# デジタルトラストへの道

安全性、セキュリティ、信頼性、プライバシー、
データ倫理にいち早く取り組むデジタル企業が
将来の巨大企業となるだろう。
今からでも取り組む価値は十分にある。

pwc

www.pwc.com/jp

# Digital Trust Insights について

PwCのグローバル情報セキュリティ調査(GSISS)は20年間、サイバーリスク環境について解説するリソースとして参照されてきた。近年は、「情報セキュリティ」よりもデジタルリスク管理が重視されるようになってきている。サイバーセキュリティ、プライバシー、データ倫理がますます結び付くなか、企業に必要なのは、信頼できるデータと具体的なアドバイスが得られる拠り所だ。そこでPwCはGSISSをDigital Trust Insightsと改め、再始動する。新たな出発点となる本書では、将来の課題に対応できる人材、プロセス、テクノロジーを確実に準備するにはどうすればよいか考察する。

Sean Joyce
Principal, US Cybersecurity and Privacy Leader

データをデジタル経済の「血液」に例えるなら、デジタルトラスト、つまりセキュアなデジタル世界を構築するための人材、プロセス、テクノロジーの信頼度は「心臓」にあたる。企業、規制当局、消費者が、ビジネス、リスク管理、コンプライアンスの新たな課題に対応するために必要とするのは、その信頼を構築するための新しい仕組みだ。その重要性は、インターネット上での人々の不信拡大への懸念に関するフォーラムを国際連合が開催したという事実にも表れている[1]。『The Economist』誌のエッセイでは、2018年は「プライバシー法がようやくインターネットに追いつき始めた年として記憶されるだろう」と予測されていた[2]。2019年にデジタルトラストを構築するための新たなレガシーが誕生することが企業にとってどのような意味を持つのかを想像してみよう。PwCでは、2020年は企業がその基盤づくりに取り掛かる極めて重要な一年になると考えている。ネットワークでつながる世界に対し、安全性、セキュリティ、信頼性、プライバシー、データ倫理にいち早く取り組む姿勢を見せたデジタル企業が将来の巨大企業となるだろう。今からでも取り組む価値は十分にある。

第1回PwC Digital Trust Insights調査では、世界各地の3,000人のビジネスリーダーを対象とし、デジタルビジネス、リスク管理、コンプライアンスに関する課題に対応するための準備状況について調査した。その結果、人材、プロセス、テクノロジーに関して改善の余地のある点として10項目が特定された。根拠となった調査結果は、世界各国のあらゆる規模の企業の回答に基づいている。金融、ヘルスケア、製造業、小売・消費財、テクノロジー・メディア・テレコム(TMT)、電力・ガス・再生エネルギー・石油などの主要セクターの中堅および大企業も含まれている。また、企業にとってビジネスを再定義するのに役立つ機会となるように、具体的なアドバイスも提供している。

1 United Nations, Cybersecurity and Fake News to Dominate List of Concerns at Internet Governance Forum, October 2018.
2 The Economist, Toward defining privacy expectations in an age of oversharing, Aug. 16, 2018.

# 人材

## 将来の変革は人材から始まる

### 1. デジタル変革の出発点からセキュリティエキスパートを参加させる

世界のいたるところで企業のデジタル変革プロジェクトが進んでいる。企業は新しいテクノロジーを導入し、問題解決や独自エクスペリエンスの創出、ビジネスパフォーマンスの加速を目指している[3]。個人のデバイス、政府、企業、および産業機器間での接続が複雑に絡み合い、サイバーリスク、プライバシーリスクの急激な増大に拍車をかけていることは周知のとおりだ[4]。デジタル変革プロジェクトを実施している企業の調査回答者の10人に9人が、プロジェクトの構想と予算化の段階からセキュリティおよびプライバシー担当者を設置し、関連するリスクを予防的に管理していると答えている。しかし、プロジェクトの予算を含む計画の「開始時から完全に」予防的なリスク管理対策を組み込んでいるという回答は53%にすぎなかった[5]。この割合は、中堅企業および大企業の回答者のうち、金融、ヘルスケア、TMTの各セクターで比較的高く、小売・消費財セクターでは相対的に低かった。ただし、改善の機会は世界各地のどの企業にも残っている。

**91%**

の全社的なデジタル変革には、関係者としてセキュリティおよび／またはプライバシー担当者が含まれる

**53%**

のデジタル変革は、プロジェクトの予算を含む計画の「開始時から完全に」サイバーリスクとプライバシーリスクを予防的に管理している

出典：Fall 2018 Digital Trust Insights, PwC
集計ベース：全回答者数　3,000

3　回答者の半分以上（55%）が、自社が全社規模のデジタル変革プロジェクトに取り組んでいると答えている。このようなプロジェクトへの取り組みは、テクノロジー・メディア・テレコム（86%）、金融（81%）などの主要セクターで1億米ドル規模以上の企業においてより多く見られる。
4　European Political Strategy Centre, State of the Union 2018: Our Destiny in Our Hands, Sept. 13, 2018.
5　この割合は小規模企業（48%）、中堅企業（48%）でやや低く、大企業（63%）でやや高い。

## 中堅企業および大企業のうち「開始時から完全に」リスクが管理されていると主張している割合は、セクターによって異なる


q1060：現在、会社が全社規模のデジタル変換プロジェクトに取り組んでいる、と回答された方へ質問します。
サイバーリスクとプライバシーリスクの予防的管理は、プロジェクトの計画と予算にどの程度組み込まれていますか？

出典: Fall 2018 Digital Trust Insights, PwC
集計ベース: 全回答者数　3,000

### ビジネスリーダーに向けた具体的アドバイス

- デジタル変革プロジェクトの開始時からサイバーセキュリティおよびプライバシー担当者を参加させ、デジタル変革イニシアティブの設計、構築、持続に対応するのに適切なスキルを持っているか、または外部リソースが必要かを評価する。
- 類似する変革プロジェクトを既に経験した同業他社と情報を交換し、成功のためにどのようなスキルを整備したかを学ぶ。
- 主要テクノロジー企業の関係者と連絡を取り、変革に向けたさまざまな取り組みを参考にする。

## 2. 人材および経営陣を「アップグレード」する

適切なチームを配置しなければ、セキュリティ、プライバシー、倫理に関するリスク管理を行うことは至難の業だ。今回の調査により、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、最高プライバシー責任者、最高リスク責任者、最高データ責任者などの重要な役職を設置していない企業が多いことが判明している。

サイバーセキュリティ（39%）およびプライバシー（40%）の責任者が自社において特定されているかという点について「非常にそう思う」と選択した回答者は半数に満たない。サイバーセキュリティおよびプライバシーにかかわる人材が十分かどうかについて「非常にそう思う」と選択した回答者も同程度（38%）だ。サイバーセキュリティ、データプライバシー、データ利用ガバナンスといった最新および今後発生する法規制等の要求事項に対応するための組織構造や人材の準備が完全に整っているという回答者は1/3にすぎない。

### ビジネスリーダーに向けた具体的アドバイス

- 適切な役職と人材を配置し、責任を明確に定め、サイバーセキュリティ、プライバシー、データ倫理の課題に包括的に取り組む。
- 組織のリスク評価を実施し、不足している人材やスキルを把握して対応する。

## 3. 従業員の意識を向上させ、説明責任を明らかにする

サイバーセキュリティおよびプライバシーに関する外部関係者への説明責任の向上について、改善余地のある企業は多い。従業員のセキュリティ意識を啓発するためのプログラムがあるという回答は34%にとどまる。プライバシーポリシーおよびその実践に関する従業員のためのトレーニングが必要であると答えたのは31%にとどまる。

### ビジネスリーダーに向けた具体的アドバイス

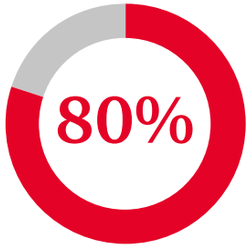
- ビジネス目標の達成を支援するため、サイバーセキュリティおよびプライバシーに関する従業員の意識向上を優先する。多忙な従業員がセキュリティについて煩わしさを感じないように配慮しつつ、のちにフィッシングやその他の高度な脅威に直面したとき、どう行動すべきなのかなど、十分に記憶に残るメッセージとする。
- IT資産とデータへのアクセスを管理する社内ポリシーを確立する。社内のあらゆるレベルでポリシーを適用し、サイバーセキュリティおよびプライバシーに関する説明責任を徹底させる。

プロセス

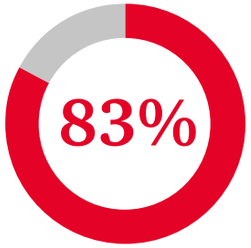
# プロセスの進化を重ね、新しい信頼の仕組みへ

## 4. 取締役会とのコミュニケーションを改善し、かかわりを強化する

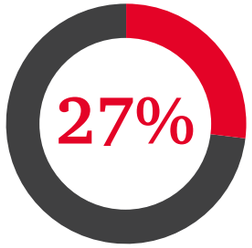
サイバーセキュリティおよびプライバシーに関して取締役会とのコミュニケーションを担当する回答者のほとんどは、サイバーセキュリティ（80%）とプライバシー（83%）に関する戦略を取締役会に提出していると述べている。しかし、そのような企業の多くがサイバーセキュリティおよびプライバシーに関する管理基準の社内報告について疑念や懸念を抱いている。取締役会がサイバーセキュリティおよびプライバシー管理基準について、十分な報告を受け取っているかどうかという点について「非常にそう思う」という回答は27%にすぎない[6]。




「取締役会にサイバーセキュリティ管理の戦略が提供されている」と選択した回答者の割合




「取締役会にプライバシー管理の戦略が提供されている」と選択した回答者の割合




取締役会がサイバーセキュリティおよびプライバシー管理基準について、十分な報告を受け取っているかどうかという点について「非常にそう思う」と選択した回答者の割合

出典: Fall 2018 Digital Trust Insights, PwC
集計ベース: 全回答者数　3,000

### ビジネスリーダーに向けた具体的アドバイス

- セキュリティプログラムの成熟度と管理策がどのように実行されているかによって、どのようなタイプの対策（実装方式、有効性／効率性、インパクト）が実施可能でパフォーマンスの向上に役立つかを把握する[7]。まず第一に、すぐに実施できる対策から始め、時間をかけてさらに高度な基準を追加する計画を立てる。また、基準はステークホルダーの要求を満たすものでなければならない。取締役会に求められるのは、セキュリティ活動がもたらすビジネスへの影響に関する基準だ。例えば、セキュリティ支出が全体のリスク状況に与える影響、セキュリティ事象への対応コスト、セキュリティへの取り組みが社会的信頼に及ぼす影響などがある。
- 脅威、外部委託先リスク、法規制などの外部要因が全体のリスク状況やリスク低減活動の有効性にどのように影響するかを取締役会などで説明する。
- 5つのヒントを参考に、CISOと取締役とのかかわりを強化する。

6 「ややそう思う」は27%、「どちらでもない」は17%、「あまりそう思わない」は29%である。
7 詳細については、National Institute of Standards and Technology, Special Publication 800-55 - Performance Measurement Guide for Information Security, July 2008 を参照。

## 5. セキュリティをビジネス目標と結び付ける

テクノロジーを活用したビジネスモデルの積極的な採用が進み、サイバーセキュリティ対策とビジネスのずれが拡大している。2019年、ビジネス目標と情報セキュリティ戦略の連携のための投資を計画していると答えた回答者は23%しかいない[8]。

### ビジネスリーダーに向けた具体的アドバイス

次のような領域に重点的に取り組むことがサイバーセキュリティ対策の向上につながる：

- サイバーセキュリティを新しい製品／サービスに組み込む。
- リスク、法規制、コンプライアンスの評価を実施する。
- ビジネス課題とサイバーセキュリティ管理策を連携させるサイバーセキュリティフレームワーク評価を実施する。
- サイバーセキュリティ戦略および計画を更新する。

## 6. データの取り扱いを中心として長期的な信頼を構築する

世界中でさまざまなデータが急増するなか、新たな収益化の方法を追求する企業も増えている。それにより多くの企業が倫理的に越えてはならない一線を越えてしまうリスクを抱えることになる。1億米ドル規模以上の企業で、「データガバナンス」、「データの利用および保存における透明性の確保」、「個人が自身のデータに対して持つコントロールの強化」に対して多額の投資を行っているという回答は半数程度だ。主要セクターの中堅および大企業の回答者で、自社にとって最も価値があり機密性の高いデジタル資産が識別されているかどうかという点について「非常にそう思う」という回答の割合は少ない[9]。当然ながら、そのような資産が識別されていることについて「非常にそう思う」と答えた回答者の割合（40%）は、識別のためのプログラムがあると答えた回答者（43%）の割合と近い。

### ビジネスリーダーに向けた具体的アドバイス

- 機密データの所在だけではなく、ビジネス価値、保護方法も把握するようなデータガバナンスプログラムを実行する。
- 作成、保存、使用、共有、アーカイブ、破棄といったデータライフサイクル全体にわたってリスクを管理する。

8　この割合は、TMT（37%）や製造業（32%）といった主要セクターの中堅および大企業の間でやや高い。
9　セクターによっては、肯定的な回答の割合が半数未満のこともある。また、「まあまあそう思う」と答えた回答者はかなりの数に上る。

# 7. サイバーレジリエンスを強化する

サイバーレジリエンスには、機敏な防御機能と回復機能の両方が含まれる。レジリエントなシステムは、サイバー攻撃を受けた場合も運用を継続でき、停止した場合も迅速に回復しやすい。システム運用の障害や停止は、たとえ短時間であったとしてもデータ漏洩より多額の経済的損失に直結するため、レジリエンスは不可欠だ。今後は企業が人工知能を使用してより多くのデータドリブン型意思決定を行うのに伴い、データ完全性を維持することの重要性は増す一方だ[10]。

サイバー攻撃やその他の破壊的事象に対してレジリエンスを大いに構築しているという回答者は、主要セクターの中堅および大企業において約半数にすぎない。自社がサイバー攻撃に対する抵抗力を十分にテストしているかについて、「非常にそう思う」と選択した回答者は半数に満たない。

## ビジネスリーダーに向けた具体的アドバイス

- 中核的なビジネスプラクティスにおけるリスクを考慮し、そのうえでリスク選好について理解を深める。最高財務責任者、最高運用責任者、最高情報責任者、セキュリティ、プライバシー、リスクを担当するその他のエグゼクティブなど、関係者によって考え方が異なる可能性を考慮に入れる。
- 最先端の各種アプローチを用いてサイバーレジリエンスに取り組む。これらのアプローチは、進化し続ける脅威環境において、企業がどの程度リスクを受容するかという懸念に取り組むための計画の策定および評価を含んでおり、高可用性、災害復旧、データ完全性を確保するためのテクノロジーインフラストラクチャの継続的なモニタリングも同様に含まれる。

10 Forrester, The Future Of Cybersecurity And Privacy: Defeat The Data Economy's Demons, April 12, 2018.『Forrester』誌に「AIの世界で企業とそのブランドを攻撃する最も簡単な方法は、データを汚染して不適切な意思決定へと誘導することだ」との記述がある。

# 8. 敵を知る

サイバー脅威への懸念は業種や企業規模によって異なる。例えば、2017年の中堅および大企業の回答者の懸念を見ると、金融セクターでは国家の支援を受けたハッカー(33%)が最も増加しており、小売・消費財セクターではサイバー犯罪(50%)に対する懸念に急増が見られる。TMTセクターでは産業スパイ(51%)が最大の懸念事項として挙げられている。しかし、自社のデジタル資産を狙う攻撃者を特定しているかという点について「非常にそう思う」と選択した回答者は全世界で31%にとどまる。

また、比較的大規模な企業では、小規模な企業と比べ、内部脅威*に対する懸念が強いことも分かっている。小売・消費財セクターの企業全体では、内部脅威への懸念はわずか9%程度の純増だ。しかし小売・消費財セクターの中でも中堅および大企業を見ると、この割合は30%を超えている。また、ヘルスケアセクターでは内部脅威の問題が突出しているというVerizonの『2018年度データ漏洩／侵害調査報告書(2018 Data Breach Investigation Report)』の調査結果にもかかわらず、本調査結果では、ヘルスケアを提供する企業における内部脅威への懸念は、緩やかな増加にとどまっている[11]。

## ビジネスリーダーに向けた具体的アドバイス

- 外部・内部脅威に関連したプログラム(セキュリティ活動の通知やリスク評価など)を活用し、セキュリティ対策への投資の意思決定を支援する。
- 保有するリスクと脅威の概観を把握し、洗い出した脅威情報をリスクシナリオへ適用する。さらに、脅威情報に関する施策と機能要件を整理し、その実現に向け最先端のツールを活用する。

*内部脅威:データへのアクセスを許可された人間が窃取・破壊などの侵害行為を資産に対して行うことを指す。

11 Verizon, 2018 Data Breach Investigation Report, 2018. この報告書では次のように述べられている。「ヘルスケアセクターは、(データ漏洩／侵害の点で)外部の脅威よりも内部の脅威の方が大きい唯一の業界であるという不名誉な地位に甘んじている。この芳しくない結果は、従業員による間違いも悪用も多い、というこの業界の事実と密接に関係している」。

# 9. コンプライアンスに予防的に取り組む

回答者はデジタルコンプライアンスおよび倫理に関する課題として、最新の法規制の進展への対応（41%）、現在の法規制の遵守（37%）、将来の法規制に対する準備（34%）を上位に挙げている。最近の例としては、ブラジルで可決されたデータ保護に関する法案がある。おそらく最もよく知られているのは、2018年5月に施行された欧州連合の一般データ保護規則（GDPR）だろう。しかし、1億米ドル規模以上の企業のうち、GDPRを遵守する準備が完全に整っていると回答した企業は半数未満だった。

米国では、2020年に施行されるカリフォルニア州消費者プライバシー法の遵守に向けた準備状況に関する自信の度合いには、セクターによってばらつきがあった。最も自信を示しているのはTMTセクター、最も自信のないのはヘルスケアセクターだった。中国では、自国のサイバーセキュリティ法に遵守する準備が完全にできているという回答が3/4を占めている。しかし、この回答の割合は他国でははるかに少ない。

## ビジネスリーダーに向けた具体的アドバイス

- 新たな法規制、規則、関連するガイダンスを把握することに、より重点を置く。
- コンプライアンスに個別に取り組むのではなく、統合されたアプローチを採用する。つまり、複数の管轄区域にまたがって事業を運営する企業は、最も高い水準に準拠する必要がある。このようなアプローチにおいては、あらゆる規則を総合的に見て境界を定めるべきだ。

テクノロジー

# 新しいテクノロジーに合わせた管理策の開発

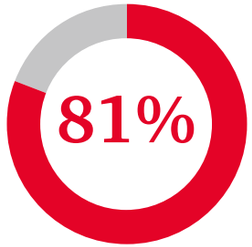
## 10. 新しいテクノロジーに遅れず対応する

今後10年でテクノロジーやデータは急成長を遂げ、サイバー空間、現実世界、仮想世界の壁は取り払われるだろう。世界的に見て、サイバーリスクおよびプライバシーリスク管理の複雑さも規模も徐々に増していく。デジタルデータおよびデバイスが重要インフラストラクチャや小売・消費財、車両、日常生活、さらには人体にも組み込まれるようになり、「物理、サイバー、仮想が融合した世界」が到来する[12]。モノのインターネット(IoT)[13]がつたのように縦横無尽に広がり、データ収集はかつてないほどの規模で行われるようになる。鳥が餌となる実を求めるように、このつたをつたってハッカーが横行するだろう。

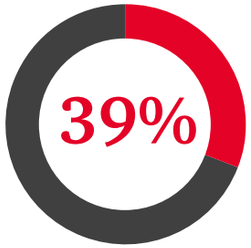
IoTが、少なくとも自社のビジネスの一部に重要な意味を持つ、と多くの回答者(81%)が選択していることは意外ではない。ただし、IoTの導入にあたり、セキュリティ、プライバシー、データ倫理といった「デジタルトラスト」における管理策を十分に構築しているかという点について「非常にそう思う」と選択した回答者は39%にとどまっている(「ややそう思う」と選択した回答者はさらに30%に限定される)。

また、今後12カ月間の投資計画の対象としてIoTセキュリティ保護策を挙げた回答者は30%だった[14]。IoTデバイスはこれまでにはない方法で現実世界とやりとりする。他の情報技術と異なり、これらのデバイスへのアクセス、管理、モニタリングは不可能であることが多く、場合によってはサイバーセキュリティおよびプライバシーのための追加の管理策が必要だ[15]。

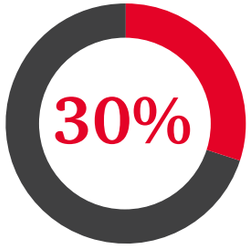
人工知能(AI)など、その他の新しいテクノロジーについても、デジタルトラストにおける管理策について自信を持つ回答者は少ない。




「IoTが、少なくとも自社のビジネスの一部に重要な意味を持つ」と選択した回答者の割合




「IoTの採用に十分なデジタルトラストを構築している」と選択した回答者の割合

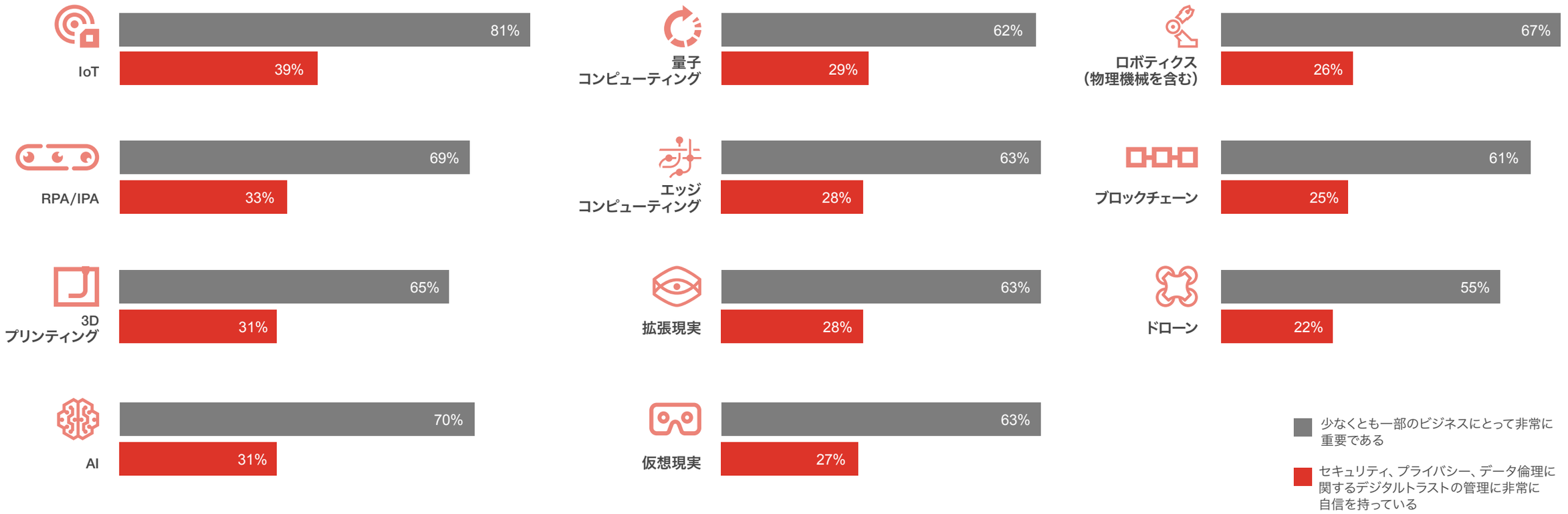



「今後12カ月間にIoTセキュリティへの投資を計画している」と選択した回答者の割合

出典: Fall 2018 Digital Trust Insights, PwC
集計ベース: 全回答者数　3,000

12 US National Security Telecommunications Advisory Committee, Report to the President on Emerging Technologies Strategic Vision, July 14, 2017.
13 モノのインターネット(IoT)は、センサー、ソフトウェア、ネットワーク接続性、演算能力を持つデバイス、車両、アプライアンスといった物理オブジェクトのネットワークであり、通常は人間の介入なしでデータの収集、交換、使用が可能だ。
14 ヘルスケアおよび小売・消費財の中堅および大企業の間では、セキュリティ投資の中でもIoTのセキュリティに関するものが最も優先順位が高い。
15 NIST, NISTIR 8228 (DRAFT): Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, September 2018.

# 多くの回答者は「新しいテクノロジーがビジネスにとって重要である」と述べているが「十分なデジタルトラストの管理策が整っている」と確信している人は少ない




q1010：将来、あなたのビジネスの成功にとって、次の技術がどの程度重要であると考えていますか？
q1030：あなたの会社が、次の技術の採用において十分な「デジタルトラスト」の管理を構築しているという自信はどの程度ありますか？

出典: Fall 2018 Digital Trust Insights, PwC
集計ベース: 全回答者数　3,000

回答者の70%（13ページ）が少なくともビジネスの一部においてAIが重要な意味を持つと答えているにもかかわらず、AIの導入にあたってデジタルトラストにおける管理策を十分に構築しているかという点で「非常に自信を持っている」との回答は31%のみだ。これらの管理策のうち、最も効果的なものは設計および実装フェーズで構築される[16]。AIには、感染の可能性の早期発見、車両の自動運転、サイバーセキュリティの迅速化および効率化など、さまざまな可能性がある[17]。2019年、セキュリティ保護策としてAIへの投資を計画しているという回答は全体のわずか22%にすぎない。AIへの投資の割合が高いのは、TMT（46%）、金融（40%）、その他の業界の中堅および大手企業だ。このような投資により、やがてCISOの役割の変化や[18]、他の方法では食い止められないようなAIを利用したサイバー攻撃[19]への対抗手段がもたらされる[20]。

PwCでは、今日のビジネスにおいて、リスク管理とコンプライアンスの課題が山積する中で、新しい信頼の仕組みの構築と実証に取り組む企業が、出遅れた競合他社を圧倒して将来のデジタル経済の行き先を定めることになる可能性が高いと考えている。今からでも取り組む価値は十分にある。

## ビジネスリーダーに向けた具体的アドバイス

- デジタルトラストのための管理策の開発、IoTやAIをはじめとする新しいテクノロジーに関するビジネス投資および目標を支援するためのセキュリティ予算を優先する。
- 新しいIoTセキュリティ調査を把握しておく。例えば、PwCがスポンサーとなっているカーネギーメロン大学のRisk and Regulatory Services Innovation Centerでは、IoTに関する新たな脅威モデリング、セキュリティ成熟度評価に関するフレームワークの開発および設計に取り組んでいる。このようなフレームワークによって、IoTセキュリティのためにどのような措置や管理策を実行するかについて、より適切な情報に基づいた意思決定が可能になる。
- ソフトウェアを開発するときには、開発と運用を統合するだけではなく、セキュリティもプロセスに組み込む（DevSecOps）。
- AIにはより強力なガバナンスと新しい運用モデルが必要になるという認識を持つ。AIに関する予測、AIに関する信頼と自信の獲得、AIのブラックボックスを開くことの意味に関するPwCの施策についてのインサイトも参考となる。
- 量子物理学における新しい研究はサイバーセキュリティとさらにその先にあるものに対して深遠な意味を持つ可能性があることを認識する[21]。準備に取り掛かるのに早すぎることはない。

16 PwC, Accelerating innovation: How to build trust and confidence in AI, 2017.

17 PwC, 2018 AI predictions, January 2018.

18 IDC, IDC FutureScape: Worldwide Security Products and Services 2018 Predictions, IDC #US43159217, October 2017. レポートでは「2020年までに、セキュリティテレメトリの50%が、機械学習と認知ソフトウェアの利用でより有用となり、記録的な速さで実用的かつインテリジェントなデータ変換を行えるようになる」と予測している。

19 New York Cyber Task Force, Building a Defensible Cyberspace, Sept. 28, 2017. 委員会は「2025年か2030年までに、スーパーコンピューターを利用した攻撃が地球上のあらゆる従来型サイバー防御を破ることは十分にあり得る。間に合うように対応できるのはスーパーコンピューターを利用した防御だけだ」と述べ、そのためには大手企業や政府により大きな権限を持たせる必要があると指摘している。

20 The New York Times, How an AI 'Cat-and-Mouse Game' Generates Believable Fake Photos, Jan. 3, 2018.

21 The Economist, Quantum computers will break the encryption that protects the internet, Oct. 20, 2018.

# PwC Cybersecurity and Privacy contacts

**Sean Joyce**

Principal, US Cybersecurity and Privacy Leader
+1 (703) 918 3528
sean.joyce@pwc.com

**Grant Waterfall**

Digital trust leader, PwC United Kingdom
+44 7711 445396
grant.r.waterfall@pwc.com

**Paul O'Rourke**

Asia-Pacific and Global Financial Services Cyber Leader, PwC Australia
+61 419 109 214
paul.orourke@pwc.com

**寄稿者：**
Christopher Castelli

## 日本のお問い合わせ先


**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


**www.pwc.com/jp**




本報告書は、PwCメンバーファームが2018年11月に発行した『The journey to digital trust』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/digitaltrustinsights
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/assets/journey-to-digital-trust.pdf
日本語版発刊年月：2019年2月　　管理番号：I201812-4