Digital Trust Insights 2025

日本企業向け示唆

2023/11/05

pwc

Global Digital Trust Insightsとは

PwCのGlobal Digital Trust Insights（以下、DTI）は、サイバーリスクのトレンドについて継続して実施している調査であり、今年で26年目を迎える。今回（2025年度）は全世界のビジネスリーダーおよびセキュリティリーダー4,042名を対象に調査を実施した。

ビジネスリーダーおよびセキュリティリーダー
4,042名を対象として調査を実施

2024年5月～7月にかけて調査を実施

77カ国　7地域で調査を実施:

- アジア太平洋
- 中東
- アフリカ
- 西欧
- 中・東欧
- 北米
- 中南米

調査テーマ

今後12カ月の間で組織内のサイバーセキュリティを改善し変革するための課題と機会について

Global Digital Trust Insights 2025概要

今回の調査では、企業がサイバーレジリエンスを構築する上で解消すべき重大なギャップがあることが明らかとなった。より安全で持続可能な未来を築くために、これらのギャップを解消し、サイバーセキュリティを事業戦略の中心に据えることが企業に求められる。

企業がサイバーレジリエンスを構築する上で解消すべき重大なギャップ

1 サイバーセキュリティレジリエンスの実装におけるギャップ

サイバーセキュリティリスクの懸念は高まっているが、調査対象の全項目について、サイバーセキュリティレジリエンスに向けた対応が全社的に実行されていると回答したCxOは、全体の2%に過ぎない。

2 サイバーリスクに対する準備態勢のギャップ

クラウド環境のリスクや第三者によるデータ漏洩などは、組織のサイバーセキュリティ上で最大の懸念事項である。しかし、組織においては、これらに対する取り組みが最も遅れていると認識されている。

3 CISOの参画に関するギャップ

戦略的な計画の策定、取締役への報告、テクノロジーの導入管理に、CISOがかなりの程度参画していると回答したCxOは、全体の半数を下回っている。

4 規制遵守に関する自信のギャップ

AI、レジリエンス、重要インフラに係る規制をどの程度まで遵守できるかについて、CEOとCISO/CSOとの間で、自社の能力に寄せる信頼に格差が認められる。

5 サイバーセキュリティリスクの計測におけるギャップ

CxOは、サイバーセキュリティリスクの計測が重要であることを認識している。しかし、このような計測を効果的に行っているのは全体の半分を下回り、さらに、財務上の影響について相当程度に把握できているのは、全体の15%に過ぎない。

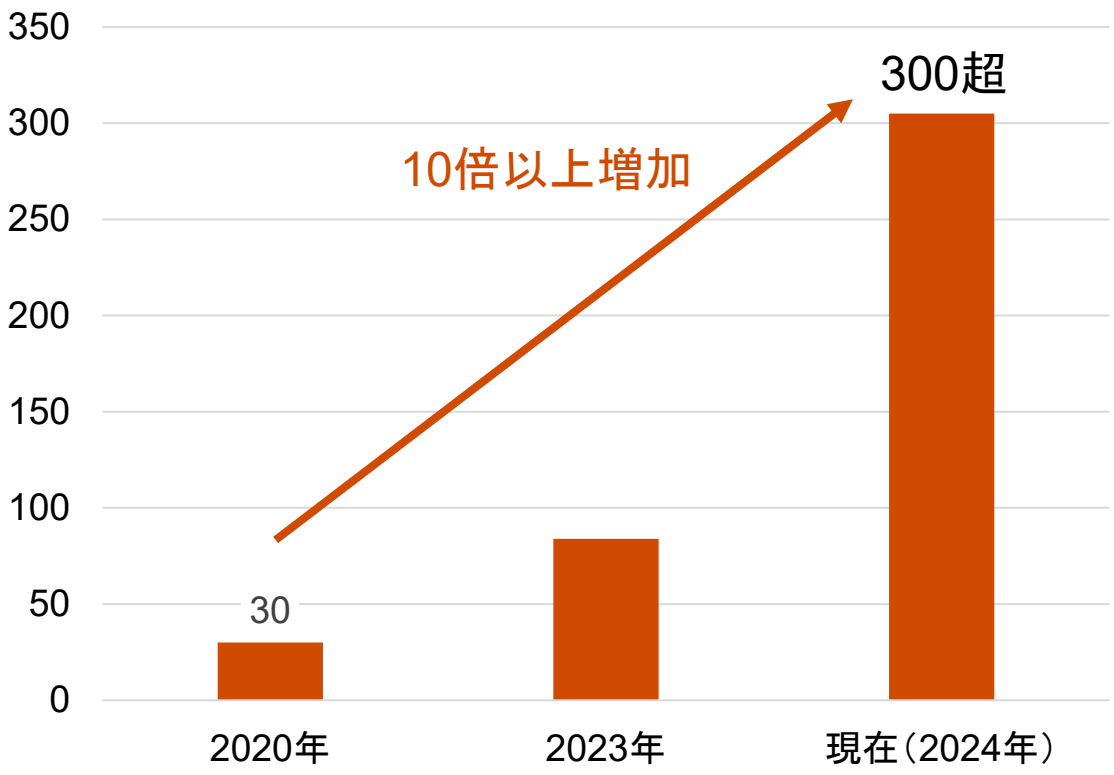
1

日本企業を取り巻く
デジタル法規制および
対応における課題

海外展開する日本企業が対応すべきデジタル法規制の動向

デジタル分野における法令・ガイドラインの数は、2020年と比較し、10倍以上に増加。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。

海外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: 各国・地域の公的情報よりPwC作成

主要な法令・ガイドラインのカテゴリー

- AI
- サイバーセキュリティ
- IoT
- プライバシー

- 昨今では、各国のデジタル分野における法令・ガイドラインは増加され、罰則も強化される傾向にある
- 海外展開する日本企業は準拠すべき法令をタイムリーに把握・対応することが必要

デジタル分野における法令で課される義務および影響

デジタル分野における法規制は、主に①セキュリティ対策の構築、②サプライチェーンリスク管理、③インシデント報告の3つにおいてコンプライアンス義務を課している。企業がコンプライアンス要件に準拠できなかった場合、影響が企業のグループ全体にまで及ぶ可能性がある。

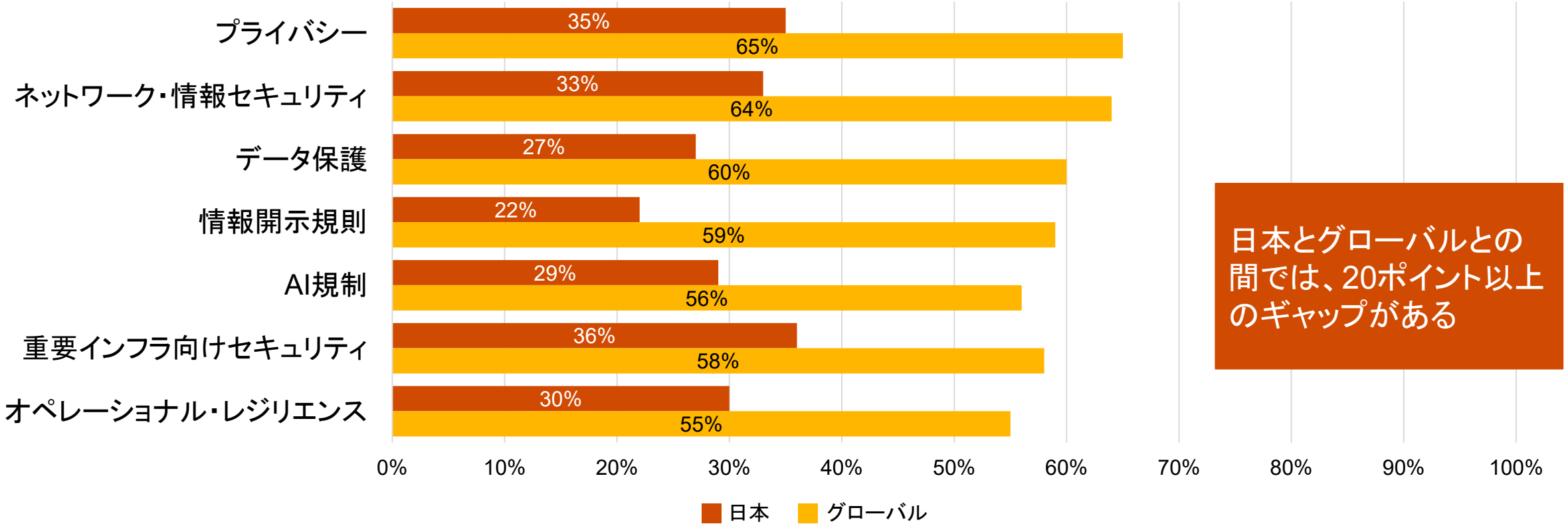
デジタル分野における法令と企業各部門との関係性および影響（一例）

3つの義務	①セキュリティ対策	②サプライチェーンリスク管理	③インシデント報告
違反による影響	高額な罰金 製品・サービス販売不可 製品・サービス競争力の低下	サプライヤー責任の自社責任への転嫁 サプライチェーン由来の責任発生	レピュテーション悪化 訴訟 高額な罰金
部門・役職との関係性	CFO：情報セキュリティ、製品セキュリティコンプライアンス実施への投資の具体化および戦略 取締役会：3つの義務を経営課題として企業戦略に組み込む CEO：各部門のコンプライアンス準拠状況の管理監督 情報システム管理担当（CSIRT）：自社に対する法令要件に従い、セキュリティ対策構築、運用 製品の研究・開発・製造関連部門：製品の企画・設計・開発・生産・販売・保守運用の全てのプロセスにおいて法定要件を具備	調達部門（特に重要インフラ事業者）：セキュアな製品調達（デューデリジェンス実施、委託先のセキュリティ状況確認など） 営業部門：顧客に対してセキュリティ関連対応	CFO：インシデント起因の財務的損失に対する準備および戦略 CLO/CRO/CCO：デジタル分野における新興法規制を理解し、準拠促進 CISO：グローバルにおけるデジタル法規制の動向と自社に対する影響を把握し、技術的対応を促進 情報システム管理担当（CSIRT） 個人情報関係者 製品セキュリティ関係者（PSIRT）：インシデントを各法令が定める期限内に当局へ報告

デジタル法規制に対する日本企業の対応状況

デジタル法規制に対して準拠している自信があると回答した日本企業の割合は40%未満であり、グローバルと比較して20ポイント以上のギャップがある。各デジタル法規制への対応が十分でないと感じている企業が多いことが分かる。

各分野のデジタル法規制に対し、準拠している自信が「非常にある」「かなりある」と答えた割合

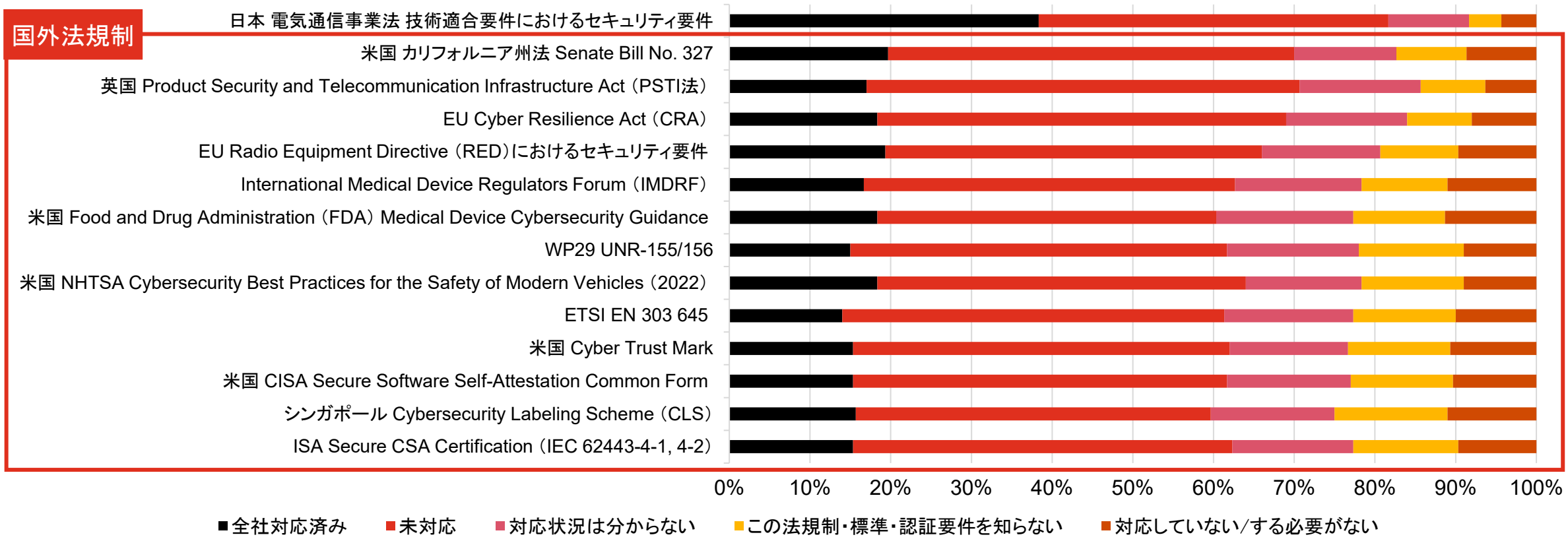


出所：PwC, 2025 Global Digital Insights Survey, Q15

（参考）製品セキュリティ関連法規制への日本企業の対応状況

国外の法規制に対しては、日本の法規制と比較し、対応状況が低い傾向にある。
日本企業は国外の法規制にまで十分に意識を向けられていないことが示唆される。

法規制の対象となる企業の対応状況　n=300（人）



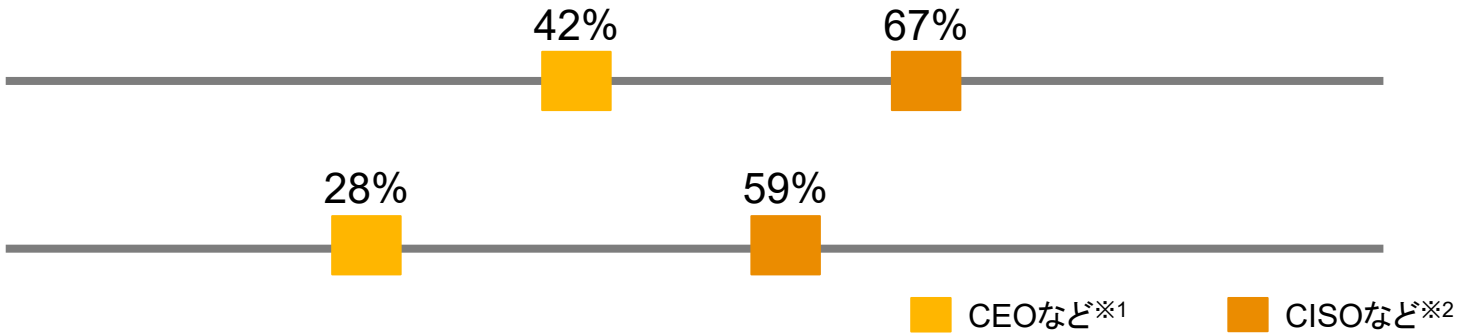
出所：PwC,「SBOMを活用したサプライチェーン管理の課題　ソフトウェアサプライチェーン実態調査」より作成

法規制に対する組織内における認識の乖離

日本企業では、2024年のDTIの結果と同様に、CEOはCISOに比べて法規制の影響を過小評価する傾向があり、両者の意識に依然としてギャップが見られる。CEOは、法規制対応の必要性を十分に認識できていない可能性がある。

2025年 DTI 新たなセキュリティ規制は、過去12カ月間に実質的な影響がなかったと答えた割合

2024年 DTI 各デジタル規制に対して大幅な業務改革が必要と答えた割合



両年ともに、CEOはCISOに比べてデジタル法規制の影響を過少評価する傾向がある。

出所：PwC, 2024 Global Digital Insights Survey, Q17
PwC, 2025 Global Digital Insights Survey

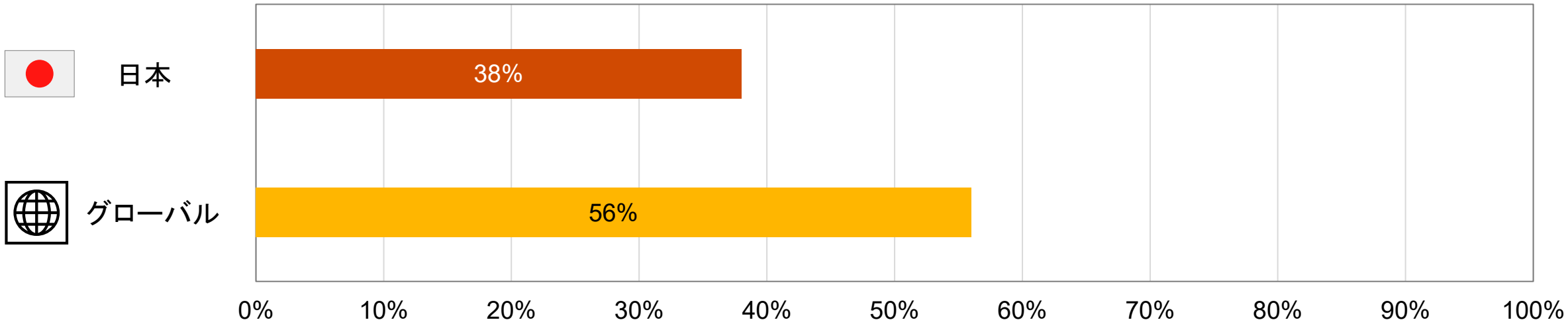
※1 CEOなど：CEO, President, Managing Director, Board Member, CAE, CCO, Head of Compliance, Chief Ethics and Compliance Officer, Chief Counsel / General Counsel / Chief Legal Officer / Senior Counsel, CFO, Chief Innovation Officer, CMO, COO

※2 CISOなど：CDO, Chief Digital Officer, CIO, CIRO, CISO, Chief Privacy Officer, CSO.

組織内における情報連携の不足

グローバルと比較して、日本企業では経営層とセキュリティ部門との間で情報を連携する機会が少ない。情報連携が不足していることにより、経営層が組織におけるセキュリティ課題を十分に把握できず、企業のセキュリティ対応の遅れにつながっていると考察される。

セキュリティ部門において、サイバーリスクや規制動向・対策に関するインサイトを
CEO・取締役会によく提供していると答えた割合※



セキュリティ部門と経営層の間での情報連携が、グローバルと比較して不足している傾向がある。
➢ 経営層が組織におけるセキュリティ課題を十分に把握できていないことが日本企業の課題と考えられる

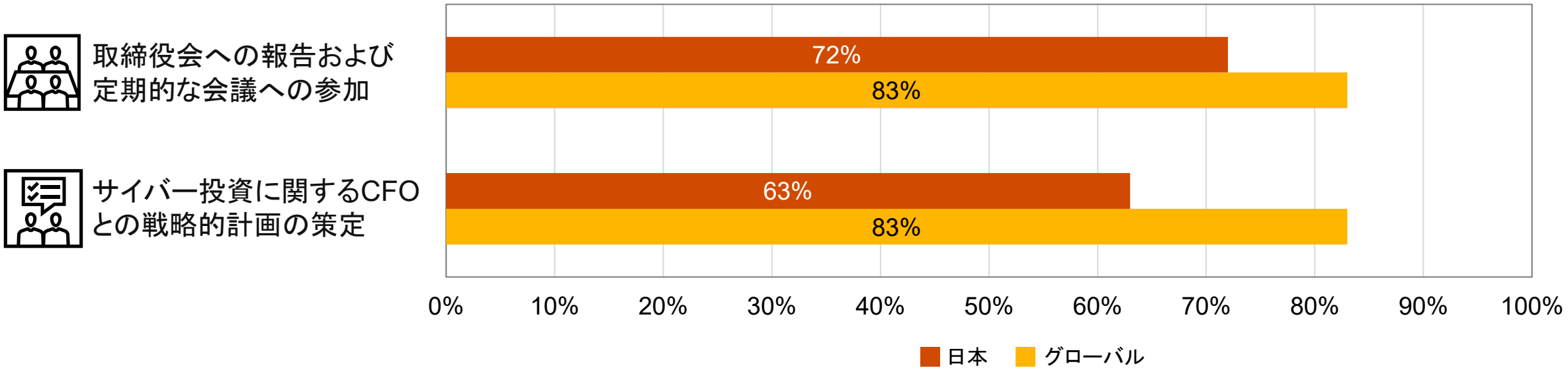
出所：PwC, 2025 Global Digital Insights Survey Q28

※ 61%以上の割合で提供していると答えた割合

日本のCISO活用における課題

日本のCISOは、グローバルに比べて経営に関与する機会が少ない。結果として、CISOを通じて組織のセキュリティ分野における課題が経営層に十分に伝達されず、組織内でのセキュリティ対応の遅れにつながっていると考えられる。

次に示す役割・業務について、CISOが積極的に関与した割合※



CISOは、組織のセキュリティ分野における課題を経営層に直接伝える役割を担うことが期待されているものの、日本においては、当該の役割が十分に機能していない可能性がある。

出所：PwC, 2025 Global Digital Insights Survey, Q21

※「非常にある」「かなりある」と答えた割合

2

CISOの地位向上の必要性

CISOの地位向上の必要性

日本企業では、CISOが経営に参画する機会がグローバルに比べて少なく、組織全体でのセキュリティ対策に遅れが生じていることが明らかになっている。CISOの立場が依然として低く、経営に関与するための権限や機会が十分に与えられていないことが課題であり、解決のためには、組織におけるCISOの地位向上が求められる。

CISO活用における現状（DTI調査より）

- ✓ CISOが経営会議に参画する機会や取締役会に報告する機会がグローバルに比べて少ない。
- ✓ 経営層が組織におけるセキュリティ課題を十分に把握することができず、組織としてセキュリティ対策・法規制対応に遅れが発生している。

CISOの立場が依然として低く、組織の経営に関与するための権限や機会が十分に与えられていないことが課題である。
➢ 組織におけるCISOの地位向上が求められる

PwC Japanグループのサイバーセキュリティリーダーによる提言

経営リスクに係る説明責任を果たす上でCISOの地位向上は不可欠

セキュリティリスクは重大な経営リスクとして捉える必要があり、法規制も強化される傾向にある。組織として各国の法規制を遵守し、ステークホルダーへの説明責任を果たすにはCISOを経営の中枢に配置することが不可欠である。

パートナー　丸山 満彦
PwCコンサルティング合同会社

セキュリティ人材の育成を強化する上でもCISOの地位向上が必要

日本企業は長年セキュリティ人材の不足に悩まされており、人材育成が進んでいないという課題がある。組織のセキュリティ人材育成やキャリアパスのためのインセンティブとして、CISOが経営に参画することを前提とした権限・報酬体系に見直すことが必要である。

パートナー　綾部 泰二
PwC Japan有限責任監査法人

CISOに期待される役割

CISOは、組織の情報セキュリティ戦略を統括する最高責任者を指す。セキュリティの専門家として、組織のセキュリティ対策の指揮・監督を行うだけでなく、経営者の一員として経営戦略の策定やステークホルダーへの説明といった役割も期待される。

CISO（Chief Information Security Officer）	組織の情報セキュリティ戦略を統括する最高責任者を指す。CISOにはセキュリティ専門家としての役割および経営層の一員としての役割が期待される。

CISOの役割※	セキュリティの専門家として期待される役割	経営層の一員として期待される役割
	• セキュリティ戦略の計画・実行に係る監督 • 法規制遵守に向けた対外対応、組織内における対応の監督 • インシデント対応の指揮	• セキュリティ計画を含む経営戦略の策定 • セキュリティ対応組織・ポリシーの確立 • サイバーセキュリティ戦略・対応状況に関するステークホルダー（投資家・当局を含む）への説明

※ The Australian Signals Directorate's Australian Cyber Security Centre, Guidelines for Cyber Security Roles を基にPwCにより定義

CISOの地位向上に向けた今後のアクション

CISOの地位向上は、組織のサイバーセキュリティリスクの低減とレジリエンス強化に不可欠。CISOの地位を向上させ、経営に関与できるようにするためには、CISOと経営層の双方が協力し、戦略的なビジョンと具体的なアクションを共有することが求められる。

CISOおよび経営層に求められるアクション （Digital Trust Insights 2025を基に作成）

CISOに求められるアクション例

◆ 経営層への説明、継続的なコミュニケーション

- ➢ 組織のサイバーセキュリティリスクの現状と影響を評価し、リスク低減のための具体的な戦略や計画について経営層・ステークホルダーに説明する
- ➢ 定期的に経営層と会議を行い、サイバーセキュリティの対応状況、組織に対する新たな脅威やリスクへの対応策を共有する

双方の
協力が必要

経営層（CxO）に求められるアクション例

◆ CISOの経営への参画、定期的なフィードバック

- ➢ セキュリティリスクも重大な経営リスクの1つであることを認識し、CISOを経営戦略の意思決定に関与させる
- ➢ 組織におけるサイバーセキュリティ演習やリスク評価の実施状況を把握し、定期的にCISOにフィードバックする

✓ CISOと経営層（CxO）の双方が協力し、継続的なコミュニケーションを通じて戦略的なビジョンと具体的なアクションを共有することが重要です。実践のためには、組織においてCISOおよび経営層（CxO）の業務や役割を明確化することが必要となります。

✓ PwCでは、最新のセキュリティ・業界知見をもとに、CISOが効果的に機能するためのアドバイザリーサービスを提供しています。

3

補足資料

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

AI

- EU 欧州委員会：AI指針
- EU 欧州委員会：AI規則案
- 米国 WhiteHouse：大統領令
- 米国 WhiteHouse：AI権利章典
- 米国 国防総省：責任あるAIの指針の採用
- 米国 連邦取引委員会：ビジネス向けのAIアルゴリズム利用に係るガイダンス
- 米国 予算行政管理局：AI規制に係るガイダンス
- 米国 NIST：AIリスクマネジメント枠組み
- UK ICO：AIおよびデータ保護リスクツールキットv1.0
- 中国 国家インターネット情報弁公室（CAC）：インターネット情報サービスアルゴリズムレコメンデーション管理規定
- 中国 国家インターネット情報弁公室（CAC）：インターネット情報サービス深度合成アルゴリズム管理規定
- 中国 国家インターネット情報弁公室（CAC）：生成人工知能サービス管理弁法（パブコメ）

デジタルサービス

- EU 電子商取引指令
- EU デジタルサービス法
- EU デジタル市場法

IoT／OT

- 米国 IoTサイバーセキュリティ改善法
- 米国 カリフォルニア州 IoTセキュリティ法
- 米国 オレゴン州 IoT法
- EU サイバーセキュリティ法
- EU サイバーレジリエンス法
- EU RED委任規制2022/30（RE指令）
- 英国 製品セキュリティと通信インフラに関する法
- ブラジル 通信機器サイバーセキュリティ要件（法律第77号）

サイバーセキュリティ

- 日本 サイバーセキュリティ基本法
- 中国 サイバーセキュリティ法
- 米国 2022年重要インフラ向けサイバーインシデント報告法
- EU サイバーセキュリティ法
- EU 共通の高度サイバーセキュリティ措置に関する指令（NIS 2指令）
- EU サイバーレジリエンス法案
- EU デジタルオペレーションレジリエンス法
- 英国 ネットワーク・情報システム規則
- インド IT法2000／インフォメーション・テクノロジー・ルール2021
- インド 国家サイバーセキュリティポリシー
- インド インドCERT-Inサイバーセキュリティ指令2022
- 国連 UNECE規則サイバーセキュリティ（UN-R155）
- 国連 ソフトウェアアップデート（UN-R156）
- ISO ISO/SAE 21434

プライバシー

- 日本 個人情報保護法
- 中国 個人情報保護法
- 中国 データセキュリティ法
- 香港 個人情報保護法
- 台湾 個人情報保護法
- 韓国 個人情報保護法
- インド 個人情報保護法
- インドネシア 個人データ保護法
- オーストラリア 個人情報保護法
- シンガポール 個人データ保護法
- タイ 個人情報保護法
- フィリピン 個人情報保護法
- ブルネイ 個人データ保護規定草案
- ベトナム 個人データ保護法
- ニュージーランド プライバシー法2020
- マレーシア 個人情報保護法
- スリランカ 個人データ保護法2022年第9号
- EU 一般データ保護規則
- EU eプライバシー規制
- ベラルーシ 個人情報保護法
- ドイツ 電気通信およびテレメディアにおけるデータ保護およびプライバシーの規制に関する連邦法
- 英国 データ保護法
- 英国 一般データ保護規則
- スイス 改正連邦データ保護法1992
- イスラエル プライバシー保護法
- カタール データ保護規則2021

- モロッコ 個人データの処理に関する個人の保護に関する法律第09-08号
- チュニジア Organic law No. 63 - 2004
- トルコ 個人情報保護法
- ロシア 2006年7月27日付個人データに関する連邦法152-FZ号の改正法
- 南アフリカ 個人情報保護法
- アラブ首長国連邦 個人情報保護に関する2021年連邦政令第45号
- ケニア データ保護法
- ルワンダ 個人情報保護法とプライバシーに関する法律
- カナダ 個人情報保護および電子文書法
- カナダ 2022年デジタル憲章実施法
- 米国 カリフォルニア州消費者プライバシー法
- 米国 バージニア州消費者データ保護法
- 米国 コロラド州プライバシー法
- 米国 コネチカット州データ保護法
- 米国 ユタ州消費者プライバシー法
- チリ 私生活の保護に関する法律
- ブラジル データ保護法
- ペルー 個人情報保護法
- メキシコ 民間団体が保有する個人データの保護に関する連邦法
- パナマ データ保護法
- エクアドル 個人情報保護法
- アルゼンチン 個人情報保護法 25.326

出所: 各国・地域の公的情報よりPwC作成

罰金額も高額化の傾向（一例）

AI	欧州AI法	• 受容できないAIに関する禁止事項（第5条）への違反 4,000万ユーロ（約62億円）または全世界売上高の7%の高い方 • ハイリスクAIに関する要求事項（第10条、13条）への不遵守 2,000万ユーロまたは全世界売上高の4%の高い方 • 上記以外の要求事項・義務の不遵守 1,000万ユーロまたは全世界売上高の2%の高い方
デジタルサービス	EUデジタルサービス法	• プロバイダの年間売上高の6%を上限
	EUデジタル市場法	• 1回目 企業の年間売上高の10%、2回目 20%
IoT／OT	EUサイバーレジリエンス法	• 1,500万ユーロまたはグローバル年間売上高の2.5%のいずれか高い方
	英国製品セキュリティと通信インフラに関する法	• 最大1,000万ポンド（約18億円）または企業の総売上高の4%
サイバーセキュリティ	EU共通の高度サイバーセキュリティ措置に関する指令（NIS2指令）	• 1,000万ユーロまたは売り上げの最大2%
プライバシー	中国個人情報保護法	• 最大5,000万元（約10億円）または前年度売上の5%の罰金
	EU一般データ保護規則（GDPR）	• 2,000万ユーロまたは組織の前年度売上の4%のいずれか高い方

出所: 各国・地域の公的情報よりPwC作成

インシデント報告義務に関する各国の法整備状況

国	年	根拠とする法規制	報告の基準
米国	2021年	Ransomware Guidance	インシデント発生後72時間以内に米国ニューヨーク州金融サービス局（NYDFS）へ報告
	2022年	重要インフラサイバーインシデント報告法2022（CIRCIA）	インシデント発生後72時間以内、ランサムウェア身代金支払い後24時間以内にCISAへ報告
	2023年	Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure	重大なインシデントと判断してから4営業日以内に米国証券取引委員会（SEC）へ報告
欧州	2016年	EU一般データ保護規則（GDPR）	漏えいを認識してから72時間以内に監督当局へ報告
	2022年	NIS2指令	重大なインシデントを把握してから24時間以内に早期警告、72時間以内にインシデント通知、インシデント通知から1カ月以内に最終報告書を提出
	2024年	欧州サイバーレジリエンス法	重大なインシデントを認識してから24時間以内に早期警告、72時間以内にインシデント通知、インシデント通知から1カ月以内に最終報告書を提出
中国	審議中	中国サイバーインシデント報告管理弁法（パブコメ）	「サイバーインシデント分類分級ガイドライン」に従って、比較的大きいレベル以上のサイバーインシデントについて、1時間以内の報告
オーストラリア	2021年	重要インフラ安全保障法（Security of Critical Infrastructure Act 2018）の改正	重要インフラ責任事業体は重大なサイバーインシデントの発生を認識してから12時間以内に、またその他関連サイバーインシデントについては発生を認識してから72時間以内に当局へ報告
インド	2022年	Cyber Security Directions of 28th April 2022	サイバーインシデントを認識してから6時間以内に報告

Thank you

www.pwc.com/jp

発刊年月：2025年3月　管理番号：I202501-12