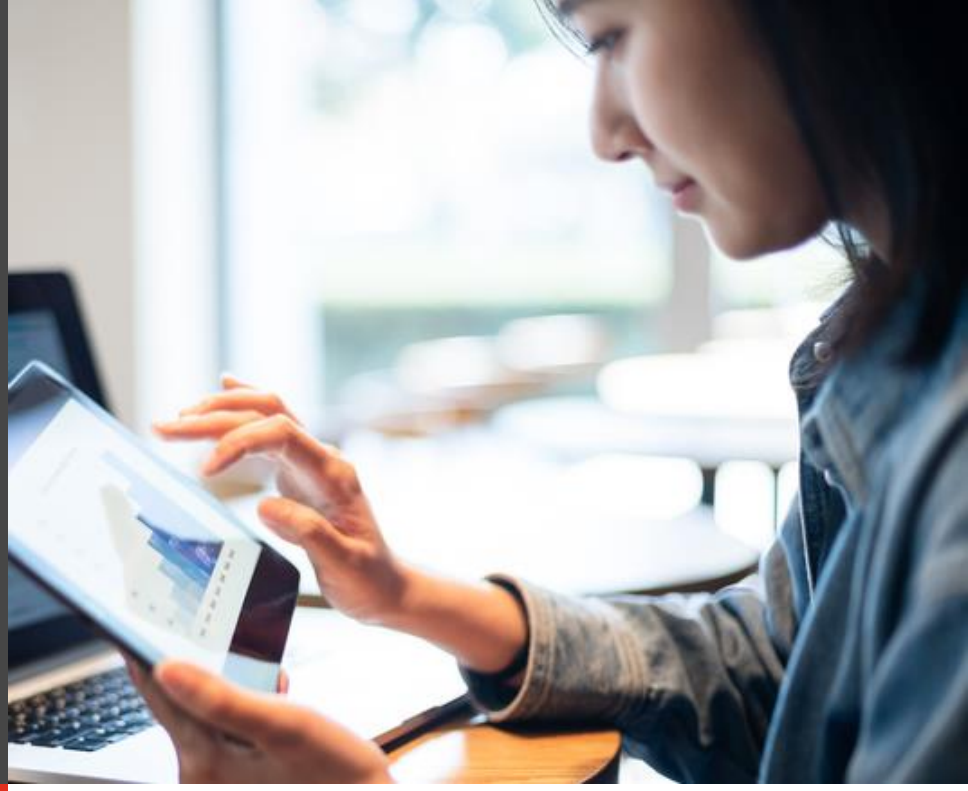
Digital Trust Insights

CEO向け示唆



2022/1/28

pwc

Global Digital Trust Insightsについて

PwCのGlobal Digital Trust Insightsでは、サイバーリスクについて20年以上継続して調査を実施している。今回は全世界の3,602名の経営層に調査を実施した。

3,602名
ビジネス・テクノロジー・セキュリティ分野の経営層
3,602名を対象として調査を実施

2021年7月-8月にかけて、
オンラインでのパネルインタビューを実施

66カ国 7地域で調査を実施:

- アフリカ
- アジア
- 中東
- 西欧
- 東欧
- 北米
- 中南米

調査テーマ

今後12ヵ月間に組織内のサイバーセキュリティを向上させるための課題と機会について

The key question

世界の注目、投資がサイバーに集中する中、経営層は変化をもたらすために何を行い、将来に向けてどのような目標を掲げているか？

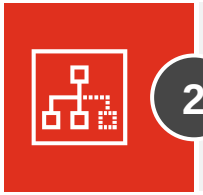
Global Digital Trust Insights 2022の調査結果

2022年のDigital Trust Insightsの主な調査結果となる4つのテーマを以下に示す。

1

CEOがどのように企業のサイバーセキュリティに変化をもたらすことができるか。

- 「わかりやすくセキュアであること」をビジネスのスローガンに



2

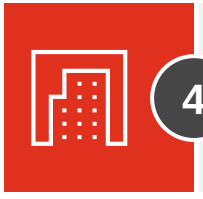
組織が複雑すぎてセキュリティを確保しにくくなっていないか。

- シンプルであること、スリム化することについて慎重に検討する

3

ビジネスにとって最も重要なリスクから企業を保護できているかを どのように判断するか。

- 信頼できるデータを使用してリスクを評価し、機会を実現する



4

サードパーティとサプライチェーンのリスクをどの程度把握しているか。

- ビジネス関係におけるリスクを隠す大きな死角を減らす

セキュリティ領域のポテンシャルを最大限に発揮するための「4つのP」

セキュリティ領域で最大限にポテンシャルを発揮している企業は以下の「4つのP」を実践し、高い成果を挙げている。

Principle（原則）

CEOは、セキュリティとプライバシーをビジネス上の必須事項として確立する、明確な基本原則を示す必要がある。

People（人材）

適切なリーダーを任命し、CISOやセキュリティチームがビジネスチームとつながるよう配慮する必要がある。従業員は、ビジネスにおいて「合理的で必要最低限の複雑性」を構築しながら、スリム化を推進することができる。

Prioritization（優先順位の決定）

デジタル化への積極性の高まりから、リスクは絶えず変化している。データとインテリジェンスを活用し、継続的にリスクを測定する必要がある。

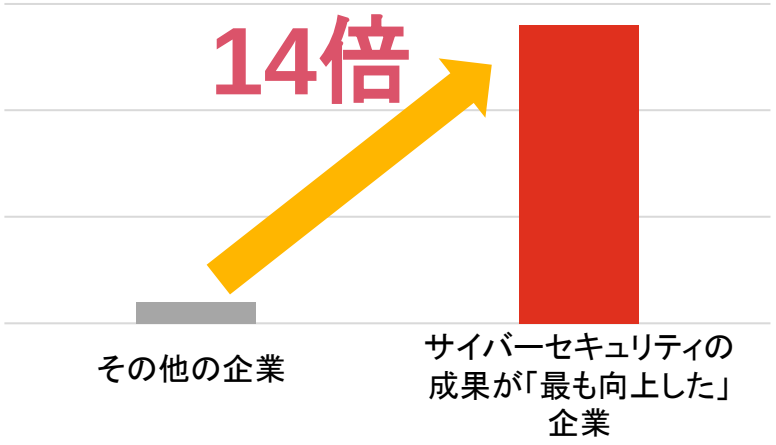
Perception（知覚）

知覚できないものを保護することはできない。
取引先やサプライチェーンにおける死角を明らかにする必要がある。

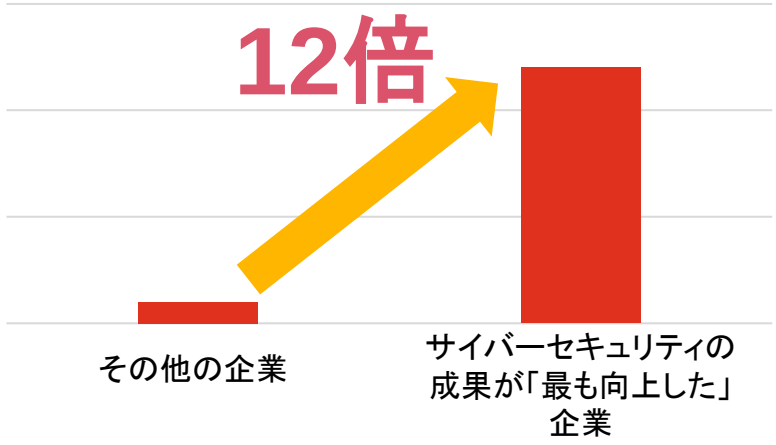
過去1年でサイバーセキュリティの成果が「最も向上した」企業の傾向

サイバーセキュリティの成果が「最も向上した」企業は、CEOがサイバーセキュリティに関して強力なサポートを提供している割合が高い。また、CEO以外の幹部からも同様の回答が得られている傾向にある。

CEOが「CEO自身がサイバーセキュリティの幅広い分野にわたり強力なサポートを提供している」と回答した割合



CEO以外の幹部が「CEOからサイバーセキュリティ分野の強力なサポートが得られている」と回答した割合



組織の責任者として、CEO自らが積極的にサイバーセキュリティへのサポートを提供している企業は、サイバーセキュリティの取り組みの成果が向上している

出典：2022 Global Digital Trust Insights Survey（PwC）

CEOのサイバーセキュリティの関与状況に関してCEOと非CEOで認識に相違がある

■ CEOがどのような場合にサイバーセキュリティに関与しているか（ランキング形式）

		CEOの見解	非CEOの見解
受動的関与	社内で大規模なサイバー侵害／攻撃が発生した後	3	1
	業界で大規模なサイバー侵害／攻撃が発生した後	5	6
	サイバーインシデントの報告、注意が必要な事項、または強制措置について規制当局から企業に連絡があったとき	2	2
積極的関与	取締役会レベルでサイバーセキュリティの重要指標について議論するとき	7	3
	M&A活動がサイバーセキュリティやプライバシーに及ぼす影響について議論するとき	8	8
	オペレーションモデルの変更に伴うサイバーセキュリティやプライバシーへの影響について議論するとき	1	5
戦略的関与	新戦略がサイバーセキュリティやプライバシーに及ぼす影響について議論するとき	6	7
	将来の戦略がサイバーセキュリティやプライバシーに及ぼす影響について議論するとき	4	4

CEOは、自身が「積極的にセキュリティに関与している」と認識している。
一方で非CEOは、「CEOはサイバーセキュリティに対し受動的である」と認識している。

出典：2022 Global Digital Trust Insights Survey（PwC）

グローバルと日本では、2030年を見据えたサイバーセキュリティの課題感に差異がある

■ 2030年までに、実現すべきサイバーセキュリティ分野の変化（ランキング形式・上位抜粋）

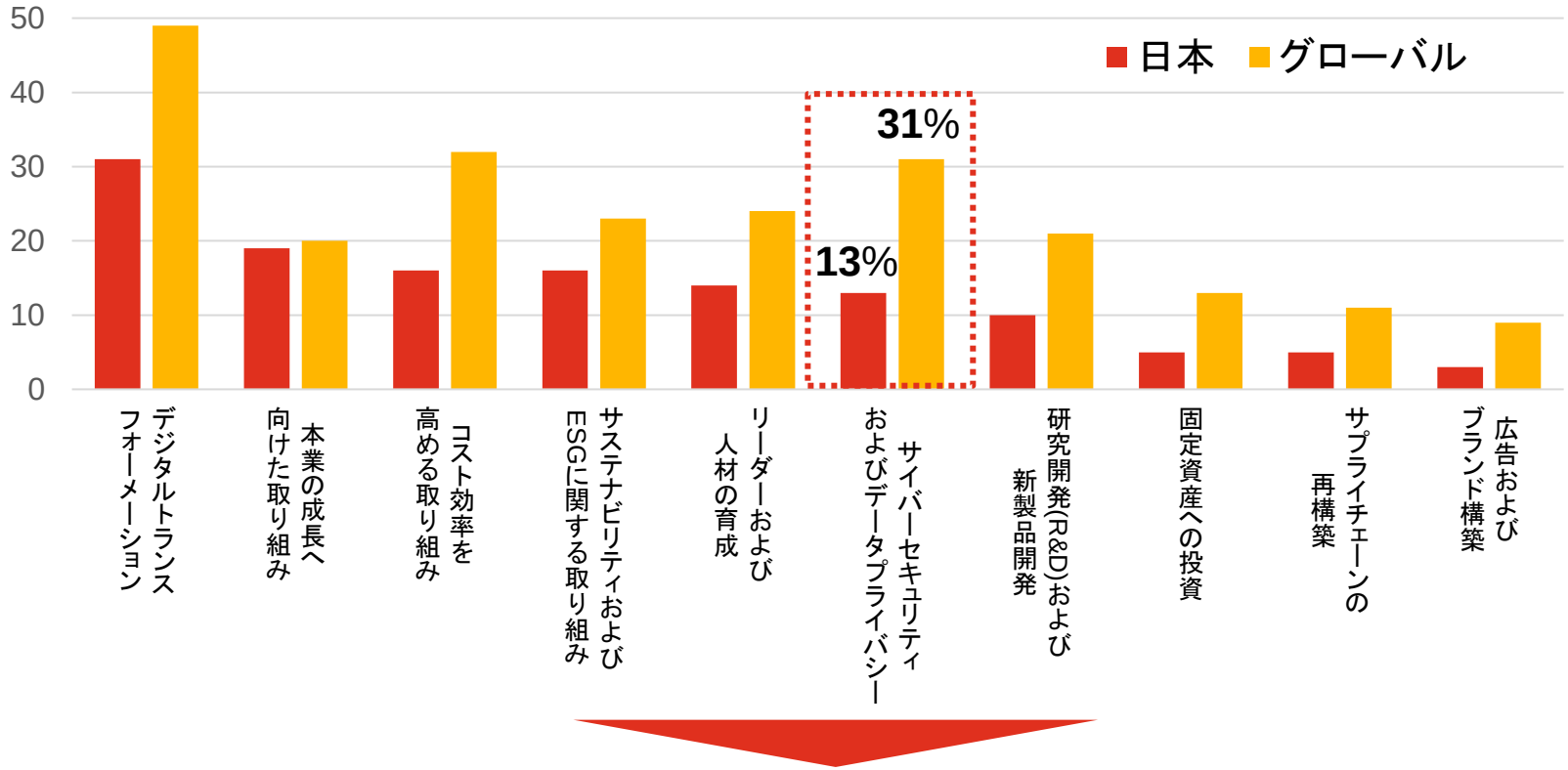
	2030年までに実現すべき変化の内容	グローバルの優先順位	日本の優先順位
実現すべき変化	経営層が義務と説明責任をより果たせるよう、サイバーセキュリティのビジネス影響に関して理解を促進する	1	5
	サイバーディフェンスを向上させ、よりシンプルにするブレークスルーを発見する	2	4
	基本的なサイバーセキュリティの実践に対する組織の責任・説明力を強化する基盤を構築する	3	1
	サイバーセキュリティとGRC、ERM、危機管理のフレームワークを融合する	8	2
	人材不足を解消する為に、安定した人材パイプラインを構築する	9	3

グローバルでは、サイバーセキュリティが経営層レベルでの課題として認識されている一方、日本では基本的なセキュリティ基盤の構築が課題となっている。

出典：2022 Global Digital Trust Insights Survey（PwC）

今後3年間の各分野への長期投資割合の比較結果

■ 今後3年間で「下記分野の長期投資割合を10%以上増加する予定」と回答したCEOの割合



日本はグローバルと比較し、サイバーセキュリティへの投資意識（投資の優先度）が低い傾向にあり、重要な課題としての認識が十分ではない状況である。

出典：第24回世界CEO意識調査（PwC）

サイバーセキュリティは経営層全体の重要課題として取り組むことが重要

【サイバーセキュリティを取り巻く動向（外的要因）】

- GDPR・中国サイバーセキュリティ関連法、国内重要インフラに対する規制など、サイバーセキュリティ関連法規の整備が世界的に進んでおり、単なる技術的な課題ではなく、安全保障上の問題となっている（対応できなければ、全社のビジネスに影響を及ぼす）。
- 世界的に要求の高まっている領域として、機関投資家も企業のサイバーセキュリティの取り組みを厳しく評価している。

【総論】

組織の責任者であり危機管理の責任者でもあるCEOが、平時からサイバーセキュリティにおいてもリーダーシップを取る必要がある（当然、有事にもリーダーシップを取って判断する必要がある）

【Next action】

- 取締役会や経営会議などで、サイバーセキュリティを重要課題として議論する。
- サイバーセキュリティのビジネス影響に関して議論できるよう、経営層がサイバーセキュリティの重要性を理解する。
- セキュリティ対策やリスク認識に関して、IR報告書などで積極的に情報開示する。
- 経営層自らが、規制当局やステークホルダに対して、サイバーセキュリティの主要なリスクや対応状況・方針に関して報告できる状態にする。

Thank you

pwc.com