供するのでしょうか？

Bruce Lyons
Professor of Economics
University of East Anglia
United Kingdom

East Anglia大学のBruce Lyons経済学教授はこう話します。「人々は個人データを他者と共有するのは不快だと言いながら、実際には個人データを提供しています。自分の生活の各場面を次々とソーシャルメディアに投稿しながら、プライバシーを失うことを気にしているのです。」

人々がなぜ個人データとなると合理的な決定や標準的な経済理論から乖離してしまうのかについて、考えられるいくつかの答えは、行動経済学が示してくれます。

「現状維持」というバイアス：人は今所有しているものに固執しようとする性質を備えています。企業はデフォルトのオプション設定を通じて、この性質を利用することができます。多くの場合、インターネットにおけるデフォルトのオプション設定は「共有する」になっています。

フレーミング効果によるバイアス：個人データを共有することのメリットが前面に打ち出される一方で、プライバシーの喪失といったデメリットは隠されています。そのため消費者は不快さを感じながらも受け入れる可能性が高くなります。

自信過剰：我々は得てして、後悔することになるようなものは共有したりしないと自負しているものです。FacebookやTwitterにおいて起きた事例の多くは、実際にはそうではないことを物語っています。

「今だけ」というバイアス：我々はソーシャルメディアの「いいね」や「共有」によって直ちに得られる満足感については強く欲するものの、情報を共有し続けることによる長期的な結果についてまでは考えが及びません。

Bruce Lyons教授は言います。
「企業は消費者に影響を与えるために利用し得る行動戦略をよく認識していますが、それは規制当局も同じです。たとえば英国の金融行動監視機構は、消費者からの搾取を防ぐため、行動バイアスの監視を既に行っています。またオーストラリアの財政規制緩和省は2012年12月、規制を改善するため、行動戦略の利用に関する文書を発表しています。」

規制当局はどこに境界線を引くのか?

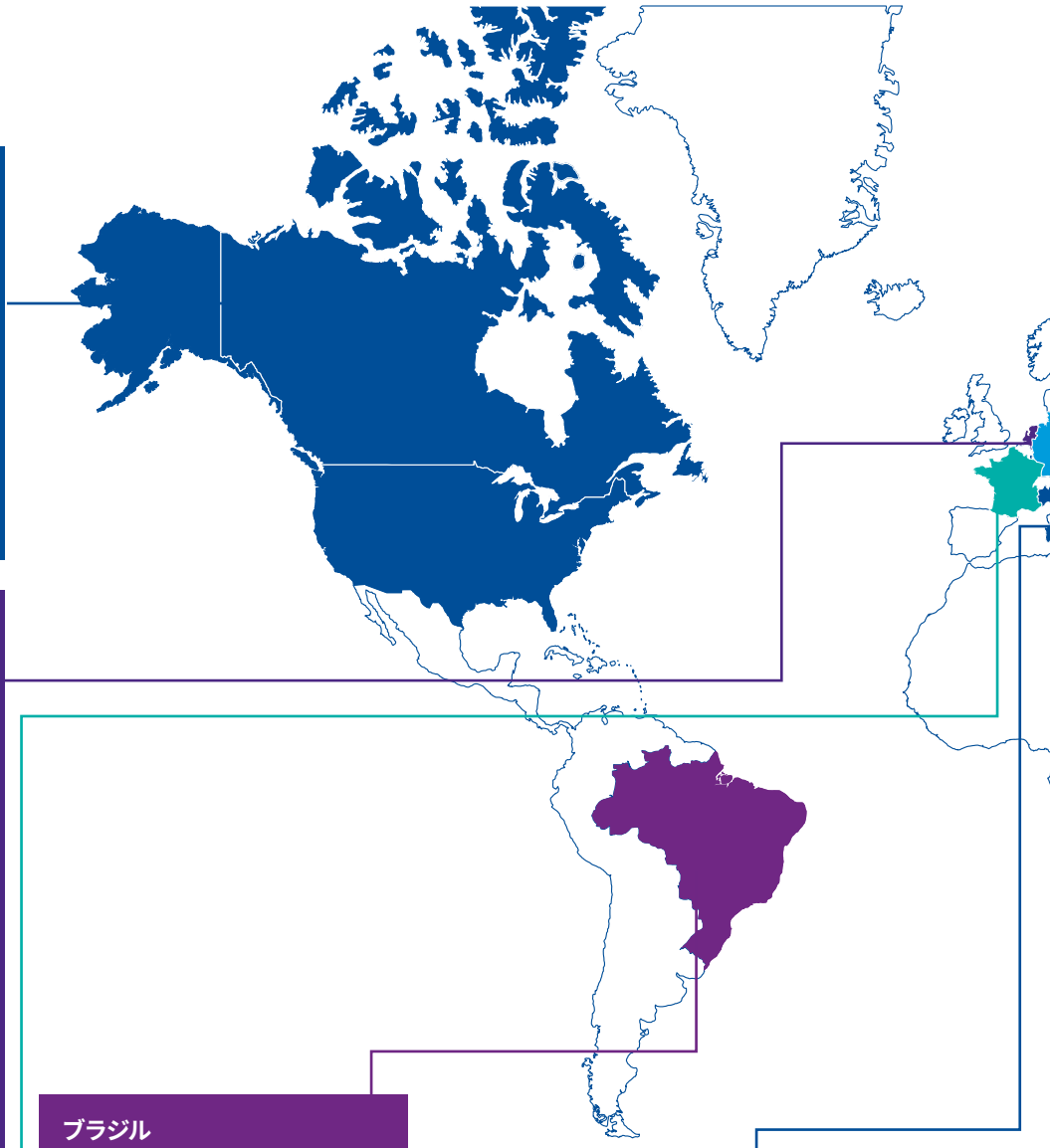
消費者のプライバシーに関する問題について、もはや企業は片手間で取り扱うことはできません。サイバーセキュリティやハッカーとの戦いは、長い間、最高情報責任者（CIO）の最重要任務でした。しかし、サイバーセキュリティとプライバシーは性質が異なります。

EUが定めた新たな規則である「一般データ保護規則（General Data Protection Regulation、以下「GDPR」という）」は、プライバシーを企業が消費者の個人データを扱う際に最も配慮しなければならないものとして位置づけており、大きな変化を示しています。GDPRが2018年5月に発効されれば、違反企業には世界の総売上高の4%を上限とする罰金（または2,000万ユーロのいずれか高い金額）が科せられることになります。

GDPRは、おそらくプライバシーに関する一貫した規制的な枠組みを定義するための、最も包括的な試みになりますが、各国の政府はプライバシー問題にさらに注目し、消費者の保護を強化し、違反企業をより厳しく処罰する法律を制定しつつあります。

プライバシーに対するより厳格なアプローチが世界的に採用されつつあることによって、企業にとってプライバシーは最重要リスクとなりつつあります。急激に変化する現在の社会環境において、企業はプライバシーに対してどのような姿勢を取るべきかを考える必要があり、また財務面や風評に対するリスクを最小限に抑えるために、早急に対策を講じなければなりません。

境界線 ―― 世界各国の視点



米国およびカナダ

米国およびカナダにおいては、個人データをハッカーに盗まれることを最も強く懸念しています。「北米ではほぼ毎日のようにデータの漏えい事件が起きているため、北米の人々がハッカーを懸念していることは何ら不思議ではありません。訴訟や集団訴訟が増加しており、またGDPRなどの法律を通じて罰則が強化されていることから、米国に本社を置く企業はプライバシーに対するアプローチを真剣に検討せざるを得ないでしょう。」
―Doron Rotman, KPMG in the US

オランダ

オランダは、企業による個人データの取扱いと利用方法を懸念する回答者の割合が、最も低い国の1つでした。また、「非常に懸念している」割合についても、ロシアに次いで2番目に低いものでした。「おそらくオランダ人の堅実的な性格が関係していると思います。その一方で、オランダはGDPRの発効よりも早い、2016年1月1日付けでデータ漏えい通知法を導入し、プライバシー保護機関に対して違反者への罰金を科す権限を与えました。また、違反に対する罰金の引き上げにより、既にオランダ企業によるデータ漏えい報告が迅速化され、プライバシーの管理が徹底化されるという成果が出ています。」
―Koos Wolters, KPMG in the Netherlands

フランス

フランスはたとえテロとの戦いに役立つとしても、政府機関による個人データの収集に最も否定的な国の1つでした。「歴史に残るような悲劇的な出来事を契機に、フランスの人々は約40年前に最初に制定されたプライバシー法を重視するようになりました。そのため、フランス政府は現代社会が直面する最も難しい問題のいくつかに対処しようとする際には、プライバシー問題に関して国民が何を期待しているかについて考慮する必要があります。」
―Vincent Maret, KPMG in France

ブラジル

ブラジルでは2015年1月、個人データ保護法案が公表されました。この法案には、本人からの同意の取得、個人データの処理・転送、データ漏えいの報告、並びに、本人による個人データへのアクセスを認めることに関する規定が含まれていました。また、この法案には違反者への罰則が定められており、違反者には罰金が科せられ、最長で10年間、個人データの処理の停止または禁止が言い渡されることになります。
―Leandro Augusto Antonio, KPMG in Brazil

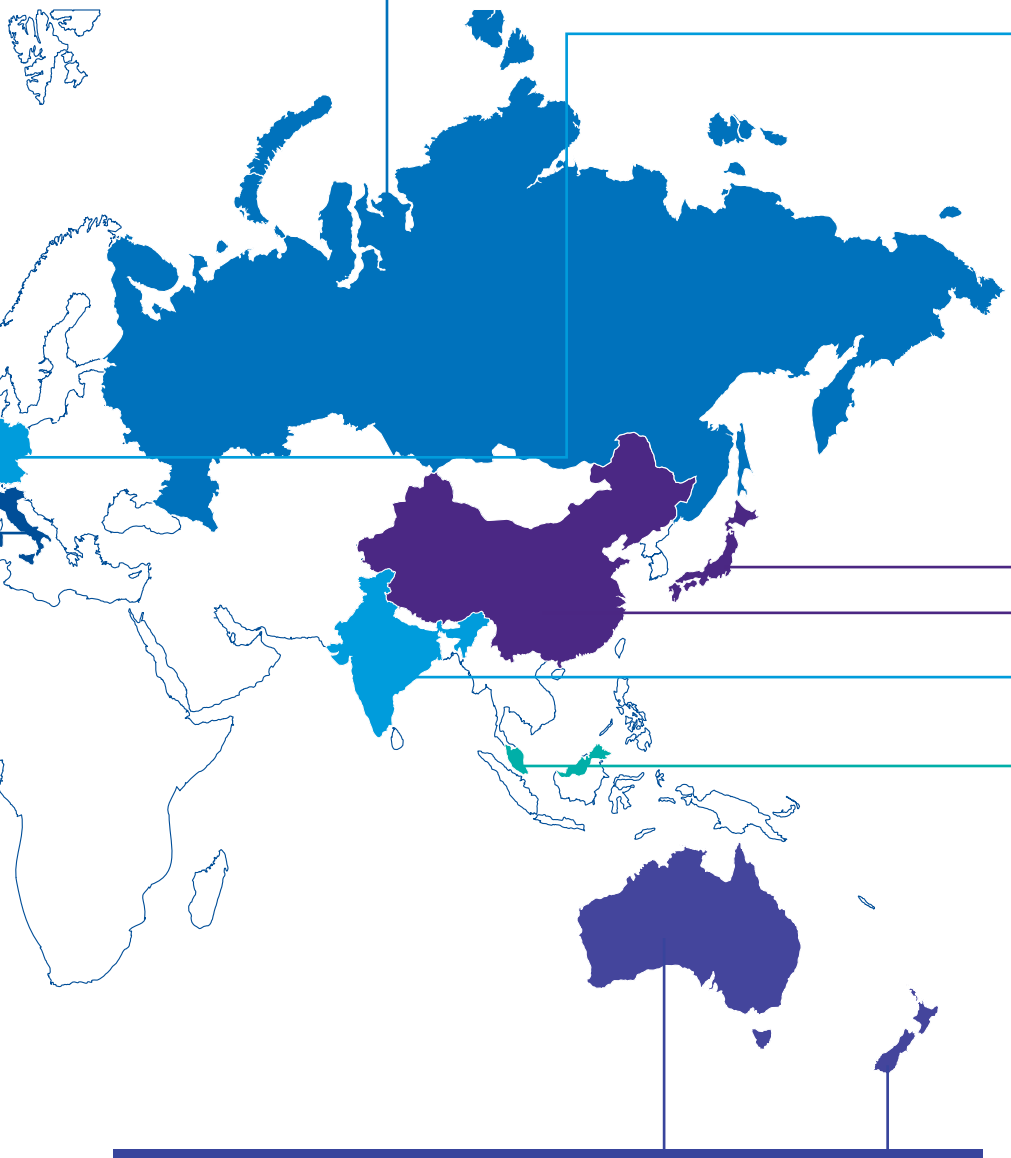
イタリア

イタリアは、政府機関による個人データの収集に最も肯定的な国の1つでした。「これはイタリアで、プライバシーに関するリスクについての意識が危険と考えられるほど低いということにも一致しています。分析結果を詳しく見てみると、イタリアは欧州諸国の中でもソーシャルメディアをよく利用する国の1つであり、インターネット上で買い物した場合、自分の個人データがどうなるかを懸念する人の割合が最も低い国でもあることがわかります。また、先の遠い話にはなりますが、デジタルメディアがイタリア社会で大きな存在感を示していることを踏まえれば、プライバシーに対する国民の意識を高めていくしかありません。」―**Luca Boselli, KPMG in Italy**

ロシア

ロシアの回答者のうち、企業による個人データの取扱いおよび利用方法を非常に懸念していると答えた割合はわずか11%でした。「このことは、個人データが漏えいした場合にどのような結果になるかについて、ロシアの人々が十分に認識していないことを表しています。ロシアでプライバシー規約が普及し始めたのは最近のことであり、平均的なロシア国民は技術的側面や、プライバシーの分野における自分の法的な権利をあまり認識していません。加えて、ロシアのマスコミがプライバシーに関する事件をあまり取り上げないことも意識の低さにつながっています。」

—Ilya Shalenkov, KPMG in Russia



ドイツ

ドイツは、勤務先が支給する無料の健康状態追跡管理装置を受け入れると答えた回答者が最も少なかった国の1つです。「ドイツ人が伝統的に個人データの共有に消極的であることを考えれば、何ら不思議ではありません。経済のデジタル化が進むにつれ、ドイツ企業にとって、プライバシー問題は本当に重要な課題となってきています。適切なバランスを見出さない限り、ドイツ企業は時代に取り残されるおそれがあります。」

—Michael Falk, KPMG in Germany

日本

日本の回答者はインターネットで企業と情報を共有することに最も消極的だったものの、個人データを守るために自ら防衛策を取る確率も最も低い傾向にありました。「このため、インターネット事業を営む日本企業は興味深いジレンマに直面しています。適切なバランスを取ることさえできれば、企業にとってはチャンスとも言えます。」

—田口　篤、KPMGジャパン

中国

「中国では、回答者の60%がパーソナライズド広告を容認できると答えたにもかかわらず、39%の回答者は企業による個人データの取扱いや利用方法について、非常に懸念しています。中国で事業を営む企業の間では、顧客を呼び込むためにデジタルイノベーションを活用することはよく受け入れられていますが、優れた新製品の活用と信頼の維持を両立させることは本当に困難です。」

—Henry Shek, KPMG in China

インド

「インドの回答者は個人データを扱う企業に対して、最も高い信頼を示しています。経済のデジタル化が進むにつれ、この信頼はインド市場で価値を創造するための大きなチャンスを与えてくれるでしょう。しかし、プライバシー問題に対する意識が高まるにつれ、インドの消費者が企業に寄せる信頼や期待は変わっていくものと予想されます。」

—Mayuran Palanisamy, KPMG in India

マレーシア

「マレーシアを含むアジア各国の企業は技術革新に大規模な投資を行っており、新興企業が数多く誕生し、デジタル技術やアナリティクス技術への投資も盛んです。プライバシーに関する顧客の懸念に十分に対応することが成功の鍵となるでしょう。」

—Dani Michaux, KPMG in Malaysia

オーストラリア

オーストラリアの回答者は、欧州諸国を除いて、ウェブサイトを開く時にプライバシーポリシーに目を通す確率が最も低い傾向にあります。「そのため、オーストラリアの企業は興味深い課題に晒されています。一般的に考えて、顧客が表示された情報に目を通さないとすれば、企業は顧客に対する透明性をどうやって確保すればよいのでしょうか？ 企業はこの透明性を確保するために、革新的で利用しやすい、新たな方法を考えなければなりません。」

—Jacinta Munro, KPMG in Australia

ニュージーランド

ニュージーランドの人々は、個人データを守るために広告をブロックするソフトウェアを用いる傾向が最も高くなっています。「ニュージーランドの人々はプライバシーを真剣に捉えています。企業は顧客やクライアントとの関わりにおいて、常にこのことを考慮しなければなりません。」

—Souella Cumming, KPMG in New Zealand

境界線 ―― 各業界の視点

ライフサイエンス業界

「従来の医薬品業界におけるビジネスモデルはもはや通用しません。ライフサイエンス業界はM&A、個別化医療へのシフト、患者のための価値感に基づいた治療成果へのフォーカス、さまざまな医療技術の進歩と連携、そしてビジネスパートナーやITパートナーとの協力強化を通じて、かつてないほどの変貌を遂げました。こうした新しいビジネスモデルを推進・維持するためには、個人データを含む情報が重要な役割を果たします。ライフサイエンスにおける近年の発展を活用するためには、利用すべき情報を特定し、保護・管理する必要があります。」

Chris Stirling
Global Chair Life Sciences

テクノロジー業界

「IoTでは靴から電源を切ったまま時刻をモニタリングするテレビ、コピー機に至るまで、ありとあらゆるものがインターネットに接続します。プライバシーの取扱いを誤った場合、企業は本当に大きな代償を支払うこととなり、膨大な費用と時間をかけて問題を修復することに務めなければなりません。」

Gary Matuszak
Global Head of Technology, Media and Telecommunications, KPMG International

消費者市場業界

「消費財企業や小売企業がターゲット顧客に送るメッセージは、ますます関連性が高く、タイムリーなものになりつつあります。これらの企業は顧客またはインターネットでの買物客に関する膨大な量の詳細な個人データや行動データを追跡することが可能であるため、とりわけ顧客が考える「容認できる／許容できない」の境界線を超えてしまうリスクが高いと言えます。消費財企業や小売企業は、どこで、いつ線引きをすべきかについて正確に把握するために、自社のマーケティングキャンペーンが及ぼす良い影響と悪い影響の両方に注意を払わなければなりません。」

Willy Kruh
Global Chair, Consumer Markets,
KPMG International

金融サービス業界

「資産と情報を保護することは金融機関の伝統であり、金融機関は今も優先事項としてこれらの分野に多額の資金を投じています。金融機関が直面している課題は、これまでの投資を活用し、顧客が期待する保護を確実に提供すること、並びに、事業とリスクの特性を持続的に管理するための適切な対応に投資することです。これら2つの課題を克服できる企業は、本業に加え、インターネットID認証サービスおよび個人データ保護サービスにおいても、必要な顧客データの保管者としての信頼獲得競争で優位に立つことができます。」

Jeremy Anderson
Global Head of Financial Services, KPMG International and Partner, KPMG in the UK

エネルギー・資源業界

「エネルギー企業は、今や家庭の内側にまで進出しようとしており、スマートメーターなどの新しいテクノロジーは、顧客に関して従来にないレベルの新たな考察をもたらしています。そこから価値を創造することは重要ですが、こうした革新的な活動が企業の中核的な事業活動に悪影響を及ぼさないようにすることが極めて重要です。」

Alejandro Rivas-Vásquez
UK Head of Cyber Security, Energy,
KPMG in the UK

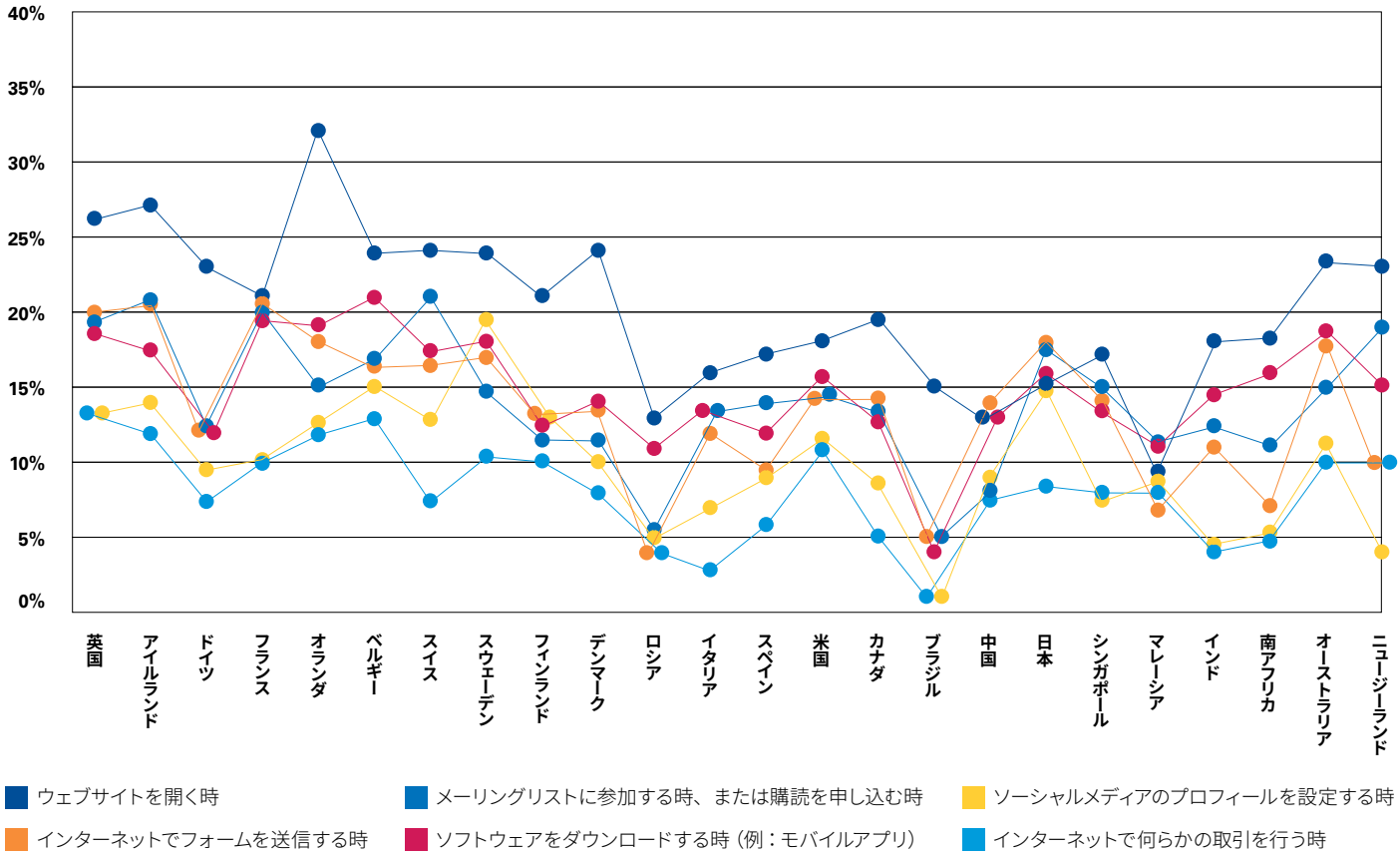
企業は生き残るためにどう変わるべきか?

最初に取り組むべき課題の1つは、プライバシーに対する考え方の見直しです。これまで受け入れられていたか、少なくとも許容されていたことについて、プライバシー関連法令に対する、より厳格化された世界的なアプローチに照らして見直す必要があります。

今までのような、長々とした法的な説明文や20ページもある免責事項によって顧客を困惑させ、顧客の同意を得る戦略をこれからも維持することはできません。本調査によれば、対象各国の回答者のうち57%がウェブサイトを開く時にプライバシーポリシーをまったく読まなかったり、ざっと目を通したりするだけで済ませています。また地域別に見てみると、ヨーロッパの消費者は、北米およびアジア太平洋地域の消費者と比べて、プライバシーポリシーに目を通す確率が低い傾向にあります（図6参照）。

企業はこれまでの戦略に代えて、プライバシーに関する基本原則に「透明性」を掲げるべきです。企業は顧客データを用いて何をしたいのか、顧客データをどこにどのように保存するのかを完全に理解した上で、それを顧客にわかりやすく、簡潔に説明する必要があります。

図6：消費者はどの程度プライバシーポリシーを読んでいるか



出所：Crossing the line: Staying on the right side of consumer privacy, KPMG International, 2016

プライバシーの適切な保護

企業はプライバシーに関する透明性を維持することを困難と考えるかもしれません。既存の、または、将来的な規制がどのような影響を及ぼすかについて把握していないことがその一因ですが、他にも以下のような原因が挙げられます。

— プライバシーポリシーを設けていないため

— 場当たり的に個人データを収集しているため

— データがどこにあるかまったくわからないため

データがどこにあるかわからなければ、データを管理することは不可能です。また、顧客リストが営業部門やマーケティング部門に存在する一方で、個人データは情報システム部、事業開発部、人事部、財務部の間を移動し、互換性のない数百種類ものシステムの中に保存されている場合もあります。

また、古いファイルサーバーに保存され、仕入業者、決済プロバイダ、監査人、規制当局、その他いくつもの第三者の間であまり考慮もされずに転送されているかもしれません。そこには埋めるべきギャップが文字通り何千も存在します。

世界中で相次いで制定されたプライバシー関連法令には、往々にしてデータローカライゼーション規定が盛り込まれており、そのことも企業にとって大きな課題となっています。データのローカライゼーションとは、データを国内で保存・処理しなければならないことを指します。コストを削減し、柔軟性と効率性を高めるため、企業活動においてクラウドコンピューティングへの依存度が高まっていることを考えれば、データを国内で保存・処理することを求める規則は、世界市場を分断化し、事実上インターネットユーザーに不利益をもたらす可能性があります。

企業はプライバシー問題を取締役会レベルで検討すべき最重要課題と捉え、プライバシー戦略、システムおよび業務プロセスに対して適切な経営リソースを投じる必要があります。それを怠った企業は高い代償を支払うことになるでしょう。

安心・安全

プライバシー問題とは対照的に、企業の上層部の関心を情報セキュリティに向けさせることは比較的容易です。本調査では、平均32%の回答者が強力なセキュリティシステムを構築・維持することは市場からの信頼を勝ち取るための最も効果的な手段だと答え、フランス、マレーシア、スペインなどいくつかの主要各国では40%以上がそう回答しています（図7参照）。

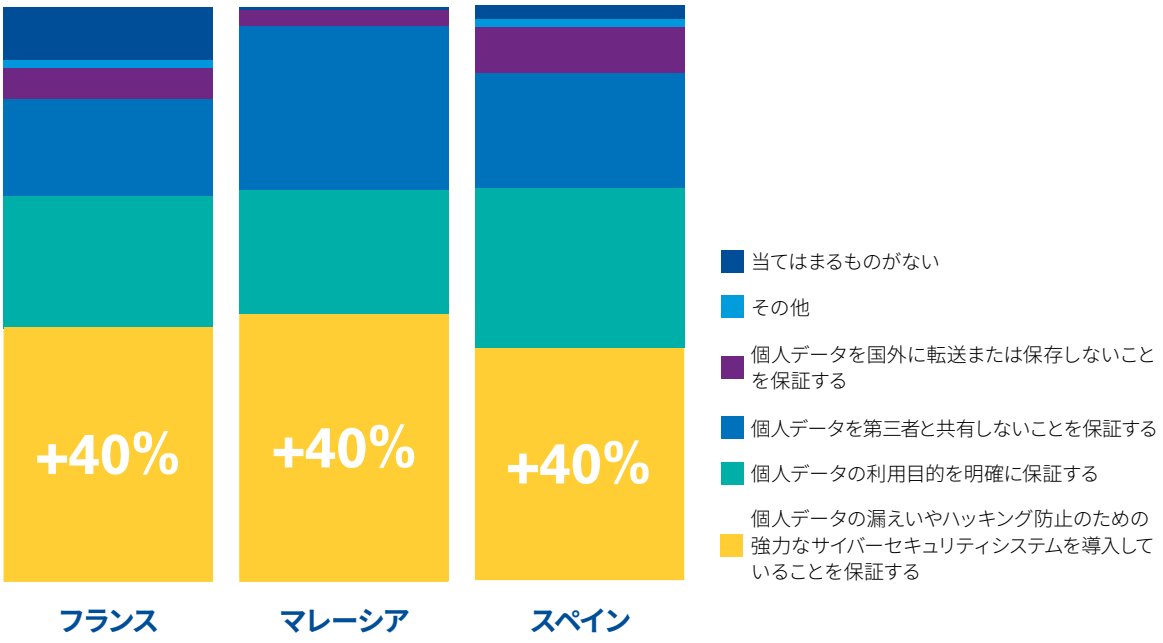
とりわけセキュリティが侵害された時はニュースになるため、セキュリティに対しては、プライバシーには滅多に注がれないような関心と経営リソースが注がれることになります。

しかし現実には、セキュリティはプライバシーに関する包括的な枠組みにおいて考慮すべき多くの要因の1つに過ぎません。たとえ企業が強力なセキュリティ管理体制を構築していたとしても、個人データに関して適切な通知を行い、本人の同意を得ているのでしょうか？ 国境を越えた個人データの転送に関する規則を遵守しているでしょうか？ 導入予定の規制要件への対処はできているでしょうか？ プライバシー管理の枠組みを厳密に構築しようとすれば、他にも多くの要素を考慮しなければなりません。プライバシー保護におけるセキュリティとは数ある要素の1つに過ぎないのです。

これらの物事を適切に行うことは、大規模かつ世界をまたがり対応する課題であり、（ごく一部の企業だけが設置することのできる）大規模なプライバシー専任チームにとっても例外ではありません。

こうした状況に対処するには、投資や時間、経験が求められます。この分野はまだ比較的新しいため、資格を持った経験豊富な人材が不足しており、このことが問題を一層困難なものにさせています。

図7：信頼を勝ち取るための最も効果的な手段は何だと思いますか



出所：Crossing the line: Staying on the right side of consumer privacy, KPMG International, 2016

「プライバシー保護体制」を整える

本調査から、平均で56%の回答者が企業による個人データの取扱いおよび利用方法を「懸念している」または「非常に懸念している」ことがわかりました。

特に中国、インド、シンガポールでは、個人データの取扱いおよび利用方法に対する強い懸念が見られました。「非常に懸念している」と答えた人々の割合はこれら3ヵ国が最も多く、それぞれ39%、35%、32%でした（図8参照）。

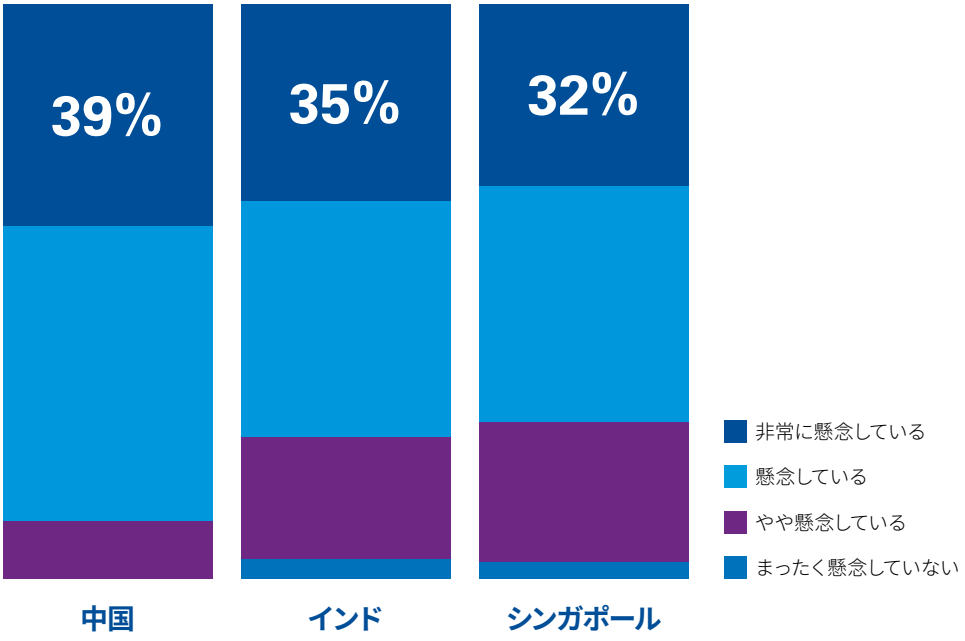
これらを踏まえると、企業にとってはプライバシーを優先事項とする包括的な枠組みの開発が極めて重要になると言えます。数千人もの従業員を抱える世界的に名の通った製造業の会社であれば、まずは従業員の個人データに焦点を当てるとよいかもしれません。一方、消費者と直接向き合う企業においては、消費者の個人データに関する問題の解決を優先すべきです。

適切に設計された、プライバシーに関する包括的な枠組みは、営業活動やマーケティングを制約するものではなく、企業が顧客をよりよく理解し、製品やサービスを改良し、顧客の具体的な要望に応じるためのツールであると見なすべきです。

その動機がチャンスであれ不安であれ、企業は問題の大きさと複雑さを理解し、迅速に行動する必要があります。企業が個人データを扱う際には、データを収集した瞬間からそのライフサイクルが終わるまでの間、絶えずプライバシーを考慮しなければなりません。まるで本格的な登山のような大仕事に見えるかもしれませんが、世界中の規制当局が間もなく対応を要求しようとしている今、企業はできるだけ迅速にこの仕事に着手した方がよいでしょう。

「本調査によれば、平均で56%の回答者が、企業による個人データの取扱いおよび利用方法について『懸念している』または『非常に懸念している』ということがわかりました。」

図8：個人データを扱う企業への信頼度



出所：Crossing the line: Staying on the right side of consumer privacy, KPMG International, 2016

時代に乗り遅れるな: プライバシーに関する次の動きとは?

個人データは今後の経済を動かす燃料であり、1つの収益源であり、繁栄の牽引役でもあります。プライバシーへの脅威に関する人々の意識が高まるにつれて、消費者の懸念に対処する新しいビジネスモデルが登場しつつあり、既存の企業にチャンスと課題の両方をもたらしています。

多くの場合、斬新なテクノロジーサービスは個人データが利用可能なことによって成り立っています。たとえば、アプリケーションを利用した自動車の相乗りサービスは、GPSによるユーザーの位置情報に依拠しており、そのためユーザーが現在いる地点を手動で入力するといったバックグラウンドでのプロセスを省き、コストを減らすことが可能です。しかし当然ながら、個人データに基づいたビジネスモデルと消費者のプライバシーの間には対立関係が存在します。

本調査によれば、84%の回答者が企業による個人データの利用方法を「十分に」コントロールできていないと感じており、完全にコントロールできていると答えたのはわずか10%でした。そろそろ消費者が個人データに対するコントロールを取り戻すのを支援するような、新しいテクノロジーが登場してもよい頃ではないでしょうか[6]。

人々が個人データを提供するのは、多くの場合、それによる明確なメリットがあると考えるからです。消費者にとってのメリットとは、たいていは無料または低価格ということになりますが、企業側にも明らかなメリットがあります。たとえば金融サービス業界では、ドイツのクレディテック社[7]や米国のフェア・アイザック社 (FICO)[8]などのイノベーション企業が、インターネットやソーシャルメディアに投稿した利用者のプロフィールを活用して信用リスクを定量化し、従来の信用分析を一変させつつあります。今まで融資判断に用いられていたプロセスは、重要性を失いつつあるのです。

消費者にとって、個人データを活用することはシェアリングエコノミーに一歩近づくことになります。シェアリングエコノミーでは、クラウドソーシングにより融資や保険、投資を手に入れることができ、投資家はそれを提供する代わりに、融資を行う前にソーシャルメディアなどに掲載されている個人データを確認するのです。

「企業による個人データの利用方法を『十分に』コントロールできていないと感じる回答者は、84%にのぼりました。」

6. 'Privacy and Cybersecurity: Key findings from Pew Research', Pew Research Center, 2015年1月15日
7. FT: 'Kreditech: A credit check by social media', Financial Times, 2016年1月19日
8. Forbes: 'Your social media posts may soon affect your credit score', Forbes.com, 2015年10月23日

個人データのコモディティ化

個人データがパッケージ化されて株式市場で取引され、裕福な消費者の個人データほど高く取引されるようになるのは、そう遠い先のことではないでしょう。企業は消費者が提供する個人データのレベルに応じて製品やサービスの価格に差をつけるようになるかもしれません。

意識の変化

ほとんどの人は、企業が自分に関する個人データをどの程度保有しているか、またそのことが自分の生活にどのような影響を及ぼすかについてまだ認識していませんが、そのような傾向は変わりつつあるのかもしれません。

最近開発された1つに、インターネット上で自分を追跡する者を逆探知するアプリがあります。米国の学術研究チームが開発したこのアプリは、どの企業がインターネット上で消費者を追跡しているかを正確に示すというものです[9]。このような知識があれば、多くの人々が自分の情報がどのように利用されているかを意識するようになり、プライバシー侵害に気づくようになります。

消費者のためのデータブローカー

もう1つの選択肢は、第三者が本人に代わって個人データを管理する「ID属性交換」です。民間投資企業がこのサービスの提供に興味を示しています。これを実現するためのツールや規制はまだ完成していないものの、現在のように急速に変化する時代においては、いつ実現してもおかしくありません。

人々は個人データと引き換えに受け取るサービスに満足している限り、自分の個人データを利用するビジネスモデルを許容し続けるのでしょうか？ 近い将来に大手検索エンジンやソフトウェア企業が市場での優位性を失うとは考えにくいものの、プライバシー保護サービスの成長は、個人データを守りたいという人々の基本的な要望を表しています。

マーケットの発展に伴い、企業は顧客データの保護とは、単に熱心過ぎる規制当局をなだめるための事務的手続ではないということを認識する必要があります。顧客の意識やマーケットの期待が高まったことによって、ある企業がデータ保護やプライバシーを真剣に捉えていないという印象を持たれてしまえば、消費者からの信頼を損なうだけでなく、企業そのものにおける財務上の安定性までもが脅かされるおそれがあります。

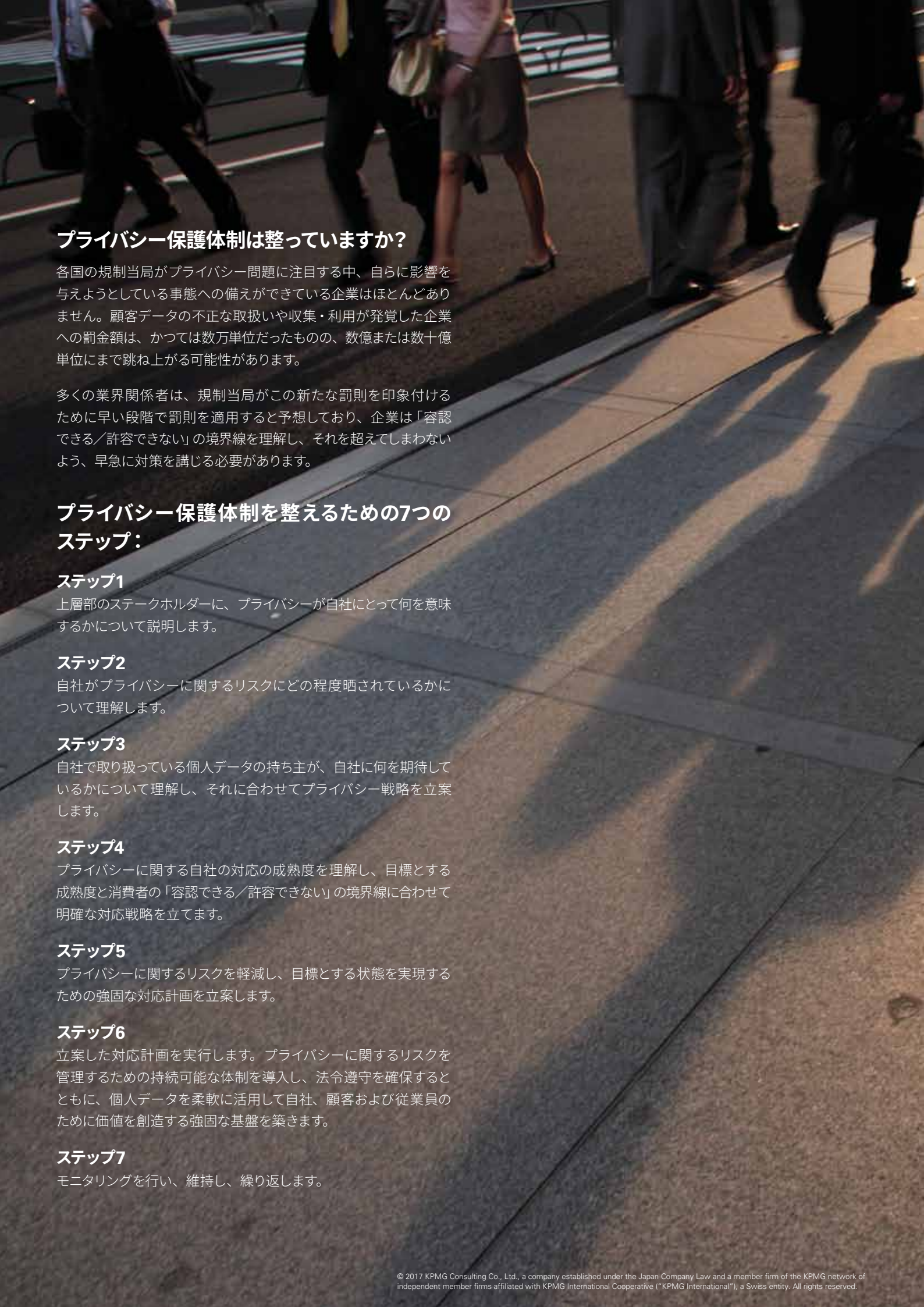
9. 'Privacy apps to help fight back against companies that track you', New Scientist, 2015年11月25日

エグゼクティブのための考察：ブローカーを呼んでくれ！

Akhilesh Tuteja
Global Cyber Security Co-leader
KPMG International

「データが消えることはありませんが、データを隠すことは可能です。そのため、インターネット上でブランドの曖昧化、つまり利用者の身元を隠したり、「再ブランディング」したりするサービスを販売する企業が登場してくることは想像に難くありません。論理的に考えて、既に存在するインターネット上のパーソナルブランドマネージャーの次に来るのはこうしたサービスでしょう。

また、消費者に直接マーケティングを行うパーソナルブローカーサービスの開発が、企業にとって現実のものになるかもしれません。個人データのブローカーは、個人と、個人データの利用を希望する企業との仲介役を果たします。あなたの車が故障したと想像してみてください。あなたは、既にあなたの現在地、車種、登録情報と銀行情報を知っているデータブローカーに連絡を取り、車の回収や修理を手配してもらうことができます。データブローカーはすべての関連情報を一瞬で呼び出し、一連のプロセスを手配する単一窓口を消費者に提供してくれます」



プライバシー保護体制は整っていますか?

各国の規制当局がプライバシー問題に注目する中、自らに影響を与えようとしている事態への備えができている企業はほとんどありません。顧客データの不正な取扱いや収集・利用が発覚した企業への罰金額は、かつては数万単位だったものの、数億または数十億単位にまで跳ね上がる可能性があります。

多くの業界関係者は、規制当局がこの新たな罰則を印象付けるために早い段階で罰則を適用すると予想しており、企業は「容認できる／許容できない」の境界線を理解し、それを超えてしまわないよう、早急に対策を講じる必要があります。

プライバシー保護体制を整えるための7つのステップ:

ステップ1
上層部のステークホルダーに、プライバシーが自社にとって何を意味するかについて説明します。

ステップ2
自社がプライバシーに関するリスクにどの程度晒されているかについて理解します。

ステップ3
自社で取り扱っている個人データの持ち主が、自社に何を期待しているかについて理解し、それに合わせてプライバシー戦略を立案します。

ステップ4
プライバシーに関する自社の対応の成熟度を理解し、目標とする成熟度と消費者の「容認できる／許容できない」の境界線に合わせて明確な対応戦略を立てます。

ステップ5
プライバシーに関するリスクを軽減し、目標とする状態を実現するための強固な対応計画を立案します。

ステップ6
立案した対応計画を実行します。プライバシーに関するリスクを管理するための持続可能な体制を導入し、法令遵守を確保するとともに、個人データを柔軟に活用して自社、顧客および従業員のために価値を創造する強固な基盤を築きます。

ステップ7
モニタリングを行い、維持し、繰り返します。

KPMGがクライアントのためにできること

KPMGのプライバシー担当プロフェッショナルは、世界各地のクライアントを支援し、特定企業に特有のニッチな課題から、高度に規制された複雑な業界における一貫したプライバシー法令遵守プログラムに至るまで、複雑なプライバシー問題の解決に携わってきました。

KPMGのプライバシーチームは、企業の多様なニーズに対応できる体系的かつ柔軟なアプローチを通じて、プライバシーリスクに起因する課題へのクライアントの対応を数多く支援してきました。KPMGメンバーファームは世界各地、複数の地域にまたがり、各地域のメンバーファームと連携しながら業務を行うことが可能です。

KPMGが多く手がける分野は以下のとおりです。

— **評価：**独立した第三者の立場から、プライバシーに関するリスクとその低減方法を評価します

— **設計：**プライバシー法令遵守プログラムを設計します

— **導入：**プライバシーに関する強固な業務プロセス、方針および統制を導入します

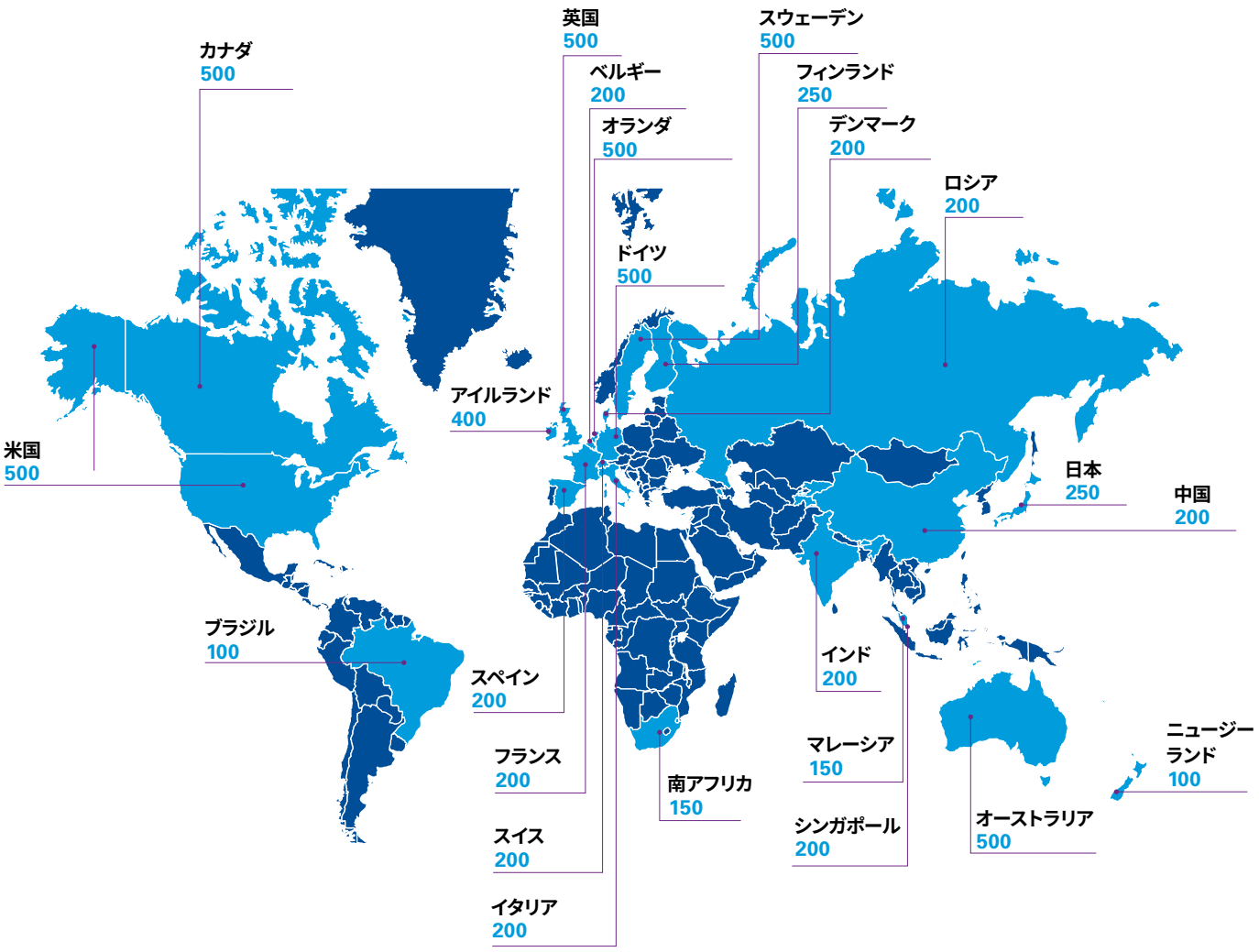
— **戦略：**実践的なプライバシー戦略を開発し、経営層の同意を取り付けます

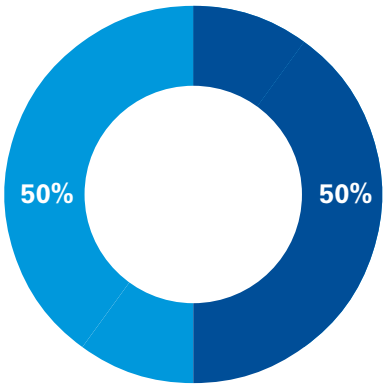
— **運用：**クライアントによるプライバシー保護の枠組みの運用を継続的に支援します

— **モニタリング：**クライアントによるプライバシー保護体制の維持と運用状況のモニタリングを支援します

本調査における回答者属性

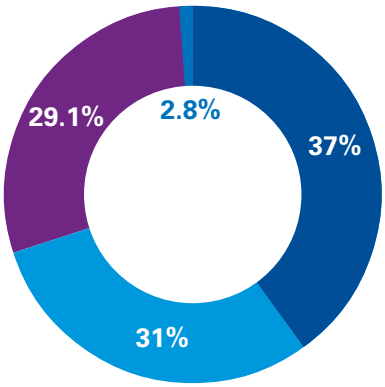
24ヵ国6,900人の回答者にご協力いただきました。





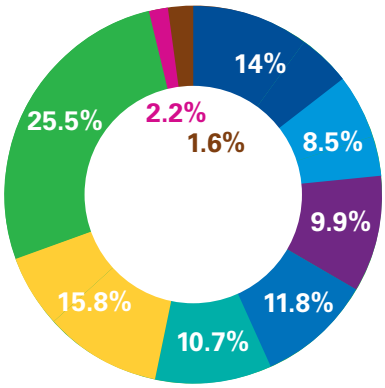
性別

男性	(3,451)
女性	(3,449)
合計	**(6,900)**



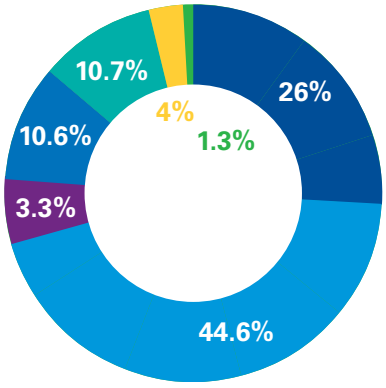
年代

ミレニアル世代（35歳以下）	(2,555)
ジェネレーションX（36～51歳）	(2,142)
ベビーブーム世代（52～70歳）	(2,009)
71歳以上	(194)
合計	**(6,900)**



ライフステージ

子供がいない若い成人	(965)
若い世帯 — 例：就学前の子供がいる	(585)
中年齢層世帯 — 例：5～9歳の子供がいる	(683)
高年齢層世帯 — 例：10～16歳の子供がいる	(811)
16歳超の扶養家族と同居している — 例：16歳超の同居している子供がいる	(738)
子供と別居している — 離れて暮らす子供がいる	(1,090)
子供がいない成人	(1,762)
その他	(155)
非回答	(111)
合計	**(6,900)**



既婚歴等

独身（未婚）	(1,792)
既婚	(3,077)
シビルパートナーシップ（法的に承認されたパートナーシップ関係）を結んでいる	(230)
パートナーと同居している	(729)
配偶者と死別、離婚、または別居し、一人暮らしをしている	(701)
恋人はいるが同居はしていない	(278)
その他	(93)
合計	**(6,900)**

注記：小数点以下四捨五入のため合計値は100%にならないことがある。

お問合せ先

KPMGコンサルティング株式会社
サイバーセキュリティアドバイザリー

TEL：03-3548-5111
cybersecurity@jp.kpmg.com

www.kpmg.com/jp/cyber-security

kpmg.com/socialmedia

本冊子は、KPMGInternationalが2016年に発行した「Crossing the line. Staying on the right side of consumer privacy」を翻訳したものです。翻訳と英語原文間に齟齬がある場合には、当該英語原文が優先するものとします。

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供するよう努めておりますが、情報を受け取られた時点およびそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

Publication number: 134122-G JAPAN: 17-1502