Digital Trust Insights 2024

日本企業向け示唆

2024年4月

pwc

www.pwc.com/jp

Global Digital Trust Insightsとは

**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（2024年）は全世界の3,876名の経営層に対して調査を実施した。**

ビジネス・テクノロジー・セキュリティ分野の
経営層 3,876名を対象として調査を実施

2023年5月～7月にかけて、オンラインでの
パネルインタビューを実施

71カ国　7地域で調査を実施:

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

調査テーマ

今後12～18カ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（2024）:

セキュリティに対する施策や規制対応について、経営層はビジネスと同じくらい革新的に、
取り組めているのだろうか？

Digital Trust Insights 2024概要

サイバーセキュリティは4つの大きな変化に直面しており、2024年は転換点となる可能性がある。
経営陣（C-suite）は組織のセキュリティ確保において、変化に対応できるよう革新的に取り組むことが求められる。

2024年にサイバーセキュリティが迎える大きな変化

1 最新テクノロジーに対する投資の強化

コスト削減が求められ、またマクロ経済に不透明感が増す状況下で、CxOはテクノロジー・インフラストラクチャーと投資の近代化および強化を主張するだろう。

2 国家レベルでのサイバーディフェンス

ハイブリッドサイバー脅威が台頭し、スパイ行為とサイバー犯罪の境界線が曖昧になることで、サイバーディフェンスが国家安全保障分野に完全に組み込まれるだろう。

3 生成AIがもたらす脅威と防御の可能性

画期的な新技術である生成AIは、新たな脅威をもたらすと同時に、サイバーディフェンスに前例のない可能性をもたらすだろう。

4 規制強化による影響

サイバーセキュリティ・インシデントとリスク管理の開示強化を求める規制によって、透明性の向上と協力の強化が、新たな段階に突入する可能性があるだろう。

出所：2024 Global Digital Trust Insights Survey（PwC）

1

変化する規制の影響と組織内の認識乖離

増加するデジタル分野の法令とガイドラインへの対応が急務に

近年、各国においてデジタル分野の法令・ガイドラインが急増している。そのため、グローバル展開する日本企業は、準拠すべき法令・ガイドラインを把握し、組織単位で遵守に向けた統制を図る必要がある。

グローバル展開する日本企業が対応すべき法令・ガイドライン一例

84

グローバル展開する日本企業が対応すべき法令・ガイドラインは80超に及ぶ（2023年11月現在）。

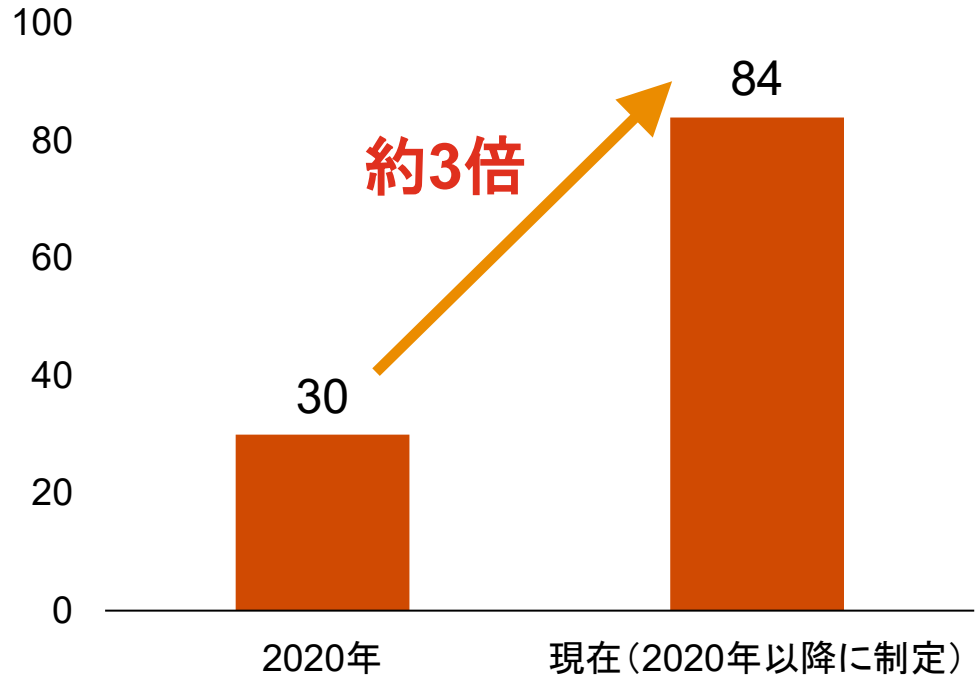
サイバーセキュリティ・プライバシーなどに関して、展開先国での遵守違反を起こさないよう、内容の把握と組織単位での統制強化が重要となる。

主要な法令・ガイドラインのカテゴリ

- AI
- サイバーセキュリティ
- IoT
- プライバシー

出所: 各国・地域の公的情報よりPwC作成

グローバル展開する日本企業が対応すべき法令・ガイドライン数の推移

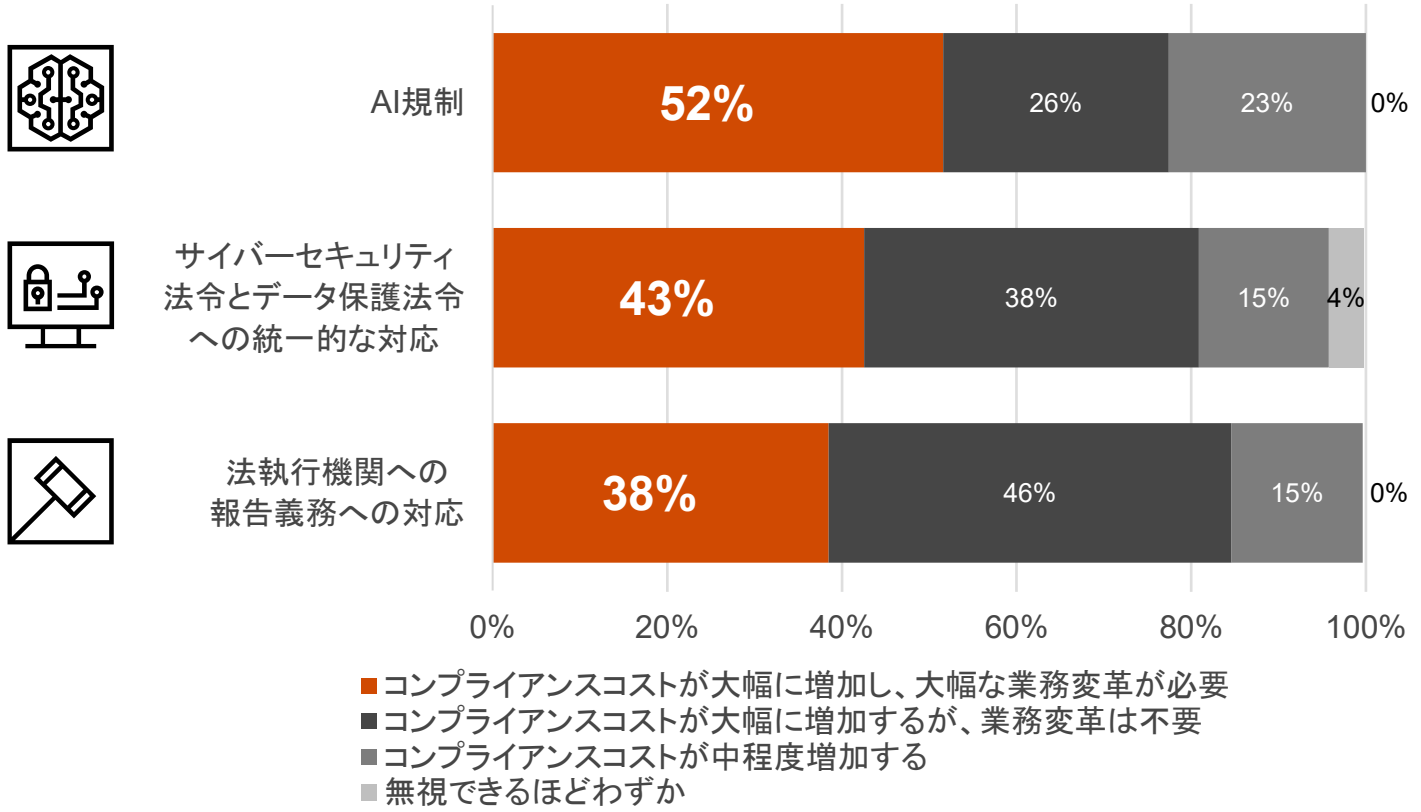


出所：「生成AIを巡る米欧中の規制動向最前線 生成AIを成長につなげる新たな企業統治のモデルとは」（PwC、2023年8月）
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/generative-ai-regulation06.html

組織のビジネスモデル変革を迫る、デジタル分野の規制

デジタル分野の法規制の変化により、「大幅なコンプライアンスコスト増加や業務改革に迫られている」と多くの日本企業の経営層が認識していることが判明。特に、AI規制は組織に与える影響が甚大である。

規制の変化が組織に与える影響



出所：2024 Global Digital Insights Survey（PwC）

企業が迫られる対応

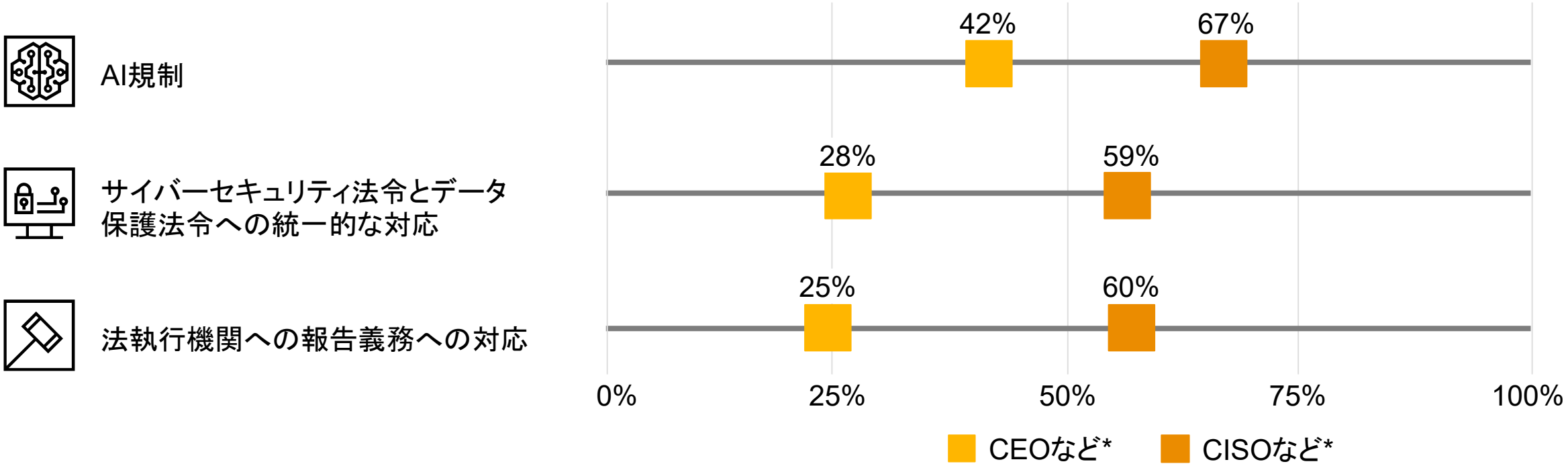
- ✓ **9割以上**の回答者が、規制の変化に対応するには**コンプライアンスコストを要する**と回答
- ✓ 特に**AI規制**は懸念されており、回答者の**半数以上**が**業務改革対応が必要**と回答

法規制が急増し、また変化し続けることで、ビジネスも変革を迫られ始めている。企業は、規制の変化をプロアクティブに把握し、規制が及ぼす影響の範囲と大きさを継続的に評価しなければならない。

規制の影響に関する情報格差が生む、組織内の認識の乖離

デジタル分野の法規制が与える組織への影響について、セキュリティリーダーであるCISOに比べて、ビジネスリーダーであるCEOは過小評価する傾向にある。背景として、CEOが影響を正確に把握できていない可能性が考えられる。

変化する規制の影響に対するCISOとCEOの認識の差



※コンプライアンスコストが大幅に増加し、大幅な業務改革が必要と答えた割合

*CISOなど：CDO, Chief Digital Officer, CIO, CIRO, CISO, Chief Privacy Officer, CSO

*CEOなど： CEO, President, Managing Director, Board Member, CAE, CCO, Head of Compliance, Chief Ethics and Compliance Officer, Chief Counsel / General Counsel / Chief Legal Officer / Senior Counsel, CFO, Chief Innovation Officer, CMO, COO

出所：2024 Global Digital Insights Survey（PwC）

組織内の認識乖離に潜むコンプライアンスリスク

デジタル分野の法令には、専門用語を用いて技術的実装を求める難解なものもあるため、他の法令と比べてビジネスリーダーに伝わる情報に格差が生じやすい。法令要件に正確に対応できない場合、コンプライアンス問題となりかねないため、ビジネス視点でセキュリティ業務を担う人材が求められる。

企業が求められる対応

企業はコンプライアンスリスクを低減するため、以下の点を正確に把握する必要がある。

- ✓ **法令がどのような要件を求めているのか**
- ✓ **法令への対応コストはどれほど必要か**
- ✓ **自社ビジネスのどの部分が法令に抵触する可能性があるのか**

企業が解消すべき課題

01 法令が専門家向けの言葉で表現されている

デジタル分野の法令は専門用語が用いられている上、技術的な実装を求めるものも多いため、ビジネスリーダーが内容を理解し、必要コストを正確に把握することが困難である。

02 ビジネスへの影響の大きさを把握できていない

セキュリティリーダーにとっては、法令対応がどの程度、企業活動に影響を及ぼすのか、特にコスト面で判断することが難しい。

03 テック・ビジネス間のコミュニケーションが不足している

規制の影響に対する、テック-ビジネス間の情報格差を解消するため、セキュリティリーダーが積極的に、分かりやすい言葉でビジネスリーダーに働きかける必要がある。

2

組織内のコンプライアンス リスクを解消する BISOの存在

ビジネス視点でセキュリティ業務を担うBISOとは

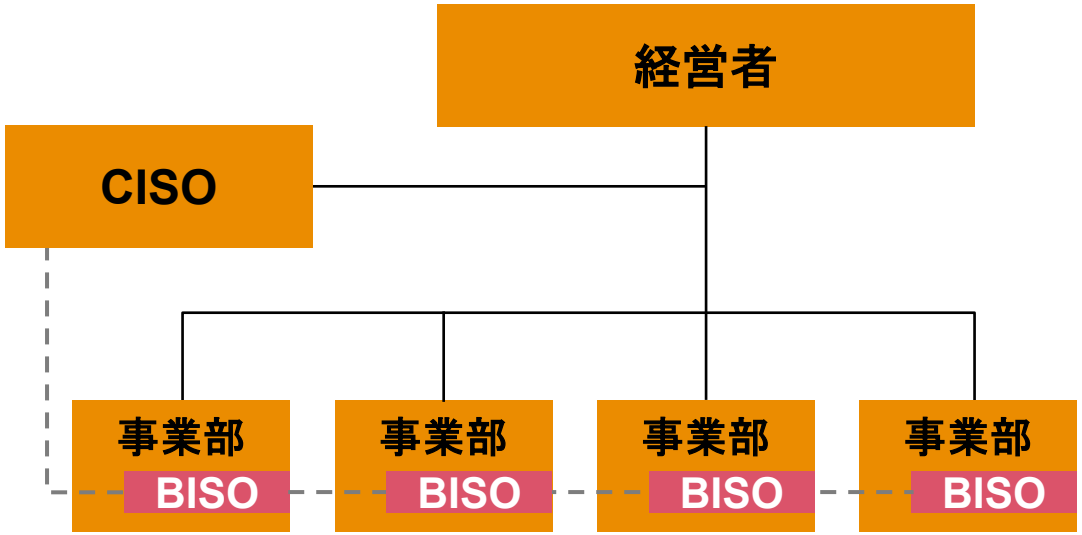
近年、ビジネスリーダーとセキュリティリーダーの認識乖離を解消すべく、ビジネス視点でセキュリティ業務を担うBISO*の設置が加速している。BISOは、CISOと事業部とのコミュニケーションの架け橋となって、情報セキュリティの迅速な推進に貢献し、製品・サービスの品質や顧客価値の向上に寄与する。

* Business Information Security Officerの略

BISOが保有すべきスキルセット

- サイバーセキュリティの重要性を**ビジネス視点で説明すること**が可能
- 情報システムやアプリケーション、サイバーセキュリティ対策など**テクノロジーについて熟知**
- 規制対応やサイバー脅威の変化に対して**リスクマネジメントの展開**が可能
- ビジネスとテクノロジー両部門の言葉で**コミュニケーション**が可能
- 日々巧妙化・多様化するサイバー脅威に対して、組織のサイバーセキュリティ対策を**ダイナミックに実施することが可能**

BISOを設置した組織のイメージ図

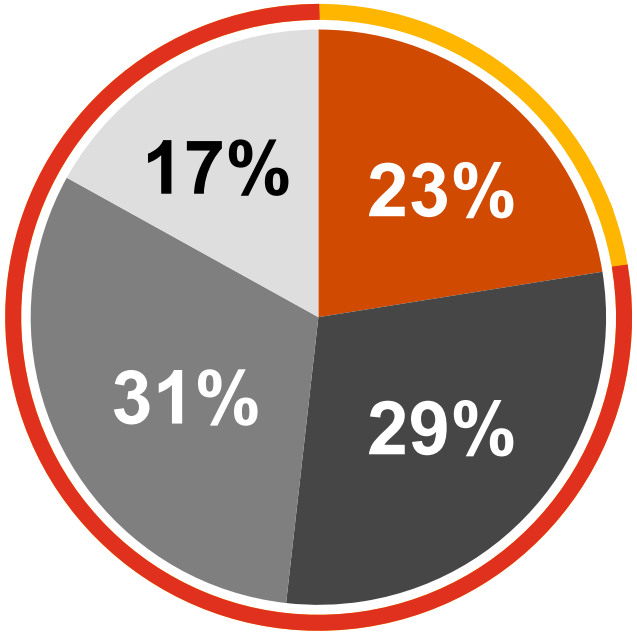


CISOと事業部の**架け橋的存在となり**、情報セキュリティの迅速な推進に貢献
→ ビジネスへのセキュリティ要件の組み込みを促進させることで、**製品・サービスの品質や顧客価値の向上**に寄与

国内でBISO導入が進むも、形骸化の可能性あり

日本ではBISOの導入が8割以上という高水準で進められているが、導入の効果を実感している割合は、わずか4分の1程度にとどまる。

日本における、BISO導入と効果実感状況



- 全社的に導入し、効果を実感している
- 全社的に導入しているが効果は実感していない
- 部分的に導入している
- 現在は導入していない

- ✓ 日本において、BISOを**全社的に導入している企業の割合は半数以上に及ぶ**。
- ✓ **一部でも導入している企業の割合は約83%**と、**グローバル水準（約76%）以上**である。
- ✓ 一方で、**BISO導入の効果を実感している割合は、約23%と低迷**。

BISOの導入が国内で進められている一方、導入の効果を感じている企業は少ないことから、BISOの設置が形骸化してしまっている可能性がある。外的脅威の変化や規制の変化に対して後手に回らないよう、BISOを設置するだけでなく、その役割と権限を明確にして効果的に運用していく必要がある。

出所： 2024 Global Digital Insights Survey（PwC）

BISOの実効性を高めるための対策

BISOを実効性のあるものにするために、経営層はBISOに組織横断的な働きかけの促進を求めることが重要である。

経営層がBISOに求めるべき組織横断的な働きかけを促進するための対策

サイバーセキュリティの専門用語で語らない

CEOやCIOなどのサイバーセキュリティの専門家以外にも理解できる言葉で語ることで、無駄な混乱を防ぐことができる。

サイバーセキュリティを経営層の主要議題とする

サイバーリスクとその管理に関する情報だけではなく、サイバーセキュリティの取り組みがどのように事業や収益に寄与しているかについて、情報を提供する。

事業全体に関わる取り組みとしてセキュリティを推進する

ビジネスとセキュリティを別々に捉えるのではなく、事業全体に関わる取り組みとして、CISOとCEOがともにサイバーセキュリティを積極的に活用する。

理想的なBISOの役割

BISOがセキュリティリーダー（CISOなど）とビジネスリーダー（CEOなど）の橋渡し役として、情報格差を埋める働きをすることで、日々刻々と変化するサイバー脅威や規制に対して、**スピーディかつダイナミック**に対応できる。

Thank you

www.pwc.com/jp

発刊年月：2024年4月　管理番号：I202403-04