Digital Trust Insights 2026

日本企業向け示唆

2026年4月

www.pwc.com/jp

Global Digital Trust Insightsとは

PwCは、サイバーリスクに関する年次調査として、「Global Digital Trust Insights」を20年以上継続して実施している。

調査対象
世界72カ国のビジネスリーダーおよび
テクノロジーリーダー3,887人

調査時期
2025年5月～7月

調査テーマ
企業のリーダーが、不確実な時代にどのように対処しているか、どういった課題を抱えているか、
課題に適切に対応するために何を変えるべきか

Global Digital Trust Insights 2026概要

サイバーセキュリティは未知の領域に踏み出そうとしている。ここ数年におけるテクノロジーの飛躍的な変化を受けて、世界秩序と脅威環境が急速に変化する中、サイバーセキュリティ戦略の真価が問われている。

Global Digital Trust Insights 2026の主な調査結果

1 地政学的リスクが戦略の立案に影響

ビジネスリーダーとテクノロジーリーダーの60%が、地政学的な不確実性の増大を受けて、サイバーセキュリティリスクへの投資を重点戦略の上位3項目の1つに位置付けている。

2 レジリエンス強化の取り組みは道半ば

地政学的情勢と連動してサイバーセキュリティリスクが高まる中で、リーダーの約半数が組織における特定の弱点（脆弱性）をターゲットにしたサイバー攻撃に対して、自社組織は「ある程度耐性がある」と回答している。調査において、組織の脆弱性に関連する全調査項目について自信があると回答したのは、全体の6%に過ぎない。

3 トラブルへの備え

サイバーインシデントの未然防止策への支出が事後対応策への支出を大幅に上回っている組織は全体の24%にとどまります。支出割合としては、前者が後者を上回ることが理想だが、大半の企業（全体の67%）では、両者がほぼ拮抗している。事前対応が不十分でインシデント発生後に初めて本腰を入れて対応する場合、事業継続リスクや総セキュリティコストが増大する可能性がある。

4 サイバーディフェンスに自律型AIを活用

自律型AIは、今後12カ月間において各組織が最も重視するセキュリティ領域におけるAI活用事例の1つである。特にクラウドセキュリティ、データ保護、サイバー攻撃に対する防御とその運用を目的とする自律型AIの導入計画が進められている。

出所: PwC, 2026 Global Digital Insights Survey

0

Executive Summary

Executive Summary

コネクテッド製品やサプライチェーンを狙った攻撃など、セキュリティリスクが多様化する中、日本では自組織の対処能力に懸念を抱く企業の割合がグローバルと比べて高い。これらのリスクへの対応として各国・地域で法整備が進んでおり、企業においては部門横断的な協力が不可欠である。特に、経営メンバーとしてのCISOと他のCxOの連携推進が推奨される。

環境の変化	• 地政学的緊張、サプライチェーンの複雑化、攻撃手法の多様化と高度化によりサイバーリスクは日本でも増大しており、本調査に回答した日本企業121社の8%が、過去3年間においてサイバー攻撃により約15.6億円（1米ドル156円換算）以上の損害を被ったとした。 • 多様化するリスクに対応する上で、プライバシーを含むデータ保護中心であった各国・地域のコンプライアンス対応が、企業のサイバーセキュリティの取り組みやサプライチェーン管理、コネクテッド製品脆弱性管理などのより広い範囲を対象とするようになっている。
日本企業の現状	• プライバシーを含むデータ保護は、法整備もあって日本企業では一定の取り組みができていると推測される。 • 一方、近年多発するコネクテッド製品やサプライチェーンといった組織のセキュリティ上の弱点（脆弱性）を狙った大規模な攻撃に「現状十分に対処可能」と回答した企業の割合は、グローバルの結果に比べて大きく下回っており、改善の余地が示唆されている。 • また、サプライチェーンリスク対応のための調達部門との連携といった、多様化するセキュリティリスクに柔軟に対応できるレジリエンス獲得のための施策推進において不可欠なCISOと他の経営メンバー（CxO）間の連携強化に課題がある。
示唆	• コネクテッド製品やサプライチェーンを狙った攻撃を含む多様化するセキュリティリスクに柔軟に対応できる組織実現のためには複数部門の巻き込みが必要であり、経営メンバーとしてCISOが積極的に他のCxOと連携していくことが不可欠である。

1

日本企業のサイバーセキュリティを取り巻く環境

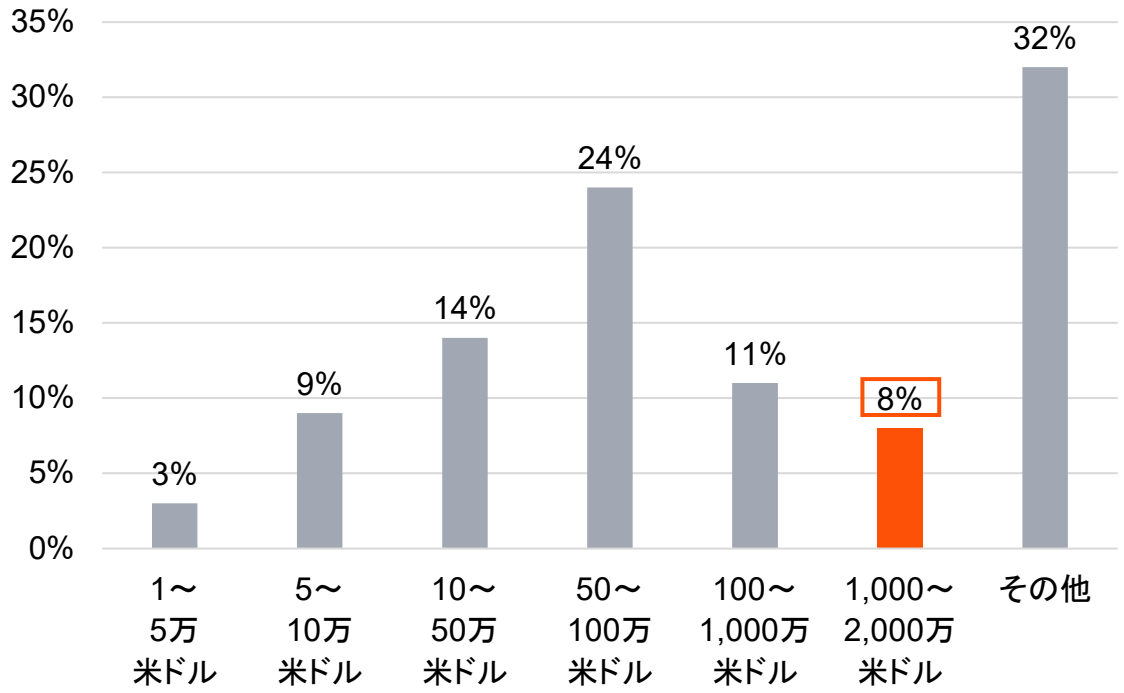
サイバーリスクの高まりと被害額の増大

地政学的緊張、サプライチェーンの複雑化、攻撃手法の多様化と高度化によりサイバーリスクは日本でも増大している。
本調査に回答した日本企業121社の8%が、過去3年間においてサイバー攻撃により約15.6億円（1米ドル156円換算）以上の損害を被ったとしている。

日本企業のサイバーセキュリティを取り巻く環境

- **地政学的リスク**
  国際的な軍事・経済的な緊張の高まりに伴うサイバー攻撃の増加
- **サプライチェーンの複雑化**
  DXに伴うサプライチェーン・サービスプロバイダー関係の複雑化によって、自組織以外も含めたセキュリティリスク管理の重要性と難しさが増大
- **攻撃手法の多様化と高度化**
  ランサムウェア攻撃、コネクテッド製品を通じた攻撃、未知の脆弱性を突いたゼロデイ攻撃の増加

企業への影響：過去3年間の日本企業におけるサイバー被害額と割合



出所: PwC, 2026 Global Digital Insights Survey

サイバー攻撃がもたらす経営へのインパクト

攻撃手法の高度化、巧妙化によってサイバーインシデントの被害は、システム復旧のコストにとどまらず業績の悪化や経営計画の見直し、株価の下落などにも波及するようになっており、企業経営へのインパクトはますます高まっている。

サイバー攻撃がもたらす経営へのインパクト

業績悪化・経営計画の見直し

- 業務復旧が長期に及ぶと経営計画の見直しも必要となる
- システム停止期間の長期化や再開見通しの不確かさは投資家や取引先にとって不安材料

株価の下落

- インシデントの公表日直後において株価が下落する傾向を確認
- 後続する情報公開で再度株価が下落するケースもあり、特に業務停止が長期化する場合は株価は総じて下落傾向
- 日経平均株価が上昇する中、インシデントの被害組織は下落傾向に転じるという対称的な値動きをすることも

リスクの多様化により、コンプライアンス要件は拡大

国際社会の緊張や経済のデジタル化により、セキュリティリスクが多様化している。各国・地域のコンプライアンス対応は、プライバシーを含むデータ保護が中心だったが、昨今はサイバーセキュリティ対策、サプライチェーン管理、コネクテッド製品の脆弱性管理、インシデント報告など、より広い範囲を対象とするようになっている。

	従来のコンプライアンス対応	昨今のコンプライアンス対応
概要	プライバシー・データ保護対応が中心	セキュリティ対策の義務化
背景	プライバシー意識の高まり	サイバーリスクの高まり
主要法令	• GDPR（EU） • 個人情報保護法（各国） • データ法／データセキュリティ法（各国） など	• 経済安保推進法（日本） • NIS2指令（EU） • 重要インフラ向けサイバーインシデント報告法（CIRCIA）（米国） など
法令のコア要件	• データ保護責任者の設置 • 透明性のある取り扱い • 個人のデータに対する権利保証 • データの分類とリスク評価 • リスクベースのデータセキュリティ管理措置 • データ漏洩／権利侵害発生時の公開と報告 • 域外データ移転の制限	• 経営層のセキュリティガバナンスへの関与 • リスク分析・リスク管理策実装・運用・評価から成る組織のサイバーセキュリティリスク管理PDCA • サプライチェーン管理 • コネクテッド製品の脆弱性管理 • インシデント発生時の当局への報告

コンプライアンス対応の範囲拡大

出所: 各国・地域の公的情報よりPwC作成

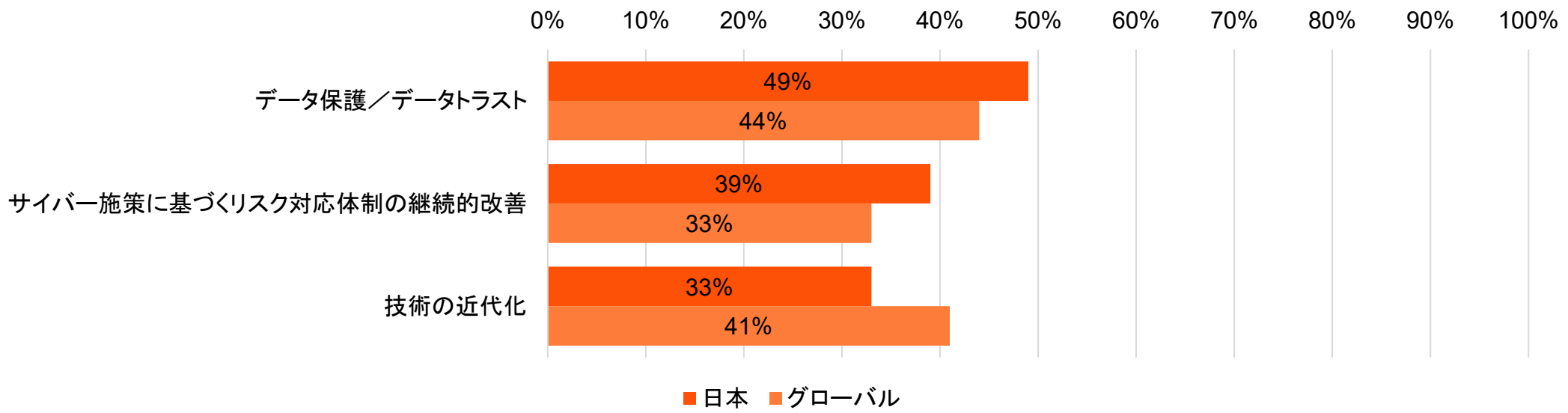
2

日本企業のサイバーセキュリティに関する現状

データ保護優先のサイバー関連支出

グローバル、日本ともに、サイバー関連の支出の優先順位に最も影響を与えているのはデータ保護である。これは以前から法整備が進んでいたプライバシー・データ保護対応が他施策に対して優先されてきたためと考えられる。一方で、グローバルでは技術の近代化への投資に関心が移りつつあり、リスクの多様化を踏まえ日本企業でも投資の見直しが推奨される。

今後12カ月間のサイバー関連支出の優先順位に影響を与えている要因について、上位3つに選ばれた割合

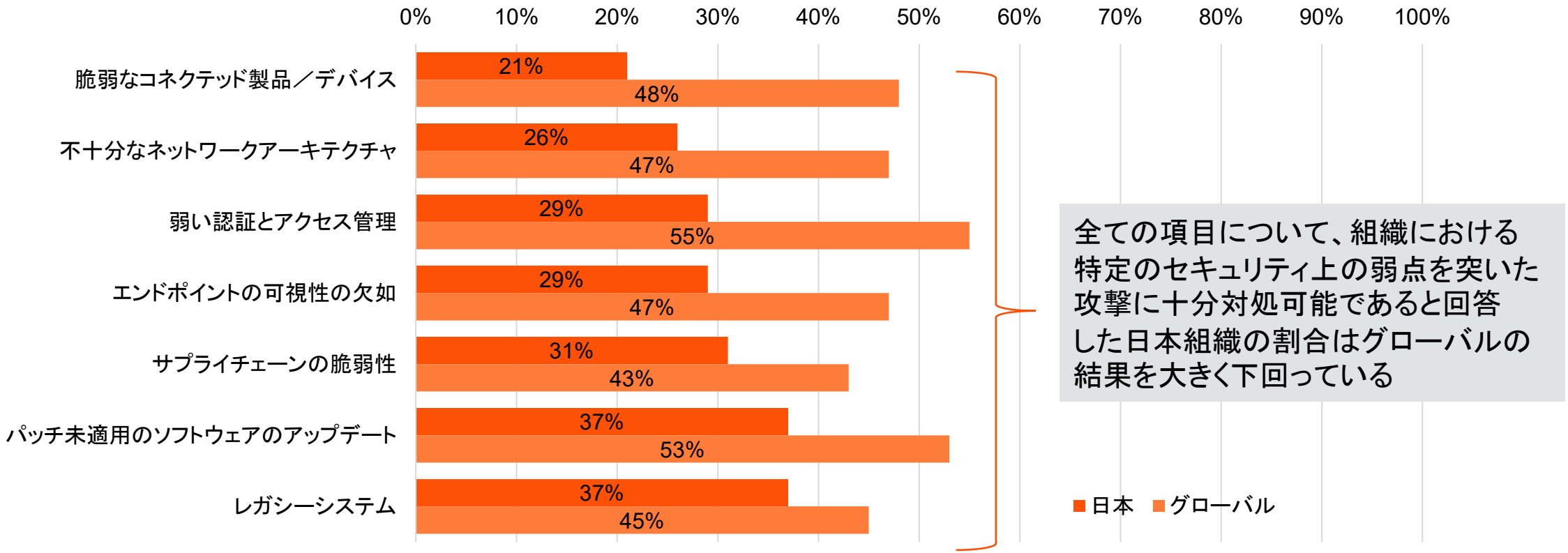


出所: PwC, 2026 Global Digital Insights Survey, Q10

組織の弱点を突いたサイバー攻撃へのセキュリティは不十分

コネクテッド製品やサプライチェーンを狙った大規模な攻撃に対して、「現状十分に対処可能」と回答した日本企業の割合は、グローバルと比べて低い。これらの領域では、組織の弱点を突いたランサムウェア攻撃などが多発しており、日本を含む各国・地域で法令や任意制度によるセキュリティ対策の規範化が進んでいる。こうした動向を踏まえると、日本企業のセキュリティ対策については、見直しが必要である。

以下の組織の脆弱性を標的とした大規模なサイバー攻撃に対して、十分対処可能と答えた割合



全ての項目について、組織における特定のセキュリティ上の弱点を突いた攻撃に十分対処可能であると回答した日本組織の割合はグローバルの結果を大きく下回っている

出所: PwC, 2026 Global Digital Insights Survey, Q3

3

CISOの役割・責任の再定義とCxO間連携強化の必要性

経営メンバーとしてのCISOとCxOの強い連携が必要

コネクテッド製品やサプライチェーンを含めたさまざまなセキュリティリスクに柔軟に適応できるレジリエントな組織実現のために、CISOは経営メンバーとして他のCxOとの連携をさらに強化していくことが不可欠である。

CISO活用における現状（2026DTI調査より）

日本企業でもCISOの必要性についての認識は向上しつつあるものの、コネクテッド製品やサプライチェーンを含めたさまざまなリスクに対応する上で必要になる他のCxOとの連携は、グローバルに比べて遅れがある。

経営メンバーとしてのCISOが他のCxOとより機動的に連携できるようにすることは、多様化するリスクに柔軟に対応する上で不可欠

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の役割・責任の再定義は不可欠

サイバーセキュリティに関する社会的重要性が増しています。法規制が強化されるとともに、企業にとって、サイバー攻撃は経営上の重要リスクになっています。これについての説明責任を果たす上でCISOの役割・責任の再定義は不可欠です。具体的には、CISOが経営メンバーとして他のCxOと連携し、全社のセキュリティを統括する必要があります。

PwCコンサルティング合同会社
パートナー　丸山 満彦

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を抱えています。人材育成の強化やキャリアパスのためのインセンティブとして、経営に参画することを前提とした権限・報酬体系に見直し、CISOの地位を向上させることが必要です。

PwC Japan 有限責任監査法人
パートナー　綾部 泰二

CISOに求められる役割

CISOは、経営メンバーとして規制やビジネス戦略と整合したサイバーセキュリティ戦略とポリシーを推進することに加え、他のCxOと協力しながら、多様化するサイバーリスクに柔軟に適応できる組織の実現に向けたアクションを主導する。また、その実施に関して取締役会を含むステークホルダーへの説明責任を果たしていくことが求められる。

CISOに求められる役割の例

サイバーセキュリティ計画とポリシー作成、実装	▪ 規制やビジネス戦略と整合した多様なリスクに柔軟に対応できるサイバーセキュリティ戦略とポリシーの計画 ▪ ポリシーの実施、管理監督および報告 ▪ サプライヤーの管理とサプライチェーンの保護 ▪ 他のCxOと連携して事業継続計画（BCP）の策定を含むビジネスに対する多様なサイバーリスクに柔軟に対応するための組織づくりを推進
サイバーセキュリティリスクの管理	▪ リスク分析、システム セキュリティ、サプライヤー セキュリティ、暗号化、アクセス制御、資産管理、人的リソースに関する セキュリティに関するポリシーの実施 ▪ 他経営層メンバーやステークホルダー、従業員に対する啓発活動
規制当局を含むステークホルダーとの協力	▪ 法規制に基づく当局への情報共有や報告、当局の指示命令への対応 ▪ コネクテッド製品やサプライチェーンの管理など、他のCxOと連携して対応すべき領域のサイバーリスクについて、対応策を共有・協議 ▪ 取締役会を含むステークホルダーに対するサイバーセキュリティリスク管理状況の報告

※The European Union Agency for Cybersecurity（ENISA）の”European Cybersecurity Skills Framework（ECSF）”を参照してPwCが作成

お問合せ先

PwC Japanグループ
www.pwc.com/jp/ja/contact.html

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwC Japan有限責任監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびブローダーアシュアランスサービス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約13,500人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。PwCは、クライアントが複雑性を競争優位性へと転換できるよう、信頼の構築と変革を支援します。私たちは、テクノロジーを駆使し、人材を重視したネットワークとして、世界137の国と地域に364,000人以上のスタッフを擁しています。監査・保証、税務・法務、アドバイザリーサービスなど、多岐にわたる分野で、クライアントが変革の推進力を生み出し、加速し、維持できるよう支援します。

発刊年月：2026年4月　　管理番号：I202603-01