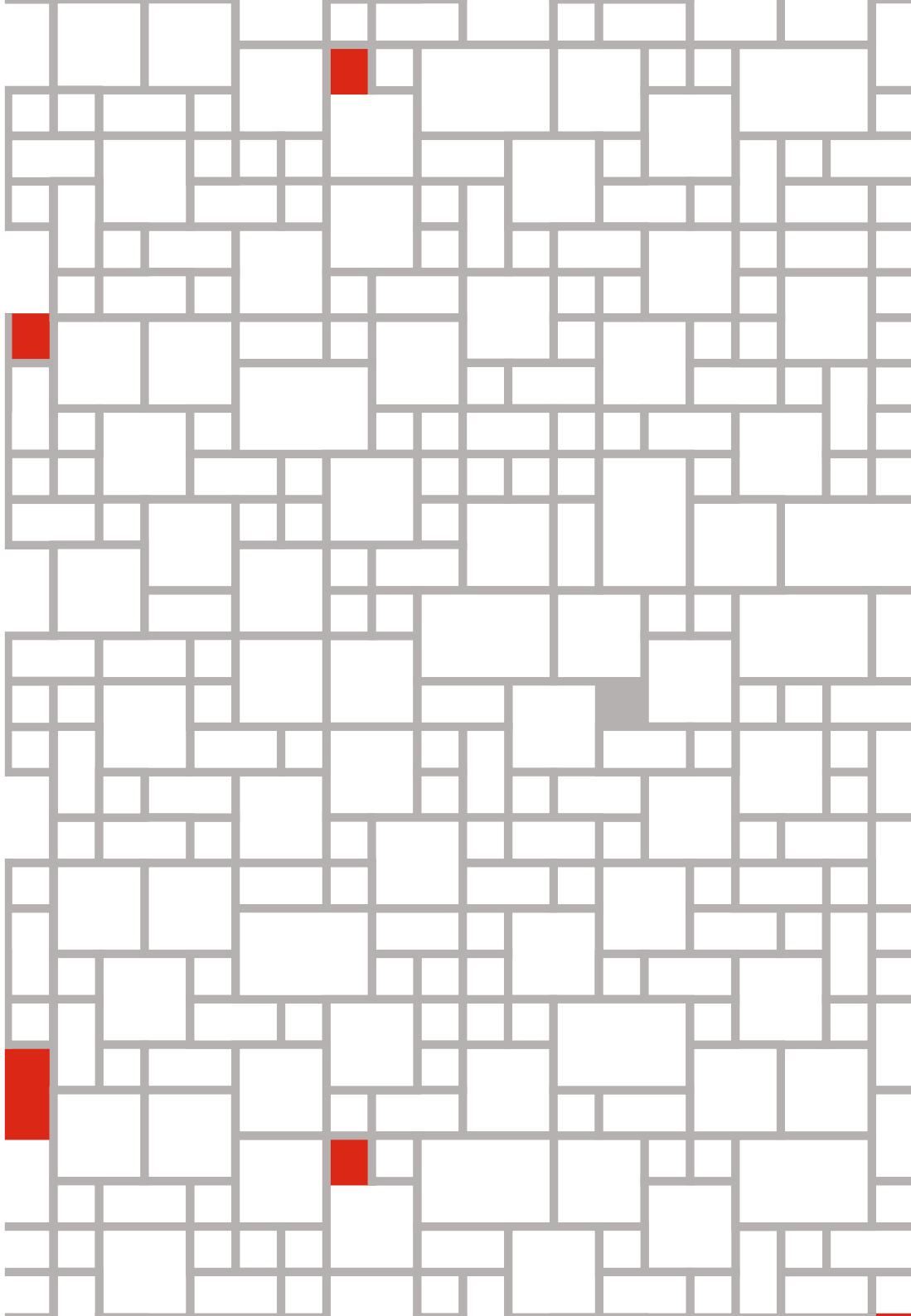
サイバーセキュリティの先進的企業は、新たな枠組みで事業の成長を推進

Digital Trust Insights

－日本企業への示唆－

pwc

www.pwc.com/jp

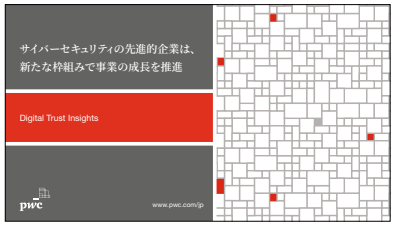


はじめに

IoTや5Gなどの革新的技術を取り込んだデジタルトランスフォーメーションが進む中で、かねてより存在するサイバーセキュリティリスクに加え、新たなリスクが顕在化し始めている。またこれに伴い、サイバーセキュリティ人材の不足が世界的に深刻化している。しかし、そのような状況下でもビジネス全体においてサイバーセキュリティを組み込むことで、デジタルトランスフォーメーションのメリットを実現し、競争優位を形成している、いわゆる先進的企業は存在している。

PwCは、世界中の企業幹部とITプロフェッショナル（回答者数3,145人）を対象にDigital Trust Insights調査を実施し、「サイバーセキュリティの先進企業は、新たな枠組みで事業の成長を推進」としてその結果を報告し、先進的企業の特徴と、その他企業との差異を明らかにしている。

本レポートでは、上記調査結果の中でも日本企業に焦点を当てて改めて分析を行い、日本企業固有の状況やグローバルとの差異、そしてそこから浮かび上がる実施すべき取り組みについて考察した結果を解説する。

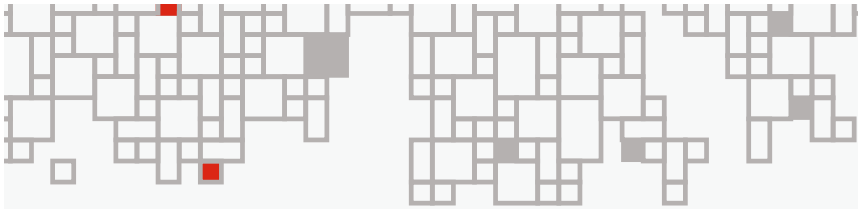


サイバーセキュリティの先進企業は、新たな枠組みで事業の成長を推進
https://www.pwc.com/jp/ja/knowledge/thoughtleadership/business-driven-cybersecurity.html

組織横断的なサイバーセキュリティリーダーの登用・育成

クラウド、IoT、AIといったさまざまなテクノロジーを活用したデジタルトランスフォーメーション（DX）が、企業におけるビジネス競争力の強化を後押ししている。新規市場・業界への参入や組織・ブランドの近代化を主眼にテクノロジー主導のDXに取り組む日本企業は、全体平均（80%）や主要各国と比較してやや下回るものの実に70%にのぼる。

カスタマーエクスペリエンスの改善やコスト削減などDXを通じて得ることが期待されるビジネスメリットは多岐にわたるが、その中でも売上拡大を期待する企業の割合が世界共通で最も高く、とりわけ日本企業の場合にはその割合が40%と、全体平均（27%）や主要各国と比較しても突出している。このことから、日本企業はDXの果たしうる役割を十分認知し、ビジネス環境が変化する中で事業拡大や市場競争力の強化を可能にするイネイブラーとして、DXに大いに期待しているといえる。



新規市場・業界への参入や
組織・ブランドの近代化を主眼に、
テクノロジー主導のDXに取り組む企業

80%
全体平均

70%
日本国内

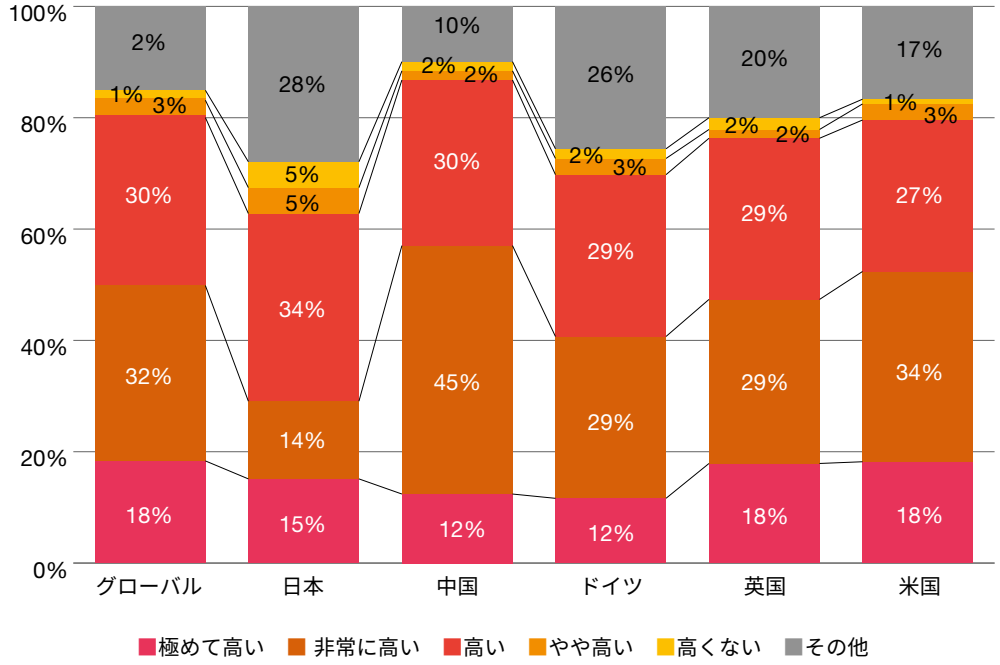
デジタルトランスフォーメーションにおけるリスクマネジメント

ビジネスのデジタル化がもたらすものは企業やサプライチェーン、顧客へのメリットだけには限られない。IoTデバイスを狙うサイバー攻撃に代表されるようなテクノロジーに起因する新たな脅威の登場や、EU GDPR（2018年5月施行）や改正割賦販売法（2018年6月施行）のような対応を余儀なくされる法規制が国内外で新設・改定されるなど、ビジネスのデジタル化に伴って企業を取り巻く外部環境にも大きな変化が生まれている。

その中で日本企業も海外企業と同様に、サイバーセキュリティ、ブランド・信用、法規制対応をDXにおける最大の懸念事項として上位に挙げており、リスクに対する企業の認知は一定レベルにあるものと考えられる。しかし、これら主要リスクの管理が自社の中で十分効果的に行われていると評価する日本企業はわずかに15%と、全体平均（30%）の半分にとどまり、また主要各国と比較してもその割合は低い傾向にある。

特に懸念すべき点は、自社のビジネスにおけるデジタルトラストの構築を重要視する企業の割合がやや小さい傾向にあるうえ、その緊急度を「極めて高い」、あるいは「高い」と評価する企業の割合においては、全体平均、主要各国と比較しても顕著に低い傾向にあることである。この傾向がみられた要因として、さまざまなリスクに対する温度感、そして対応の緊急度に対する認識に大きな差があることが考えられる（図表1）。

図表1　あなたの組織はデジタルトラストの構築をどのような緊急度で考えていますか。
（N：グローバル=3145、日本=86、中国=121、ドイツ=172、英国=190、米国=588）



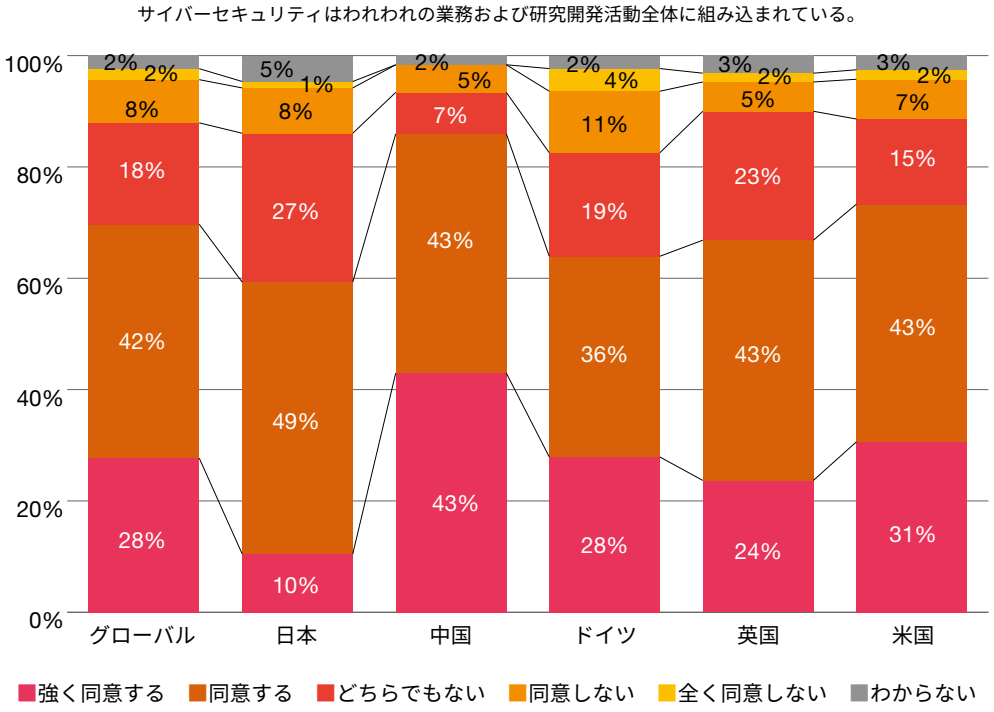
サイバーセキュリティと事業の関係性

DXにおける信頼構築を重要視する国内企業が少数派であることは、サイバーセキュリティと事業との関係について、戦略、リスクベース・アプローチ、統一性の3つの分野からも見て取ることができる。

戦略の分野を見てみると、自社の事業や製品開発にサイバーセキュリティが組み込まれているか否かについて、先進的企業の場合には65%、回答者全体でも27%が「強く同意する」と答える中、日本企業におけるその割合はわずか10%にとどまっている（図表2）。前項の内容と合わせると、日本でも多くの企業がDXにおけるリスクやデジタルトラスト構築の重要性に気づき始めてはいるものの、グローバルの企業に比べて、これを自社の戦略の一部として考え、実行レベルにまで落とし込めている日本企業は決して多くないことが浮き彫りになったといえる。

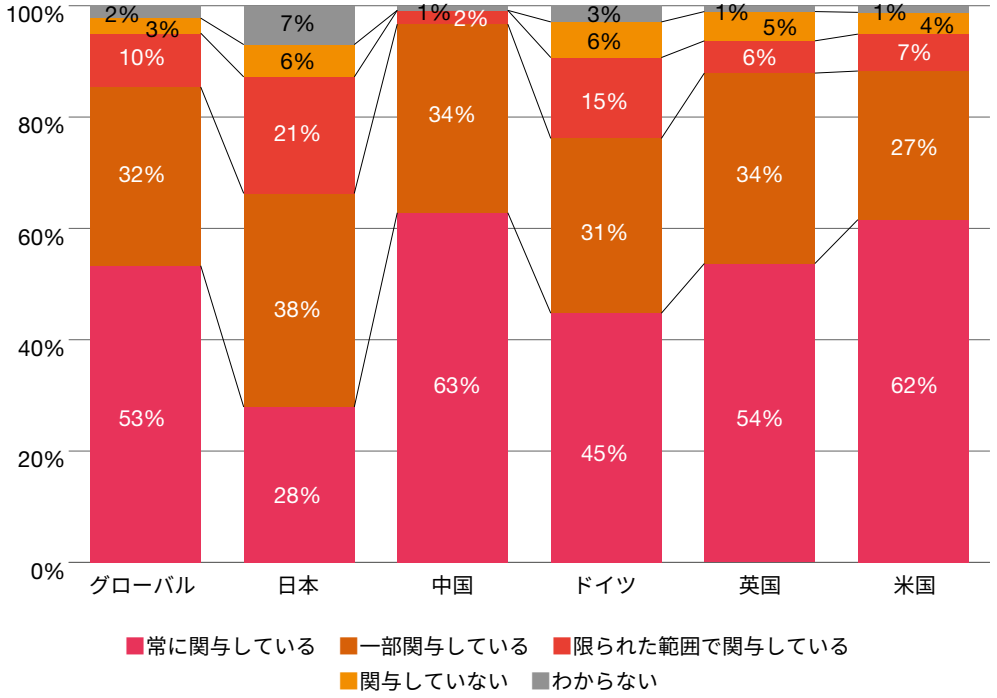
図表2　あなたの組織のサイバーセキュリティおよびサイバーセキュリティ部門に関する下記の文にどの程度同意できますか。

（N：グローバル=3145、日本=86、中国=121、ドイツ=172、英国=190、米国=588）



リスクベース・アプローチの分野を見てみると、先進的企業では89%、それ以外の企業では41%が、DXのリスク管理にサイバーセキュリティ部門が常に関与していると答えている一方、日本企業に至ってはその割合はわずか28%にとどまっている（図表3）。このことは、DXのリスク管理におけるサイバーセキュリティ部門の重要性の認知、そしてその結果としての影響力が日本企業においてはいまだグローバル水準に大きく後れを取っていることを示しており、企業組織全体での意識・仕組みの改革が必要であることを示唆している。

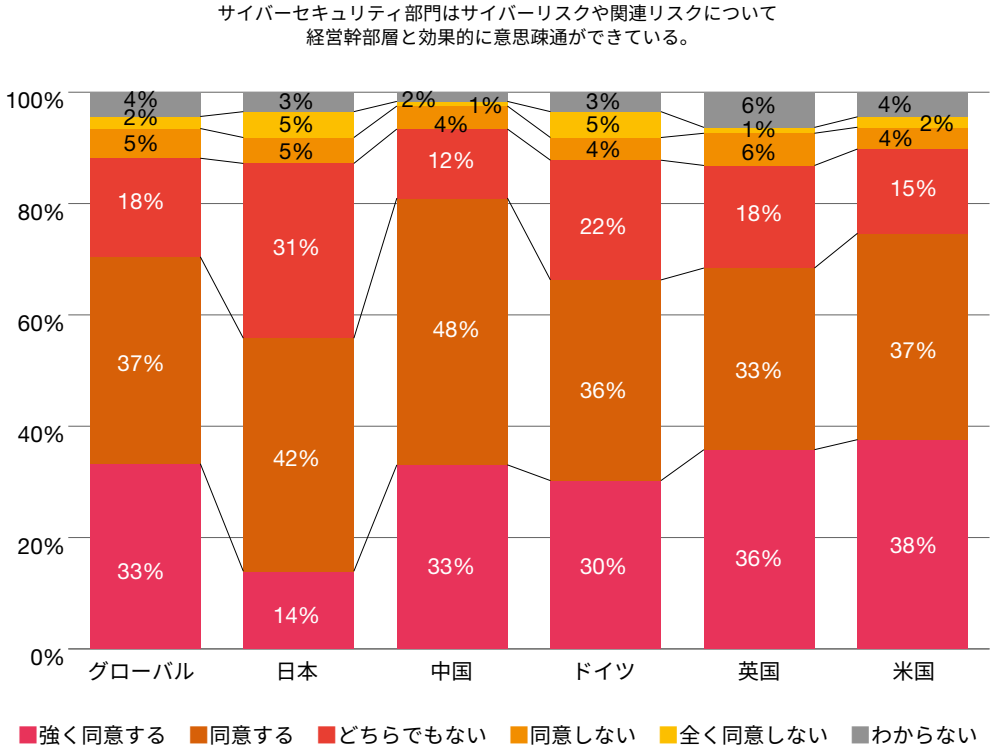
図表3　DXやデジタルに係る取り組みに由来するリスクに関してあなたの組織のサイバーセキュリティ部門はどの程度関与していますか。
（N：グローバル=3145、日本=86、中国=121、ドイツ=172、英国=190、米国=588）



統一性の分野においては、サイバーセキュリティ部門が経営幹部と十分に意思疎通を行い、中核事業における自社のリスク選好度を把握できているかという質問に対し、先進的企業の77%が、そしてそれ以外では22%が「強く同意する」と答えている中、日本企業の場合には25%と全体平均（35%）や主要各国の数値を下回る結果となっている。また、自社のサイバーセキュリティ部門が経営層や役員会とサイバーリスクについて効果的に意思疎通ができていると答えている割合も、13%と全体平均の33%を大きく下回っているうえ、サイバーセキュリティ部門から自社が享受している価値は「極めて高い」とする企業の割合も、日本企業においては全体平均や主要各国と比較しても大幅に小さい傾向にある（図表4）。

図表4　あなたの組織のサイバーセキュリティおよびサイバーセキュリティ部門に関する下記の文にどの程度同意できますか。

（N：グローバル=3145、日本=86、中国=121、ドイツ=172、英国=190、米国=588）



デジタルトランスフォーメーションにおける信頼の構築

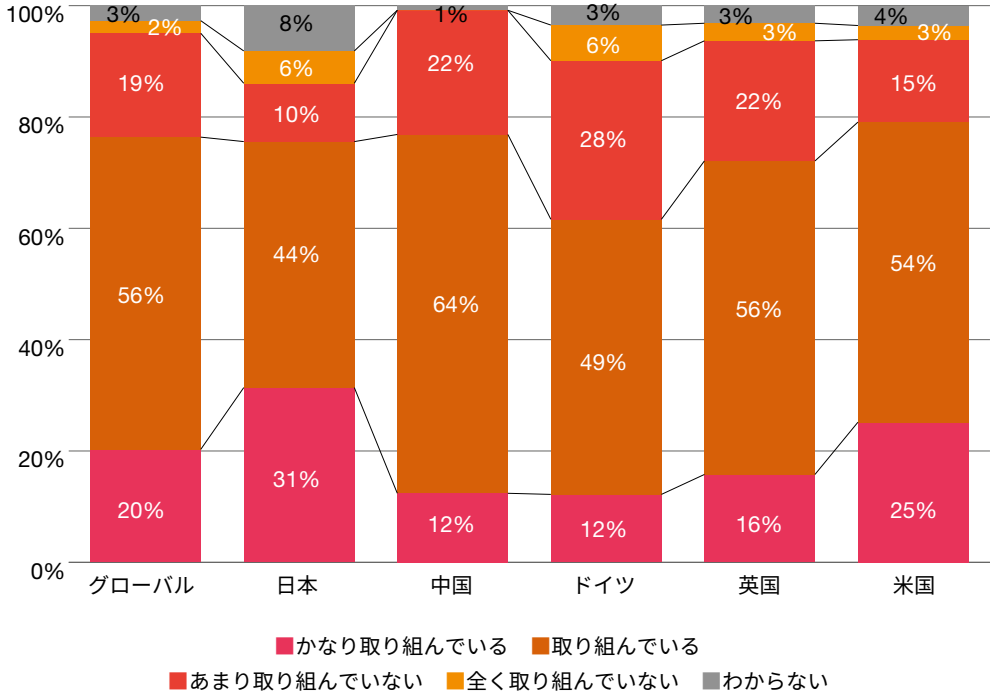
従来であれば、サイバーセキュリティは追加的措置とみなされることから、結果的に関連費用はコストとしてみなされ、積極的な財源の提供は行われてこなかった。しかし、企業における機密情報や個人情報の漏洩が後を絶たず、新しいテクノロジーや仕組みを悪用するサイバー攻撃が続々と登場する中で、DXの時代においては、後付けで行うサイバーセキュリティという発想自体が陳腐化しているといえる。

進化するテクノロジーとビジネスの融合によってもたらされるリスクを特定し解決策、緩和策を考案するうえで、サイバーセキュリティ部門が果たしうる役割は極めて重要なものであるはずである。ここまでの調査結果をもとに先進的企業とそれ以外の企業を比較すると、メリットとリスクのバランスを考慮したDXを実現するカギとして、サイバーセキュリティ部門がビジネス全般にどの程度組み込まれているかが重要であるということが示唆される。デジタル化をどのように推進していくかを計画段階から検討することに加え、サイバーセキュリティを含むリスクの管理を計画段階から組み込むことがポイントであるともいえる。すなわち、サイバーセキュリティを含むリスクマネジメントの視点が事業に組み込まれることこそが、企業がサイバーセキュリティ部門に担わせるべき役割なのである。

日本企業におけるサイバーセキュリティ部門の役割の変化にも明るい兆しがある。サイバーセキュリティ部門がビジネスニーズを満たすべくどれだけ変革をしているかを尋ねる問いに対しては、「かなり取り組んでいる」と回答する割合は日本企業が最も大きい（図表5）。

この結果はサイバーセキュリティ部門が果たしうるビジネス貢献への期待の表れともいえ、これがDXにおいても適用されることが期待される。その実現にあたっては、事業の中核にサイバーセキュリティ部門を組み込むことが重要であり、サイバーセキュリティ部門をビジネスゴールの達成を支援する重要な役割と位置付けることがカギである。

図表5　あなたの組織のサイバーセキュリティ部門はビジネスニーズに合わせた変革にどの程度取り組んでいますか。
（N：グローバル=3145、日本=86、中国=121、ドイツ=172、英国=190、米国=588）



当然ながら、セキュリティ人材を単に増やすことだけがサイバーセキュリティ強化の解決策にならないことと同様に、単にサイバーセキュリティ部門を事業に組み込むだけでは大きな効果は期待できない。ビジネスゴールを理解し、それをリスクマネジメントの視点でどのように支援するか、ということがサイバーセキュリティ部門には求められる。これを可能にするためには、経営層、役員会、事業部門などさまざまなファンクションとの意思疎通ができる、いわば組織横断的なマネジメント人材の登用やスキル開発が企業には求められる。

DXが業務効率化や売上拡大、新規事業参入など、さまざまなメリットをもたらす可能性を秘めていることは事実である。しかしそれと同時に、メリットとリスクのバランスをどのように最適化していくかという視点が重要であり、この視点こそがDXにおける企業の信頼、つまりデジタルトラストを実現する礎になるといえる。

関連コンテンツ

2019年 Vol.2
「2019年は地政学的サイバー活動が激化、CEOはレジリエンスが試される」

PwCは、グローバル情報セキュリティ調査（GSISS）として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ました。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います。そこでPwCはGSISSをDigital Trust Insightsと改めた調査を継続して実施しています。

調査結果をまとめた報告書を参照していただく以外に、地域別、業種別、企業規模別等のデータを抽出し、企業のデジタルリスク管理対策に関わるベンチマークデータとして活用していただくことが可能です。

2019年 Vol.1
「デジタルトラストへの道」

2018年 Vol.2
「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」

2018年 Vol.1
「サイバーショックに備え、デジタル社会を強化する」

2017年 Vol.3
「IoTの可能性を探る」

2017年 Vol.2
「スレットマネジメントの新たな可能性に向けて」

2017年 Vol.1
「先進的サイバーセキュリティおよびプライバシーの実現」

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）

外村 慶
パートナー
kei.tonomura@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）

綾部 泰二
パートナー
taiji.t.ayabe@pwc.com

www.pwc.com/jp

電子版はこちらからダウンロードできます。 www.pwc.com/jp/ja/knowledge/thoughtleadership.html
発刊年月：2019年12月　　管理番号：I201911-2