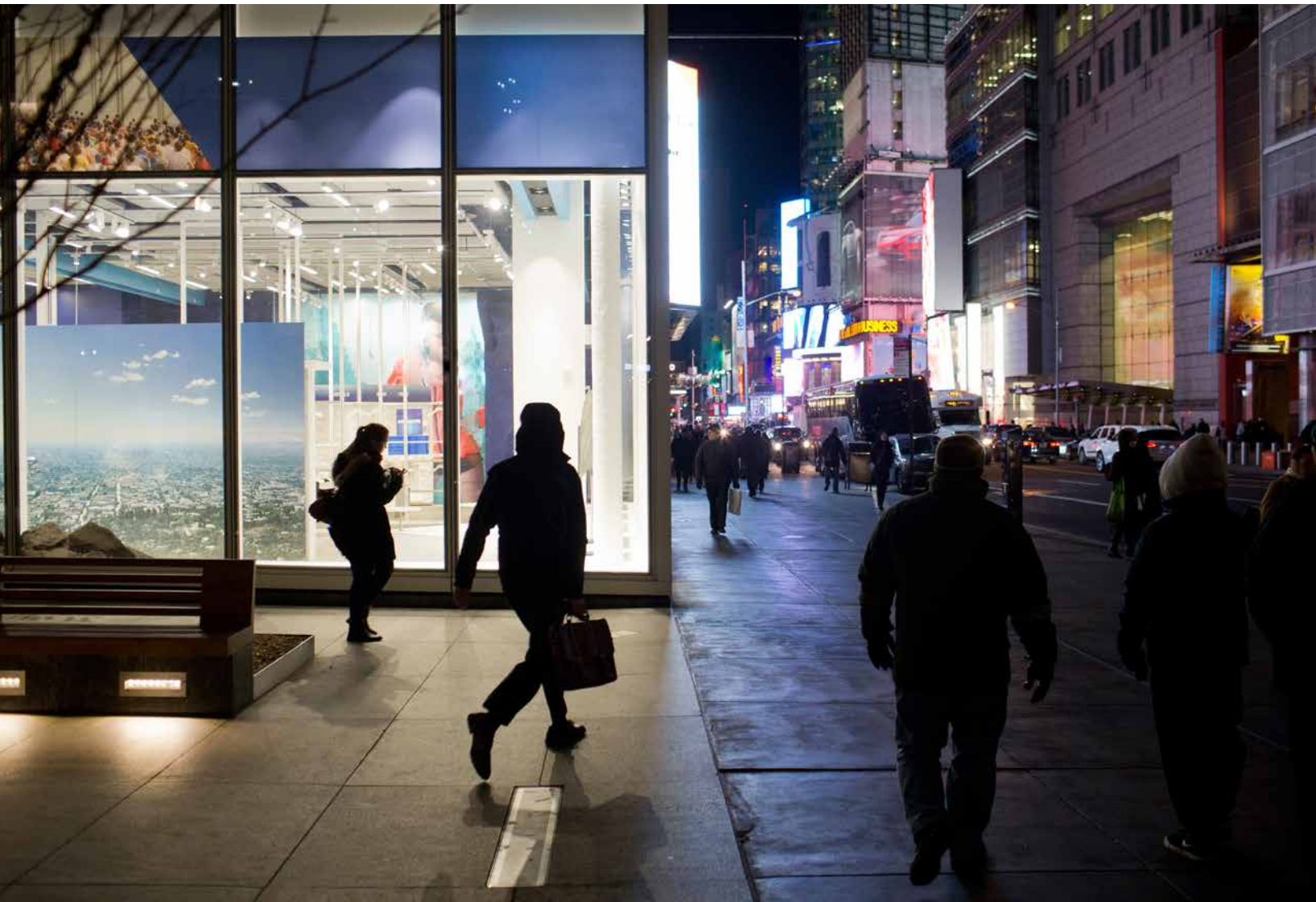


www.pwc.com/jp

サイバーセキュリティおよびプライバシー

データが動かす世界に向けて プライバシーと信頼に新たな命を吹き込む



グローバル情報セキュリティ調査 2018 Vol.2





大規模なデータ漏洩や個人情報収集の常態化により、デジタル社会において旧来の意味でのプライバシーは既になくなったのではないかという議論に拍車がかかっている。私たちはプライバシーなき世界を生きているのだろうか？ この問いは、多くの点で間違っている。プライバシー、セキュリティ、信頼——いずれもますますリスクにさらされているが——は、データが動かす社会においてよりその重要性を増し、相互に密接に絡み合っているのだ。

データプライバシー および信頼に関する PwCの知見

- 1 CEOは、認識するだけに留まらずアクションを起こすべき 3
- 2 デジタルトランスフォーメーションにおけるリスクマネジメントへの真剣な取り組みが、企業の存亡を左右する 5
- 3 プライバシーへの期待は、機密性からデータ利用へ 6
- 4 高度な認証テクノロジーが信頼を築く 8
- 5 業界大手企業においても、取締役会の関与強化は必須 9
- 6 より多くの企業が最高プライバシー責任者(CPO)の設置を検討すべき 10
- 7 後れを取る欧州および中東の企業が抱える課題はさらに多い 11
- 8 インターネットの分断がビジネスを変える 12
- 9 消費者の支持を得るのは、イノベーションやデータ利用に対する責任ある取り組み 14
-  グローバルビジネスリーダーが取るべき次のステップ 16
-  日本企業への示唆 18

PwCが実施したグローバル情報セキュリティ調査 2018 (GSISS2018) によると、世界中の多くの企業は、プライバシー保護に全力を尽くしていない。プライバシー・リスク・マネジメントを行うために、再び議論を活発化させ、より強固にサイバーセキュリティと統合することが求められる。消費者や規制当局もそれを望んでいる。CEOや取締役会にとっての目の前の問題は、プライバシーの未来ではなく、自社の将来についてである。企業はプライバシー・リスク・マネジメントの行き詰まった状況を打開するために、意思と想像力を結集しようとするだろうか？ その勢いを利用してサイバーセキュリティを統合し、イノベーションとデータ利用に信頼のおけるブランドを築こうとするだろうか？ それとも、より熱心に取り組む競合企業に、市場における優位なポジションを譲り渡してしまうのだろうか？

本資料において、GSISS2018の主要な調査結果などから、データが動かす社会に向けて、プライバシーと信頼の取り組みを改めて見直すために9つの知見を提示し、グローバルビジネスリーダーが取るべき次のステップを示すこととする。

1 CEOは、認識するだけに留まらずアクションを起こすべき

エグゼクティブらはサイバー空間の危険性の高まりを感じている。これはGSISS2018の結果にも、第21回世界CEO意識調査の結果にも表れている¹。後者の結果では、世界中のCEOがサイバー脅威をビジネス上の最大の懸念事項と位置づけている。米国のCEOの回答はさらに先を行き、サイバー脅威は最大の包括的な懸念事項であり、過剰な規制や地政学的な不確実性、テロリズムよりも上位に置いている。世界経済フォーラムの『グローバルリスク報告書2018』によると、今後十年で最も発生可能性の高いリスク上位5位以内に、大規模なサイバー攻撃と、不正による深刻なデータ漏洩または不正利用の二つを挙げている²。

1 PwC、[第21回世界CEO意識調査](#)、2018年1月

2 World Economic Forum、[2018 Global Risks Report](#)、2018年1月

データ利用と 保管における 透明性向上に大いに取り組んでいる との回答は **44%**

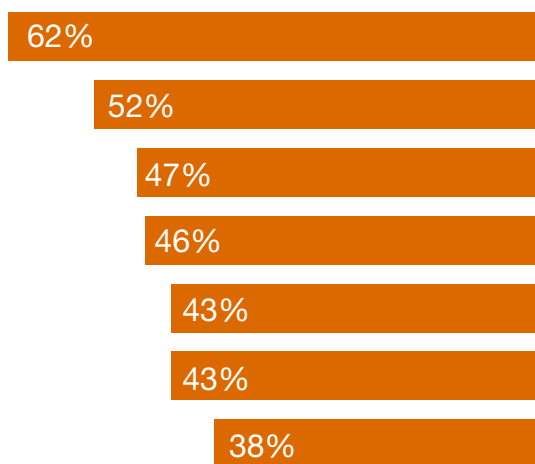


出典: PwC、第21回世界CEO意識調査、2018年1月
N= 1,293

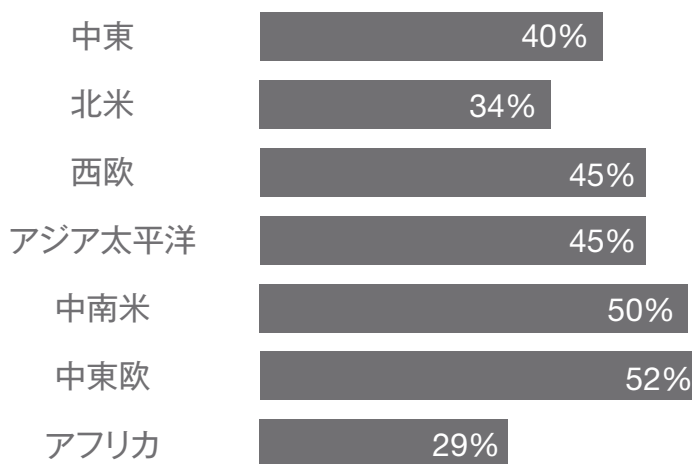
安心材料もいくつかある。例えば、世界のCEOの87%が、顧客の信頼を得るためにサイバーセキュリティへの投資を行っていると回答している。また同様に、81%の回答者が、データ利用と保管における透明性を向上させていると答えている。とはいえ、これで十分と言えるだろうか？ 残念ながら、これらの取り組みを“大いに”行っていると答えたCEOは、半数に満たない³。さらには、アフリカのCEOの3分の1、北米のCEOの約4分の1 (22%) のCEOは、データ利用と保管における透明性向上にまったく取り組んでいないと回答している。

世界のCEOは、サイバーセキュリティおよびプライバシーへの取り組みをさらに強化できる

顧客との信頼関係を構築するためにサイバーセキュリティ投資を大に行っていると答えたCEOの割合



顧客の信頼を得るためにデータ利用と保管における透明性向上に大いに取り組んでいると回答したCEOの割合

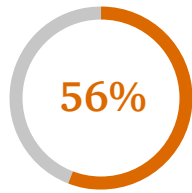


出典: PwC、第21回世界CEO意識調査、2018年1月
N= 中東(52)、北米(148)、西欧(274)、アジア太平洋(464)、中南米(136)、中東欧(139)、アフリカ(80)

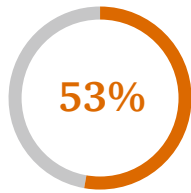
³ 世界のCEOの47%がサイバーセキュリティに大いに投資していると回答、また44%がデータ利用と保管における透明性向上に大いに取り組んでいると回答。

多くの企業はまだデータ利用に対するガバナンスの経験が浅い

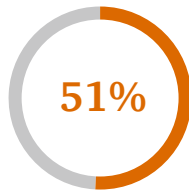
重要な対策を講じているとの回答者は約半数に留まる



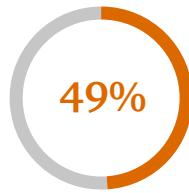
総合的な情報セキュリティ戦略がある



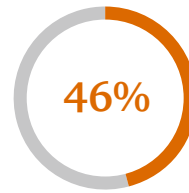
プライバシーポリシーおよび実務に関する従業員トレーニングを行っている



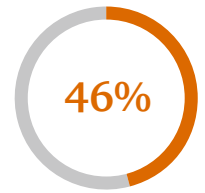
正確な個人データインベントリがある



個人データの収集・保持・アクセスを必要最小限に制限している



個人データを扱うサードパーティへのコンプライアンス監査を実施している



サードパーティにプライバシーポリシーの遵守を義務づけている

出典: PwC、CIOおよびCSO、グローバル情報セキュリティ調査 2018
N= 9,500

2 デジタルトランスフォーメーションにおけるリスクマネジメントへの真剣な取り組みが、企業の存亡を左右する

デジタルテクノロジーは、現在の基準では完全に捉えることができない方法で、社会がどのように消費し、取引し、相互に関連し、組織化しながら動くかを変えようとしている⁴。2025年時点で毎年作成・コピーされると想定されるデータ量は驚異的だ⁵。だが、122カ国9,500人の経営幹部の回答に基づくGSISS2018の結果からは、多くの企業ではデータ利用に対するガバナンスの経験がまだ浅いことが分かる。

欧州委員会の内部シンクタンクによると、個人データの保護のためにはサイバーセキュリティを「データ収集から伝送、処理、保存、利用まで、あらゆるレベルで」強化することが極めて重要とされている⁶。にもかかわらず、GSISS2018では、包括的な情報セキュリティ戦略を策定していないと答えた回答者が44%に上る⁷。また 2017 Global Digital IQ[®]調査によると、経営幹部はサイバーセキュリティとプライバシーに関するスキルの立ち遅れを懸念している⁸。

4 米商務省、[First Report of the Digital Economy Board of Advisors](#)、2016年12月

5 エコノミスト誌、[Data is giving rise to a new economy](#)、2017年5月6日。記事内の市場調査会社 (IDC) の予測では、2025年には一年間に作成・コピーされるデータの量が180ゼタバイト (ゼタは10の21乗) に達するとされている。

6 European Political Strategy Centre、[Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level](#)、2017年5月

7 PwC、[Strengthening digital society against cyber shocks](#)、2017年10月18日

8 PwC、[2017 Global Digital IQ[®]調査](#)、2017年2月

今日、課題やリスクをじっくり考える前にまず技術革新を進めようとする古い習慣は、前例のない問題を引き起こす可能性がある。「サイバーおよびプライバシー・リスク・マネジメントをデジタルトランスフォーメーションに適切に組み込んでいる企業はほとんどない」とSean Joyce (PwC、US Cybersecurity and Privacy Leader) は語る。「デザインフェーズから生産までの全てを通じてリスクマネジメントを組み込む企業が、未来の勝者となるだろう。これはブランドを確立する絶好の機会だ」

「サイバーおよびプライバシー・リスク・マネジメントをデジタルトランスフォーメーションに適切に組み込んでいる企業はほとんどない」

– Sean Joyce, PwC’s US Cybersecurity and Privacy Leader

3 プライバシーへの期待は、機密性からデータ利用へ

機密性に対する危険性がますます高くなり、サイバーセキュリティでは、システムの信頼を損ないかねないデータ操作や破壊の防止が重視されるようになりつつあり、データプライバシーではデータの利用をどう制御するかに重点が置かれるようになってきている⁹。例えば金融分野のSheltered Harborイニシアチブは、銀行が大規模なサイバー攻撃を受けた際に口座データを復旧・復元するために役立つ標準を策定している¹⁰。

9 Dan Geer氏、[SOURCEの締めくくりとなる基調講演](#)、ボストン、2017年4月27日。
スピーチの中に次の発言がある。「これまで私たちは、機密性、完全性、可用性という従来の三つの要素の中で機密性を優先していました。軍事分野では特にそうです。今後は機密性に代わって、完全性が民間部門におけるサイバーセキュリティの最も重要なゴールになるでしょう。既に軍事分野では完全性を攻撃する武器が、機密性を攻撃する武器をしのぐ、はるかに強力なものとなっています。」

10 PwC、[Strengthening digital society against cyber shocks](#)、2017年10月18日



しかし、企業が責任を持って個人データを利用するだろうと考える消費者はそれほど多くない。PwCが実施した 2017 US Consumer Intelligence Series調査では、機微情報を含む個人データを、多くの企業が責任を持って扱っていると考えている消費者は、わずか25%にすぎない¹¹。EUのサイバーセキュリティに関する世論調査2017年版では、個人データが不適切に利用されるリスクがオンラインバンキングおよびEコマースに関する最大の懸念事項となっている¹²。

米国立標準技術研究所 (NIST) は、プライバシーエンジニアリング——システムエンジニアリングの中でプライバシーソリューションの開発に重点を置いた新分野——の当初の目標の一つに機密性を挙げていた¹³。しかし、この目標はすぐに「非関連性」（個人のアイデンティティと関連づけられないトランザクションを可能にすること）に変更された。これは暗号化とデータの最小化の原則に関連している¹⁴。EUの一般データ保護規則 (GDPR) では、データの最小化を含むプライバシー・バイ・デザインが求められ、企業は必要に応じて個人データを仮名化または暗号化する必要があるとされている。これらは全て、データの管理、保護、利用に関するコーポレートガバナンスの必要性を強調している。

11 PwC, [Consumer Intelligence Series: Protect.me](#), 2017年11月

12 欧州委員会, [Special Eurobarometer 464a, Europeans' attitudes towards cyber security](#), 2017年9月

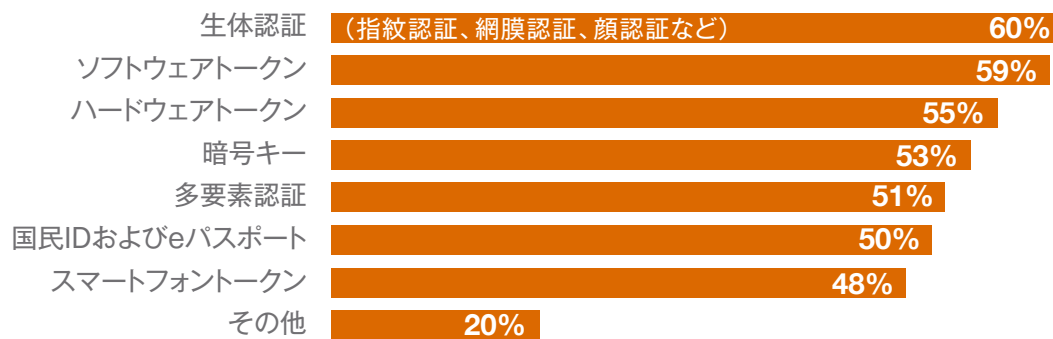
13 Inside Cybersecurity, [NIST's draft privacy-engineering concepts avoid defining privacy](#), 2014年10月3日

14 NIST Interagency/Internal Report (NISTIR) 8062, [An Introduction to Privacy Engineering and Risk Management in Federal Information Systems](#) (連邦政府システムにおけるプライバシーエンジニアリングとリスクマネジメント導入), 2017年1月。他の二つの目標は予測可能性と管理性。

4 高度な認証テクノロジーが信頼を築く

2017年7月に開催されたG20サミットの宣言では、「デジタルテクノロジーへの信頼」の必要性が強調された¹⁵。ビジネスリーダーが信頼できるネットワークを構築できるように、生体認証や暗号化など、認証テクノロジーの新たな発展が期待されている。GSISS2018では回答者の半数が、高度な認証テクノロジーの利用によって、自社の情報セキュリティおよびプライバシーの能力に対する顧客やビジネスパートナーからの信頼が向上したと答えている。また48%が不正の減少に寄与したとし、41%がカスタマーエクスペリエンスを向上させたと回答した。さらに、46%が本年中に生体認証など高度な認証テクノロジーへの投資を拡大する計画があると回答した。ただし、生体認証を単純に利用することは、企業として生体情報を追跡管理する必要が生じ、プライバシー規制や社会的関心にさらされるリスクを負うことにもなる。また、ユーザーが母親の旧姓を入力するような知識ベースの認証に頼れば、その知識が別のデータ漏洩で盗まれてしまった場合に攻撃に対して無防備になるおそれがある¹⁶。

高度な認証テクノロジーの採用が進んでいる



出典: PwC、CIOおよびCSO、グローバル情報セキュリティ調査 2018
N= 9,500

また、暗号化によるデータ保護に向け、業界に対するプレッシャーが高まることも期待される。そうなれば関連投資も活発になるだろう。金融業界では、回答者の46%が本年中に暗号化への投資を拡大する計画があると答えた。

¹⁵ G20首脳宣言、[Shaping an interconnected world](#) (相互に連結された世界の形成)、2017年7月

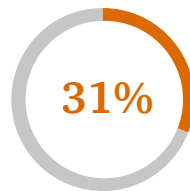
¹⁶ PwC、[2018 Global Economic Crime and Fraud Survey](#)、2018年2月。サイバー犯罪は今後24カ月で企業に損害をもたらす最大の要因となると予測している。

5

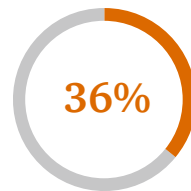
業界大手企業においても、取締役会の関与強化は必須

規模を問わず、あらゆる企業において、サイバーおよびプライバシー・リスク・マネジメントの監督に対する取締役会の関与を強化する必要がある。GSISS2018では、取締役会が現在のセキュリティおよびプライバシーリスクのレビューに直接参加しているという回答が、3分の1に満たなかった。この割合は、時価総額250億ドル以上の企業ではやや高くなっている。リスクの的確な理解なくして、取締役会がデータ保護やプライバシーの問題に関する監督責任を果たすことは難しい。加えて、PwCが実施した2017 Annual Corporate Directors Surveyによれば、自社のデータセキュリティおよびプライバシープログラムが包括的であることや、最も重要で慎重な取り扱いを要するデジタル資産が特定できているということに、多くの米国の役員が強い確信を持っていない¹⁷。

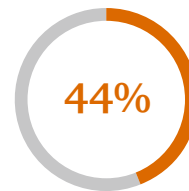
取締役会の関与には大いに改善の余地がある



取締役会が現在のセキュリティおよびプライバシーリスクのレビューに直接参加している*



取締役会が現在のセキュリティおよびプライバシーリスクのレビューに直接参加している(時価総額250億ドル以上の企業)**



自社にデータセキュリティおよびプライバシーに対応する包括的なプログラムがあることを強く確信している***



自社が最も重要で慎重な取り扱いを要するデジタル資産を特定できていることを強く確信している***

* 出典: PwC、CIOおよびCSO、グローバル情報セキュリティ調査 2018
N= 9,500
** N= 435

*** 出典: PwC、2017 Annual Corporate Directors Survey
N= 842~849

¹⁷ PwC、[2017 Annual Corporate Directors Survey](#)、2017年10月

6 より多くの企業が最高プライバシー責任者 (CPO) の設置を検討すべき

世界の回答者の約3分の2が、最高プライバシー責任者 (CPO) またはこれに相当するプライバシー責任者を設置していると答えている。この傾向は大企業でより顕著で、時価総額100億ドル以上の企業では、プライバシー責任者が設置されているという回答が少なくとも79%を占めた。時価総額150億~250億ドルの企業では81%に上る。

3分の2が

最高プライバシー責任者 (CPO) またはこれに相当するプライバシー責任者を設置していると答えている。

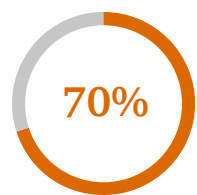


出典: PwC、CIOおよびCSO、グローバル情報セキュリティ調査 2018、
2017年10月18日
N= 9,500

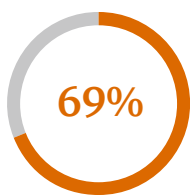
時価総額250億ドル以上の企業の回答は、データの収集・保持・アクセスの制限、正確なデータインベントリの維持、プライバシーポリシーおよび実務に関するトレーニングの実施、サードパーティーへのコンプライアンス監査の実施、サードパーティーに対するプライバシーポリシー遵守の義務づけの面でも他を上回っている。とはいえ、裏を返せば、大企業の回答者の約3分の1は、これらの主要な対策をまだ実施していないということでもある。

時価総額250億ドル以上の企業はデータ利用ガバナンスが進んでいる

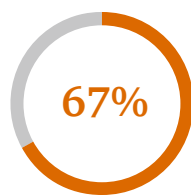
ただし、これら大企業の3分の1は、主要な対策をまだ実施していない



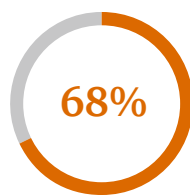
包括的な情報セキュリティ戦略がある



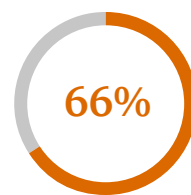
プライバシーポリシーおよび実務に関する従業員トレーニングを実施している



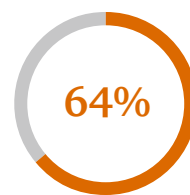
正確な個人データインベントリがある



個人データの収集・保持・アクセスを必要最小限に制限している



個人データを扱うサードパーティーのコンプライアンス監査を実施している



サードパーティーにプライバシーポリシーの遵守を義務づけている

出典: PwC、CIOおよびCSO、グローバル情報セキュリティ調査 2018
N= 407



7 後れを取る欧州および中東の企業が抱える課題はさらに多い

GSISS2018の結果によると、概して欧州および中東の企業は、総合的な情報セキュリティ戦略の策定、データ利用ガバナンスのプラクティス実装の面で、アジア、北米、南米の企業に後れを取っている¹⁸。このデータは、欧州がサイバーリスクに対して「準備不足」であるというEuropean Political Strategy Centreの結論¹⁹や、中東の企業がサイバーセキュリティについて「誤った認識」を持ちがちであるというPwCの以前の調査結果²⁰と一致する。

地域別ランキングでは、主要なプラクティスでアジアおよび北米がリード

包括的なセキュリティ戦略	プライバシーに関する従業員トレーニングの実施	正確な個人データインベントリがある	データの収集・保持・アクセスを制限	サードパーティーへのコンプライアンス監査	サードパーティーのコンプライアンスの義務づけ
アジア 59%	北米 58%	アジア 55%	アジア 53%	南米 50%	南米 50%
北米 59%	アジア 57%	北米 53%	北米 53%	アジア 49%	北米 47%
南米 54%	南米 50%	南米 52%	南米 47%	北米 47%	アジア 47%
欧州 52%	欧州 47%	欧州 47%	欧州 44%	欧州 42%	欧州 44%
中東 31%	中東 29%	中東 20%	中東 19%	中東 26%	中東 26%

出典: PwC、CIOおよびCSO、グローバル情報セキュリティ調査 2018
 N= 北米(3,175)、南米(1,261)、欧州(2,416)、アジア(1,585)、中東(94)

18 ただし、英国の回答者の64%は包括的な情報セキュリティ戦略があると答えている。
 また、英国の回答者がデータ利用ガバナンス対策を採用している割合は他国よりも高い。例えば、英国の回答者の60%は正確なデータインベントリがあると回答している。
 19 European Political Strategy Centre、[Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level](#)、2017年5月
 20 PwC、[A false sense of security? Cybersecurity in the Middle East](#)、2016年3月

32%が

2017年春の時点で GDPRアセスメントを 開始したと回答



出典: PwC、CIOおよびCSO、グローバル情報セキュ
リティ調査 2018、2017年10月18日
N= 9,500

EUでは、EUで事業を運営する全ての企業に一般データ保護規則 (GDPR) が適用され、2018年5月に施行された。GSISS2018では、対応期限の一年前にあたる2017年春の時点で、既にGDPRの対策を行っていると答えた回答者もいた。一例を挙げると、約3分の1の回答者はGDPRのアセスメントを開始しており、この割合は他の地域に比べてアジアがやや高め (37%) であった。PwCが米国、英国、日本の300社の幹部を対象として実施した最新のGDPR Pulse Surveyでは、大半の回答者が、GDPR対応はアセスメントおよび運用準備フェーズに留まっていると回答しており、地域全体としてはあまり進んでいないことが分かる²¹。

サイバーレジリエンスの向上を目的としたEUのネットワークと情報システムのセキュリティに関する指令 (NIS指令) も、2018年5月から効力を発している。当該指令の下、加盟国が必須サービス (重要インフラ) 事業者と指定する企業や、デジタルサービスプロバイダー (検索エンジン、クラウドサービス、オンラインマーケットプレイス) は、セキュリティ確保や国の機関へのインシデント報告といった新たな要件への対応に迫られている。GDPRと同様、遵守しなければ深刻な事態を招く可能性もある²²。「CEOは、GDPRとNIS指令をコンプライアンス上の試練としてではなく、データが動かす社会でビジネスを成功に導くための戦略的な機会として捉えるべきだ」とGrant Waterfall (PwC、Europe, Middle East and Africa Cybersecurity and Privacy Leader) は言う。「また対応期限が来る前に、企業は規制当局に働きかけ、常に情報を得られるような関係を構築しておくべきである」

8 インターネットの分断がビジネスを変える

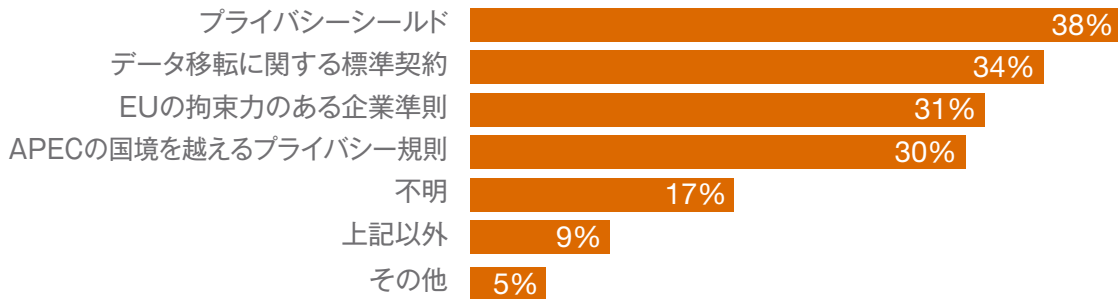
GDPRや中国の新たなサイバーセキュリティ法、ロシアのプライバシー法などその他の規制に企業がどのように対処するかは、この先長期にわたって影響を与え続けるであろう。

²¹ PwC、[Corporate GDPR preparations to stretch past May 2018](#)、2018年2月

²² 英国政府による報道発表、[Government acts to protect essential services from cyber attack: Britain's most critical industries are being warned to boost cyber security or face hefty fines](#)、2018年1月28日

米国家情報会議の最新予測によると、世界的なデータへの依存の高まりによって、「今後ますます国内および国際政策上の重要な対立点となりうる、データ所有権、データプライバシーおよび保護、国境を越えるデータフロー、サイバーセキュリティに関する明確な制限と基準を確立する必要がある²³」という。この領域における規制がさらに強化される可能性はかなり高いのだ。

国境を越えるデータフローに対して採用しているアプローチはどれか？



出典: PwC、CIOおよびCSO、グローバル情報セキュリティ調査 2018
N= 9,500

中国をはじめとするいくつかの国において、企業が営業を行う地理的境界内にデータやアプリケーションソフトウェアを留めることを義務づけようとする動きが見られる²⁴。このようなインターネットの分断により、企業のビジネスの方法が変わるだろう。効率性は低下し、マクロな視点で見ても世界経済に何らかの影響が及ぶとみられる。国境を越えるデータフローに対する新しいアプローチ、世界中で利用されるデータに対する新たなプライバシールール、強化され続ける規制。これらは全て、企業がグローバルデジタル経済において成功を収めるために通る、いばらの道なのだ。「企業は新しい法律だけではなく、実装ガイダンスにも注意を払う必要がある。これらは従来のもものと重要な点で異なる可能性がある」とPaul O'Rourke (PwC, Asia Pacific Cybersecurity and Privacy Leader) は指摘する。「例えば、中国のサイバーセキュリティ法の『国境を越えるデータフローガイダンス (2017年4月草案)』では、全てのネットワーク運営者が遵守すべき新たな義務が示されている」

²³ 米国家情報会議、[Global Trends: Paradox of Progress](#)、2017年1月。「プライバシーとセキュリティによる利益のバランスに対する相反する圧力は、ガバナンス、経済競争力、社会的結束に非常に大きな影響を及ぼすだろう」という一節がある。

²⁴ PwC、[Top Policy Trends of 2018](#)、2018年1月



9 消費者の支持を得るのは、イノベーションやデータ利用に対する責任ある取り組み

社会を変革させ、さらなる繁栄をもたらすかもしれない新たな方法で、データが世界経済を動かし始めている。テクノロジーは日々の生活に欠かせないものになり、その有用性は多くの人々が認めている。PwCが実施した 2017 US Consumer Intelligence Series調査では、回答者が最も許容できるテクノロジーの新しい活用方法を聞いている。1位はGPS（全地球測位システム）テクノロジーを使用した紛失物または盗難物の搜索。次いで総合的な健康記録を活用した発症前の異常数値の把握。さらにはスマートホームテクノロジーを活用した、外出時の空調や電気システム制御による資源および支出の節約が挙げられた。

消費者はプライバシーに金銭的価値を置くが、あくまで状況によってである。消費者がプライバシーの懸念を訴える一方で個人データをオンライン入力することは矛盾しているように見えるが、だからといって消費者がプライバシーに価値を置いていないということではない。カーネギーメロン大学ハイツ・カレッジで情報技術および公共政策を教えるAlessandro Acquisti教授は、昨年秋のPwCのPrivacy Retreatでそう述べている²⁵。同氏によると、プライバシーに対する価値の置き方は絶対的なものではなく、状況によって変化することが、研究結果によっても示されている。

PwCの 2017 US Consumer Intelligence Series調査では、消費者が認識するプライバシー保護を脅かす最大の要素にはハッカーの他、AIや機械学習、IoTなどの新しいテクノロジーの登場が含まれる²⁶。

²⁵ PwC、[What CEOs need to know about privacy ethics, economics and risks](#)、2018

²⁶ PwC、[Consumer Intelligence Series: Protect.me](#)、2017年11月

2018年には企業に対してエンドユーザーや規制当局が、説明可能で透明性があり、数学的に証明可能な方法で判断するAIの導入を求める声が強まるだろうと、私たちは考えている²⁷。AIの潜在的能力は、しっかりしたガバナンスと新しい運用モデルがあってはじめて最大限に発揮される²⁸。「AIソリューションの普及は、エンドユーザーが、(機械ではなく)自分たち自身でその情報や人生の選択を決定できていることに自信を持てるかどうかにかかっている」とJay Cline (PwC, US Privacy Leader) は言う。

また私たちは、セキュリティやプライバシーを念頭に置いて設計されたテクノロジー製品に対して、消費者はその財布の紐を緩めるとも考えている。2017年のEU世論調査では、半数以上(61%)が情報技術製品の選択時にセキュリティおよびプライバシー機能を考慮すると答えている。また、4分の1以上(27%)がより良いセキュリティおよびプライバシー機能に対してであれば、より多くの費用を支払っても良いと答えている²⁹。この調査では、後者の数字が一部のEU加盟国で著しく高いことも分かっている³⁰。中国ではデータプライバシーへの消費者の関心が高まっていると言われている³¹。さらに、2017年のPwCの調査では、調査対象の米国の消費者の75%が、機会があれば追加費用を払ってでもスマートホームデバイスのセキュリティを強化したいと答えた³²。しかし、ほとんどの場合消費者にその選択肢は与えられていない。なぜなら、多くのIoTデバイスは低コストで製造され、基本的にセキュリティまたはプライバシー保護機能を備えていないからだ。この状況は変えなくてはならない。

27 PwC, [2018 AI predictions](#), 2018年1月

28 PwC, [Accelerating innovation: How to build trust and confidence in AI](#), 2017年

29 European Commission, Special Eurobarometer 460, [Attitudes towards the impact of digitisation and automation on daily life](#), 2017年5月

30 この調査で高額でも購入するという回答が特に高かったEU加盟国は、デンマーク(44%)、ドイツ(43%)、アイルランドおよびキプロス(いずれも37%)、英国(36%)。

31 エコノミスト誌, [In China, consumers are becoming more anxious about data privacy](#), 2018年1月25日

32 PwC, [Smart home, seamless life: Unlocking a culture of convenience](#), 2017年1月



グローバルビジネスリーダーが取るべき次のステップ

最高責任者はデジタル・リスク・マネジメントの当事者でなければならない: 企業の内部でも外部でも、サイバーセキュリティ、プライバシー、信頼の関連性は強まる一方だ。データ保護やプライバシーの問題は、事業運営やリスク選好に全責任を持たない者に簡単に委譲されるべきものではなく、CEO自らがリードしなければならない。CEOの意思決定の助けとなるよう、最高プライバシー責任者が設置されるべきである。またこれらの課題について取締役会と密に連携することも優先される事項だ。さらに、CEOは破壊的なサイバー攻撃を受けた際にオペレーションを継続できるよう、レジリエンスの構築も主導する必要がある。例えば緊急時に正確なデータにアクセスできる経路を維持するためにも、事業継続戦略のアップデートは重要である。世界経済フォーラムのサイバーレジリエンス原則も活用すべきだ³³。

取締役会を巻き込む: 最高責任者がデータ保護およびプライバシーに関する新たなリスクにどのように対応しようとしているのかを、個々の役員だけではなく取締役会全体が常に深く理解しておくべきである。そのためには、取締役会の教育への長期的なコミットメントが不可欠だ。手始めに、PwCが初心者向けに提供している[How your board can be effective in overseeing cyber risk](#)、および[Five questions boards should ask about data privacy](#)を利用してよいだろう。一例を挙げると、自社の

新しいテクノロジーやデータアナリティクスの導入計画が世界的なプライバシー規制に沿っているか？という質問などは、もっと多くの取締役が投げかけているべき質問だと言える。

データ利用に対するガバナンスを優先する: より革新的な方法でデータを利用することは、チャンスと同時にリスクを増やすことにもなる。企業は強固な予防および発見的な管理策の整備と、データ利用とのバランスをとる必要がある。最も一般的なリスク——例えばデータの収集や保持に対する危機意識の無さ——を理解することが、データ利用のガバナンスフレームワークの出発点となる。詳細については、[Monetizing data while respecting privacy](#)、[Responsibly leveraging data in the marketplace](#)、[Strategically managing emerging cyber risks](#)を参照。

GDPRをチャンスと捉える: ビジネスリーダーはGDPRを未来の成功に組織を導くチャンスと捉え、単なる法令遵守ではなく、戦略的なリスクマネジメントであると考えべきである。企業は欧州の規制当局と積極的に連携し、期限到来後も即応態勢を維持しておく必要がある。なぜなら施行のピークが本年とは限らないかもしれないし、活動的な法律事務所がGDPR関連訴訟を追い続けることで、事実上の執行機関のようになる可能性もあるからだ。詳しくは、PwCの[リサーチおよびインサイト](#)を参照。

33 WEF, [Advancing Cyber Resilience: Principles and Tools for Boards](#), 2017年1月18日

海外での規制リスクを戦略的に検討する: インターネットの分断は、ソースコードなど機密性の高い知的財産の開示を要求する外国政府からの圧力に直面する企業が増えることを意味する。このような圧力にどう対応するかは、機密情報を外国政府関係者に開示することで発生するサイバー、プライバシー、信頼のリスクを考慮したうえで決められるべきである。

責任あるイノベーションを支援する: 新しい標準の策定や、プライバシー専門家とテクノロジー専門家を結びつける新たな取り組みを業界が支援し、参加することが求められる³⁴。そうすることで、プライバシー原則が実践され、サイバーセキュリティとプライバシーを念頭に置いて設計された、よりスマートなデバイスが消費者に提供されることになるだろう。さらに、デジタルトランスフォーメーションへの取り組みの過程であらかじめサイバーおよびプライバシーの

リスクマネジメントを考慮しておくことで、破壊的なサイバー脅威に対処して事業継続を可能とし、ブランドとビジネスの強化により消費者との信頼関係や競争優位性を強化することができるだろう。

これを機にデータ保護およびプライバシー・リスク・マネジメントに取り組む企業は、データが動かす社会において優位なポジションを得て成功を収め、デジタル社会におけるレジリエンスを構築できるだろう。

逆にセキュリティおよびプライバシーを確保せずにデジタルトランスフォーメーションを急ぐ企業は、衰退への道をたどるだろう。GSISS2018第三弾では、関連するテーマとして、サイバーセキュリティの未来について取り上げる。

³⁴ NIST、[Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1](#)、2017年12月5日。プライバシーエンジニアリングに関する項が盛り込まれている。

日本企業への示唆

本セクションは、グローバル情報セキュリティ調査 2018にご協力いただいた日本企業 257社のデータを、PwC Japanグループが独自に分析し、グローバルとの比較を通じて、日本企業が今後取り組むべきサイバーセキュリティのポイントをまとめたものである。

示唆1：パーソナルデータの活用を促進する二つのアプローチ

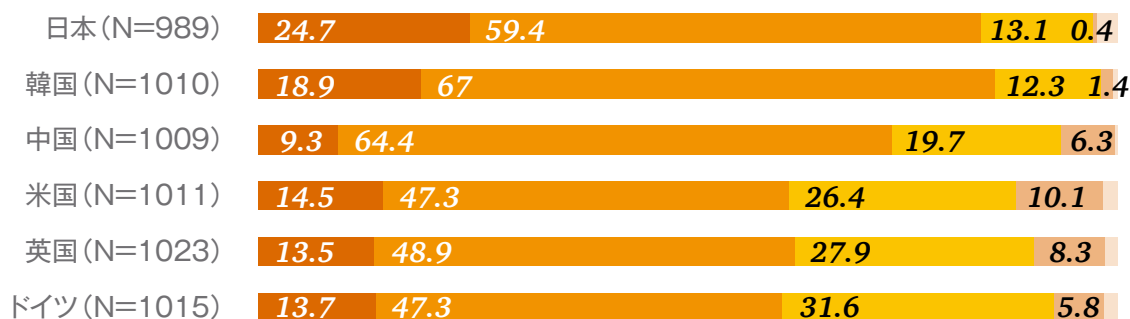
パーソナルデータをめぐる企業と消費者の埋まらない「溝」

パーソナルデータは、消費者の行動ログや購買履歴など、顧客の動向を分析するための情報であり、今やBtoC企業にとって業績を大きく左右する最も重要な経営資源の一つである。2018年6月に日本政府が閣議決定した「未来投資戦略2018」では、『データ駆動型社会』への変革が掲げられており、パーソナルデータは、個人のニーズに即したサービス提供を可能とし、一人ひとりの生活を豊かにするだけでなく、さまざまな分野での社会課題を解決し、経済成長や国際的な競争力向上にまで影響を及ぼすものと期待されている³⁵。企業によ

るパーソナルデータの活用は、それほど大きな可能性を秘めている。

一方、消費者自身はどのように考えているのだろうか。総務省が個人を取り巻く情報通信の状況などの調査を目的に毎年実施している「情報通信白書」の最新版（平成29年）を見ると、企業が自分のパーソナルデータを利活用することに対して不安を持っている個人は、国内外問わず多く存在することが分かる³⁶。なかでも日本では、80%以上の人々が、企業に対して個人データを提供する際に不安を感じている（「とても不安を感じる（24.7%）」+「やや不安を感じる（59.4%）」）。（図1参照）

図1: パーソナルデータの提供全体に対する不安感



■ とても不安を感じる ■ やや不安を感じる ■ あまり不安を感じない ■ 全く不安を感じない ■ よく分からない

35 首相官邸、[未来投資戦略2018](#)、2018年6月15日
36 総務省、[情報通信白書平成29年度版](#)、2017年7月

残念ながら、企業と消費者の間にはまだ埋めることのできない溝があるらしい。このままでは、企業のデータ活用は進まない。どのようにしたらこの溝を埋めることができるのか、2種類のアプローチを探ってみたい。

一つ目のアプローチ: データ管理の主導権を個人へ返す

近年、世界各国では、パーソナルデータの利活用を牽制するプライバシー規制が次々と制定されている。2018年5月に施行されたEU一般データ保護規則 (General Data Protection Regulation; GDPR) はその代表例である。また、業界ごとの自主規制を重視してきた米国でも、2018年6月にカリフォルニア州消費者プライバシー法が成立した。こうした規制の多くは、『データポータビリティ』、『プライバシー・バイ・デフォルト』、『忘れられる権利』といった概念が示すとおり、「パーソナルデータは個人の資産である」という考えに基づいている。企業は、消費者からパーソナルデータを預かる立場であり、その管理方法などについて、本人に対して説明する責任を負っている。(図2参照)

多くの消費者が企業におけるパーソナルデータの管理に不安を覚える根本的な原因は、「不透明

さ」にある。企業が自分に関するどのようなデータを保有しているのか、それを何に使っているのか、どこに流通しているのか、自分をどのような顧客だと位置づけているのか、正しく破棄されたのか等々、これらが消費者側からははっきり見えないことが、企業と個人の間に溝を作る主因となっている。

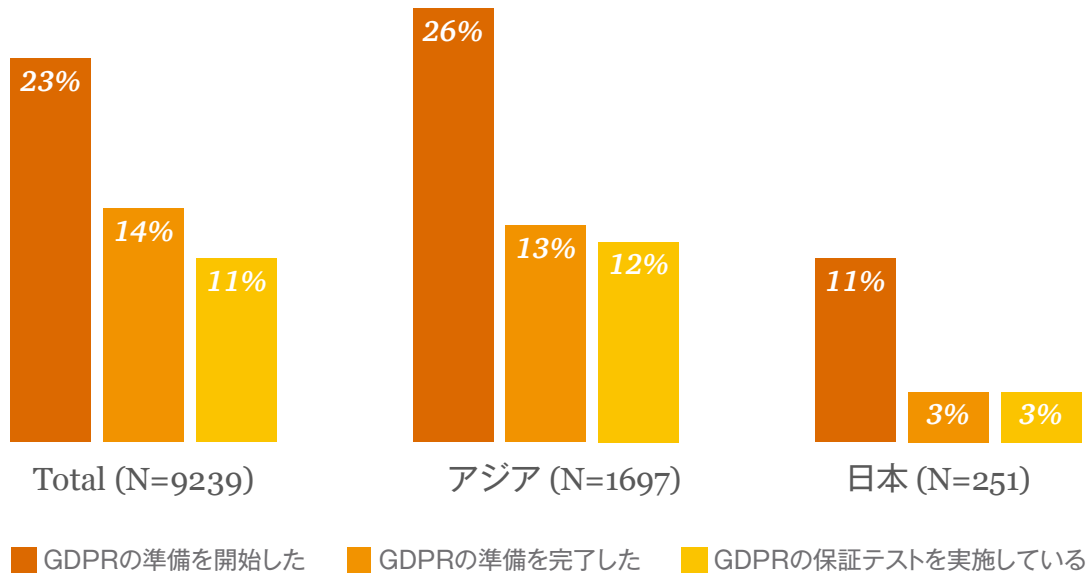
逆に言えば、企業におけるパーソナルデータの管理状況を、本来のデータ主体である個人に開示し、これまで企業が一方的に握っていたパーソナルデータの管理権限を潔く本人に移譲してしまえば、消費者の不安は払拭できるとも言える。利用履歴の閲覧、利用目的の選択、利用可能範囲の設定、一時的な利用停止、永久削除など、消費者が自らの意思でデータをコントロールできる状態、これが実現できれば、結果として、企業は消費者のパーソナルデータを集めやすくなるはずだ。

現在、日本企業において、データ管理権限を消費者に渡す動きはそれほど広がっていない。GDPR施行前に実施したGSISS2018の調査結果から、こうしたデータ管理方法の重要性を示すGDPRへの対応状況を見てみると、「準備を完了した」と「保証テストを実施している」企業を合わせても6%に過ぎず、「準備を開始した企業」も11%程度とグローバルと比較して低い状況である。(図3参照)

図2: 代表的なプライバシーに関する概念

概念	説明
データポータビリティ	企業が保有するデータから、消費者が本人のデータを引き出し、他サービスへ転用できるようにすること
プライバシー・バイ・デフォルト	企業によるサービス企画・開発の初期段階から、消費者のプライバシーを保護するようにサービス設計を行うこと
忘れられる権利	企業が保有するデータから、消費者が本人データの消去を要求することができる権利

図3: GDPRへの対応状況



GDPRは、違反時の高額な制裁金ばかりが話題になっているが、こうしたコンプライアンスプログラムの導入をきっかけとして、パーソナルデータの管理権限のあり方や関係するビジネスプロセスを前向きに見直す機会も実は与えている。データ駆動型社会において、消費者のパーソナルデータという重要な資源を取り逃さないためにも、こうした機会を前向きに捉える姿勢が重要だろう。

二つ目のアプローチ：パーソナルデータを提供したくなるインセンティブを個人へ与える

PwCやその他の機関が実施した各種調査の結果が物語っているように、消費者はより高度なセキュリティやプライバシー機能が得られるのであれば、少々値の張るサービスでも積極的に活用したいと考えている。また、総務省の調査によれば、日本の消費者の半数以上がパーソナルデータを「条件によっては提供してもよい」とも述べている³⁶。つま

り、消費者がパーソナルデータを提供する「対価」として、納得できるインセンティブを企業が提示できるかどうか、企業と消費者の「溝」を埋めるためのポイントといえるだろう。

パーソナルデータの利活用の事例をいくつか示そう。米国の企業では、消費者へインセンティブを付与する仕組みを整備することで、データの収集への抵抗感の解消に成功している。

例えば、米国のホテル向けサービスでは、宿泊客の同意取得の上で、宿泊施設のドア・照明・ミニバーの利用状況をモニターするIoT機器から施設内機器の不具合情報や宿泊客の行動ログを取り、分析している。これにより故障機器の早期修繕や人員配置、サービス構成などの見直しが可能になり、業務の効率化だけでなく、宿泊者の満足度の向上をあわせて実現している。

また、米国のある適応学習サービスでは、学習コンテンツを有する教育機関や提供事業者と連携し、生徒一人ひとりに対して個別にカスタマイズしたサービスを提供している。各生徒の取り組んだ問題、正誤情報、コンテンツを閲覧した時間などのデータを総合的に分析し、各生徒の学習習熟度に適合したオーダーメイドな学習サービスは既に1,300万人以上への提供実績を誇っている。

日本でも、既に生命保険会社が顧客のメリットに着目した商品を展開しはじめている。例えば運動量の増加や食生活の改善などのプライバシーデータの内容に応じて、保険料を安くする健康増進型保険商品はその典型であろう。今まで本人に

しか価値のなかったデータが商品の核を占め、商品やサービスの訴求力の主因となっている。

これらの事例に共通することは、消費者が自身のパーソナルデータを利用されることに伴うインセンティブ、つまり「対価」を得られる仕組みをサービスや商品のなかに具体的に組み込んでいることである。企業に自分のパーソナルデータを握られることに対する心理的なマイナス面と、提供されるサービスの中で得られる見返りを天秤にかけた際に、ポジティブな側面が勝っていれば、顧客が自分のパーソナルデータを預けてみようという動機づけに繋がる。

示唆2：プライバシー・バイ・デザインを実践する体制づくりを

「攻め」の個人情報管理手法

今やパーソナルデータを利活用し、サービスの質の向上を実現する商品・サービス開発の取り組みは、さまざまに進み始めている。その一方、企業における個人情報管理といえば、法務部門やコンプライアンス部門が主導して、国内外の個人情報保護規制に沿ったプライバシーポリシーを策定し、全部門に遵守を徹底するといったものが未だ多い状況である。例えば、年に一度のコンプライアンス研修で個人情報保護について教育する企業は多く存在する。

一方、実際に顧客などのパーソナルデータを大量に保有しているのは、営業部門やマーケティング部門などであり、さまざまな顧客の購買特性を分析したり、顧客とのコミュニケーションに活用した

りする。この際、現場担当者の感覚は、法律や会社のプライバシーポリシーに違反しない範囲で最大限データを活用して、なんとか業績を上げるために試行錯誤するというものが多いのではないだろうか。中には相当グレーな取り扱いをしているケースもあるかもしれないが、法務部門やコンプライアンス部門が、ビジネスの現場で日々起きていることを詳細に把握することは難しい。

前述のように、パーソナルデータの管理状況を顧客本人に開示しようとする、まず企業自身が社内のデータ管理状況を把握しなければならない。これは実際のところ容易ではない。多くの企業では、顧客データベースがあちこちに分散していたり、そこから抽出した部分的なデータが社員のPCにスプレッドシートとして保存されていたりと、乱雑で無秩序な状態が続いている。しかし、この状

態のまま、無理矢理データ活用を推進しようとする
と、どこかでプライバシー侵害が発生するか、そう
でなかったとしても、効果的にデータ活用ができな
い結果となってしまふ。

そこで重要なのが、「プライバシー・バイ・デザイン」である。「プライバシー・バイ・デザイン」とは、ビジネスプロセスやシステムを検討する際に、企画や設計などの初期段階から、データ利用を前提にプライバシー対策を織り込んでおくことである。従来型の個人情報管理が「守り」だけを意識したものだったのに対して、プライバシー・バイ・デザインに基づいた個人情報管理は、データ活用を促進するための基本概念でもあり、「攻め」の手法だと言ってよい。

プライバシー・バイ・デザインは、法務部門やコンプライアンス部門だけでは実現できない。サービス設計や収益を試算する事業企画部門、サービスを販売し顧客のパーソナルデータを入手する営業部門、パーソナルデータを分析しさらなる営業手法を検討するマーケティング部門、パーソナルデータを活用するための基盤を用意しデータの流れや変更ログを可視化するIT部門、パーソナルデータが決められた手続きに則って処理されているかを確認する内部監査部門など、さまざまな部門の関与が必要である。企業を挙げての総合的な体制づくりが成功のカギとなる。

図4: 「攻め」のプライバシー・バイ・デザイン

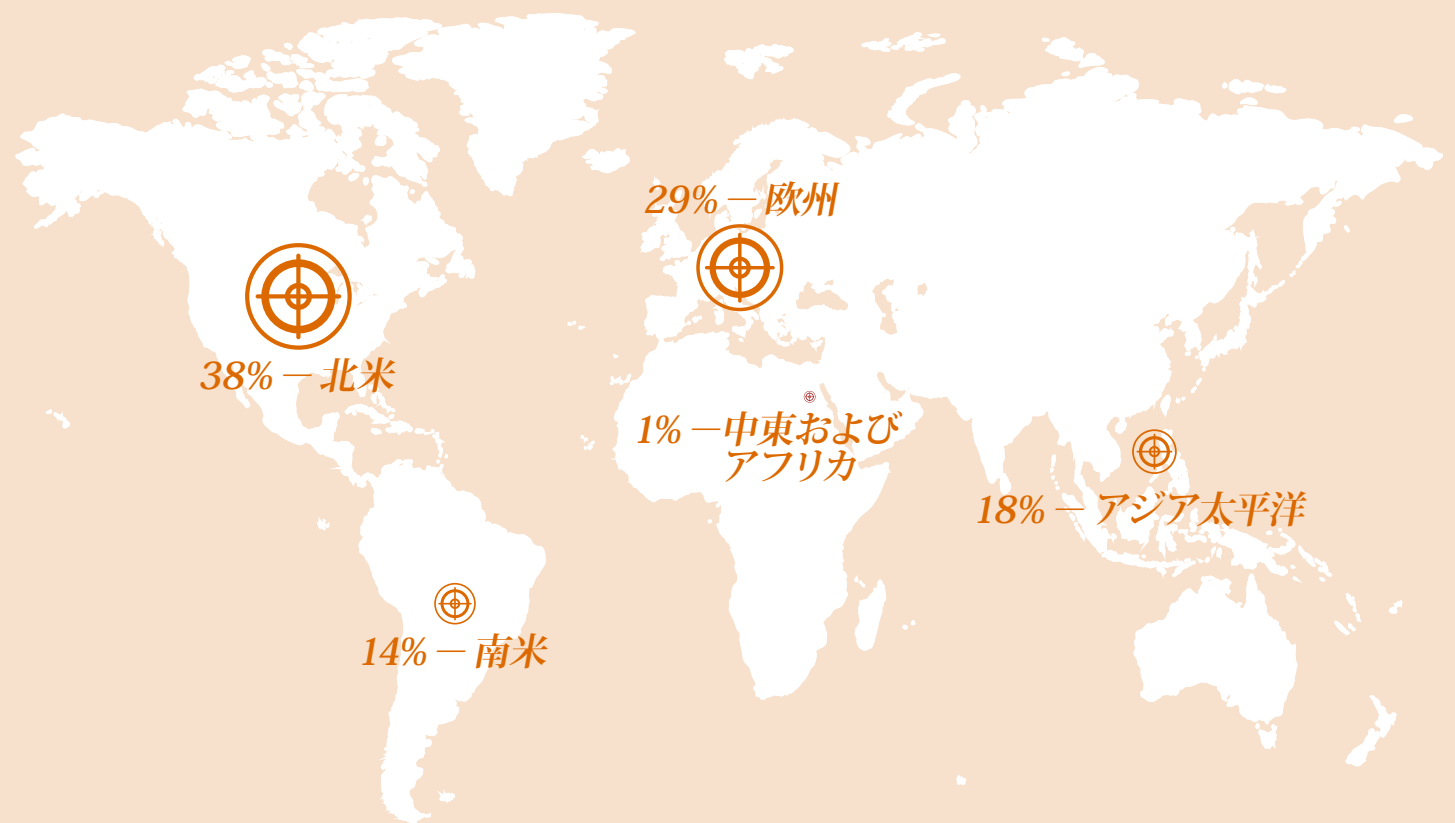


調査方法

グローバル情報セキュリティ調査 2018は、PwC、『CIO magazine』、および『CSO magazine』が実施した情報セキュリティに関する世界的な調査です。2017年4月24日から2017年5月26日までの期間において、『CIO magazine』および『CSO magazine』の読者および全世界のPwCクライアントに対して、電子メールによって調査への協力を依頼し、オンライン調査を実施しました。

本報告書で解説する調査結果は、122カ国にわたる9,500人以上の最高経営責任者(CEO)、最高財務責任者(CFO)、最高情報責任者(CIO)、最高情報セキュリティ責任者(CISO)、最高セキュリティ責任者(CSO)、副社長、ITおよび情報セキュリティ役員からの回答に基づいています。

回答者の地域別では、北米が38%、欧州が29%、アジア太平洋が18%、南米が14%、中東およびアフリカが1%です。



誤差は1%未満です。ここでは四捨五入した数値を使用しているため、数値の合計が100%にならない場合があります。本報告書の全ての図および図形は、調査結果に基づき作成したものです。

サイバーセキュリティおよびプライバシーに関するPwCのお問い合わせ先（国別）

オーストラリア

Richard Bergman

Partner

richard.bergman@au.pwc.com

Steve Ingram

Partner

steve.ingram@au.pwc.com

Andrew Gordon

Partner

andrew.n.gordon@pwc.com

Megan Haas

Partner

megan.haas@pwc.com

Robert Martin

Partner

robert.w.martin@pwc.com

オーストリア

Christian Kurz

Senior Manager

christian.kurz@pwc.com

ベルギー

Pascal Tops

Partner

pascal.tops@pwc.com

ブラジル

Edgar D'Andrea

Partner

edgar.dandrea@br.pwc.com

Eduardo Batista

Partner

eduardo.batista@br.pwc.com

カナダ

Sajith (Saj) Nair

Partner

s.nair@ca.pwc.com

David Craig

Partner

david.craig@pwc.com

Richard Wilson

Partner

richard.m.wilson@pwc.com

Justin Abel

Partner

justin.abel@pwc.com

Kartik Kannan

Partner

kartik.kannan@pwc.com

中国

Ramesh Moosa

Partner

ramesh.moosa@cn.pwc.com

Kenneth Wong

Partner

kenneth.ks.wong@hk.pwc.com

Kok Tin Gan

Partner

kok.t.gan@hk.pwc.com

Marin Ivezic

Partner

marin.ivezic@hk.pwc.com

Chun Yin Cheung

Partner

chun.yin.cheung@cn.pwc.com

Lisa Li

Partner

lisa.ra.li@cn.pwc.com

Samuel Sinn

Partner

samuel.sinn@cn.pwc.com

デンマーク

Christian Kjær

Partner

christian.x.kjaer@dk.pwc.com

Mads Nørgaard Madsen

Partner

mads.norgaard.madsen@dk.pwc.com

フランス

Philippe Trouchaud

Partner

philippe.trouchaud@fr.pwc.com

ドイツ

Derk Fischer

Partner

derk.fischer@pwc.com

インド

Sivarama Krishnan

Partner

sivarama.krishnan@in.pwc.com

インドネシア

Subianto Subianto

Partner

subianto.subianto@id.pwc.com

イスラエル

Rafael Maman

Partner

rafael.maman@il.pwc.com

イタリア

Fabio Merello

Partner

fabio.merello@it.pwc.com

日本

Yuji Hoshizawa

Partner

yuji.hoshizawa@pwc.com

Sean King

Partner

sean.c.king@pwc.com

Naoki Yamamoto

Partner

naoki.n.yamamoto@pwc.com

韓国

Soyoung Park

Partner

s.park@kr.pwc.com

ルクセンブルク

Vincent Villers

Partner

vincent.villers@lu.pwc.com

メキシコ

Fernando Román Sandoval

Partner

fernando.roman@mx.pwc.com

Yonathan Parada

Partner

yonathan.parada@mx.pwc.com

Juan Carlos Carrillo

Director

carlos.carrillo@mx.pwc.com

中東

Mike Maddison

Partner

mike.maddison@ae.pwc.com

オランダ

Gerwin Naber

Partner

gerwin.naber@nl.pwc.com

Otto Vermeulen

Partner

otto.vermeulen@nl.pwc.com

Bram van Tiel

Director

bram.van.tiel@nl.pwc.com

ニュージーランド

Adrian van Hest

Partner

adrian.p.van.hest@nz.pwc.com

ノルウェー

Lars Fjørtoft

Partner

lars.fjortoft@pwc.com

Eldar Lorezntzen Lillevik

Director

eldar.lillevik@pwc.com

ポーランド

Patryk Geborys

Senior Manager

patryk.geborys@pwc.com

Tomasz Sawiak

Senior Manager

tomasz.sawiak@pwc.com

Piotr Urban

Partner

piotr.urban@pwc.com

シンガポール

Tan Shong Ye

Partner

shong.ye.tan@sg.pwc.com

Jimmy Sng

Partner

jimmy.sng@sg.pwc.com

Paul O'Rourke

Partner

paul.m.orourke@sg.pwc.com

南アフリカ

Sidriaan de Villiers

Partner

sidriaan.de.villiers@za.pwc.com

Elmo Hildebrand

Director/Partner

elmo.hildebrand@za.pwc.com

Busisiwe Mathe

Partner/Director

busisiwe.mathe@za.pwc.com

スペイン

Javier Urtiaga Baonza

Partner

javier.urtiaga@es.pwc.com

Jesus Manuel Romero Bartolomé

Partner

jesus.romero.bartolome@es.pwc.com

Israel Hernández Ortiz

Partner

israel.hernandez.ortiz@es.pwc.com

スウェーデン

Martin Allen

Director

martin.allen@se.pwc.com

Rolf Rosenvinge

Partner

rolf.rosenvinge@se.pwc.com

スイス

Reto Haeni

Partner

reto.haeni@ch.pwc.com

トルコ

Burak Sadic

Director

burak.sadic@tr.pwc.com

英国

Zubin Randeria

Partner

zubin.randeria@pwc.com

Richard Horne

Partner

richard.horne@uk.pwc.com

Alex Petsopoulos

Partner

alex.petsopoulos@uk.pwc.com

Grant Waterfall

Partner

grant.r.waterfall@uk.pwc.com

米国

Sean Joyce

Principal

sean.joyce@pwc.com

Jay Cline

Principal

jay.cline@pwc.com

Joseph Nocera

Principal

joseph.nocera@pwc.com

Carolyn Holcomb

Partner

carolyn.c.holcomb@pwc.com

Joe Greene

Principal

joe.greene@pwc.com

Mark Lobel

Principal

mark.a.lobel@pwc.com

Prakash Venkata

Principal

prakash.venkata@pwc.com

Richard Kneeley

Managing Director

richard.j.kneeley@pwc.com

Shawn Connors

Principal

shawn.joseph.connors@pwc.com

www.pwc.com/gsis

www.pwc.com/cybersecurityandprivacy

Contributing author

Christopher Castelli

お問い合わせ先 (日本)

PwCコンサルティング合同会社

〒100-6921 東京都千代田区丸の内2-6-1
丸の内パークビルディング
03-6250-1200 (代表)

山本 直樹

パートナー

naoki.n.yamamoto@pwc.com

PwCサイバーサービス合同会社

〒100-0004 東京都千代田区大手町1-1-1
大手町パークビルディング
03-6212-9080 (代表)

星澤 裕二

パートナー

yuji.hoshizawa@pwc.com

PwCあらた有限責任監査法人

〒100-0004 東京都千代田区大手町1-1-1
大手町パークビルディング
03-6212-6800 (代表)

岸 泰弘

パートナー

yasuhiro.kishi@pwc.com

グローバル情報セキュリティ調査2018
日本版レポート執筆委員

PwCコンサルティング合同会社

道輪 和也

本川 友理

小林 啓将

PwCあらた有限責任監査法人

綾部 泰二

三澤 伴暁

江原 悠介

米山 善章

武谷 遼太

森澤 佳子

前川 初美

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwCあらた有限責任監査法人、PwC京都監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立して事業を行い、相互に連携をとりながら、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、法務のサービスをクライアントに提供しています。

PwCは、社会における信頼を築き、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界158カ国に及ぶグローバルネットワークに236,000人以上のスタッフを有し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細はwww.pwc.comをご覧ください。

本報告書は、PwCメンバーファームが2018年3月に発行した「Revitalizing privacy and trust in a data-driven world」を翻訳し、日本企業への示唆を追加したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。

電子版はこちらからダウンロードできます。 www.pwc.com/jp/gsis

オリジナル（英語版）はこちらからダウンロードできます。 <https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey/revitalizing-privacy-trust-in-data-driven-world.html>

日本語版発刊年月：2018年9月 管理番号：I201803-8