CxOプレイブック：サイバーセキュリティレジリエンスにおけるギャップの解消

「Global Digital Trust Insights 2025」調査結果より

www.pwc.com/jp

pwc

「Global Digital Trust Insights 2025」調査結果より

2% 調査対象の全分野について、サイバーセキュリティレジリエンスのための全社的な活動を実施しているのは全体のわずか2%

50% 重要な事業活動にかなりの程度参画しているCISOは半数未満

13% 13%は、AIやレジリエンスに関する規制遵守の自信について、CISO/CSOとCEOとの間に格差があると指摘

人工知能（AI）、コネクテッドデバイス、クラウド技術の進歩に伴い、アタックサーフェスの拡大が続いています。また、規制環境は常に変化しています。このような状況下、企業レベルでのサイバーセキュリティレジリエンスの構築が不可欠です。

これらの課題の存在については幅広く認識されているものの、依然として解消していない大きなギャップがあります。CxOは、自らの組織を保護するために、日常的な課題としてサイバーセキュリティに取り組むとともに、戦略的意思決定に際しては、常にこれを念頭に置いて、CxOの連携を求める必要があります。

PwCが世界77カ国のビジネスリーダーおよびセキュリティリーダー計4,042名を対象に実施した「Global Digital Trust Insights 2025」調査によると、サイバーセキュリティレジリエンスを構築するために、企業は大きなギャップを解消しなければならないことが明らかになりました。

- **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ますが、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%に過ぎません。
- **サイバーリスクに対する準備態勢のギャップ：**クラウド関連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す。しかし、組織はこれらに対する取り組みが最も遅れていると認識しています。
- **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ます。
- **規制遵守に関する自信のギャップ：**特に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、自社の能力に対する自信に格差が認められます。
- **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認識しています。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%に過ぎません。

以上からも、サイバーセキュリティレジリエンスの強化を図るために、CxOの連携強化と戦略的な投資が必要とされることは明らかです。このようなギャップを解消し、サイバーセキュリティを事業経営の根幹に据えることで、より安全な将来に向けた橋渡しができるのです。CISOは、テクノロジーに裏付けされた知見を共有するとともに、サイバーセキュリティ上の重点項目について、コスト、機会、リスクといったビジネス的観点から説明することによって、今回得られた結論の推進に向けて貢献することができます。

目次

サイバーセキュリティの脅威を乗り越える：準備態勢の構築に向けた認識の共有

66% セキュリティリーダーの66%が、低減すべき最大のリスクはサイバーセキュリティであると回答。一方、ビジネスリーダーで同様の回答をした人は48%

42% CxOの42%は、サイバーセキュリティ関連の脅威の中で、クラウド絡みの脅威を最も懸念

Top 2 セキュリティリーダーは、クラウドとコネクテッドアイテムに対する攻撃への対応が最も遅れていると認識

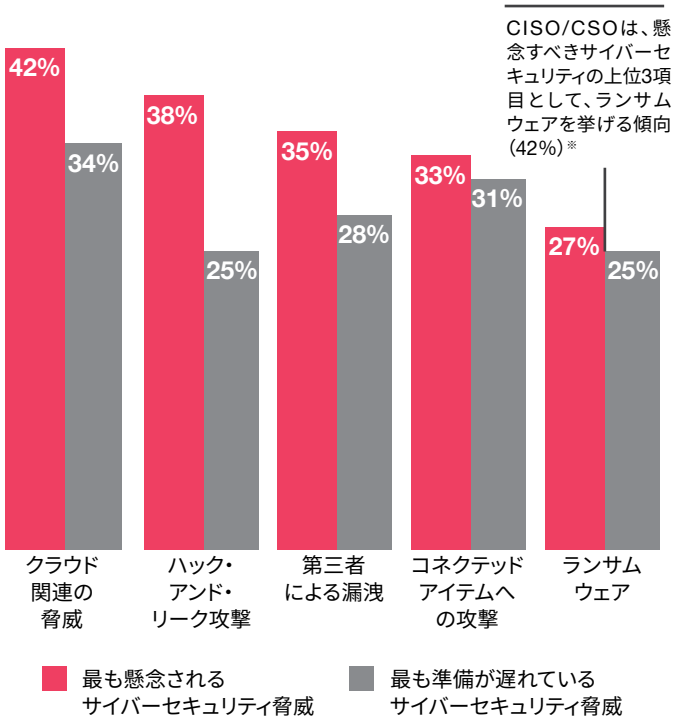
サイバーセキュリティを取り巻く環境が進化を続ける中、ますます不安定で予見し難くなる脅威を前に、組織が対策を講じるのは容易ではありません。クラウド、AI、コネクテッドデバイスへの依存が強まり、第三者頼みの案件が増えるにつれ、アタックサーフェスが拡大しています。こうした状況においてレジリエンスを構築するには、全社的で迅速な対応が求められます。組織の重点項目と準備態勢の構築との調整を図り、セキュリティの維持と事業の継続性を確保することが不可欠です。

最も懸念される脅威への準備が不十分

組織にとっての最大の懸念事項は、準備が最も遅れている事項と言えます。サイバーセキュリティに関する最大の懸念事項として挙げられた上位4項目は、クラウド関連の脅威、ハック・アンド・リーク攻撃、第三者による漏洩、コネクテッドアイテムへの攻撃でした。これらの脅威は、セキュリティリーダーが最も対応が遅れていると認識しているものでもあります。このように、脅威の実態と組織の体制整備状況との間にギャップが見られることから、投資の強化と対応能力の充実が急務とされる実情がうかがわれます。

さらに言えば、組織内においても、セキュリティリーダーとそれ以外の社内関係者との間で、認識の齟齬が存在します。すなわち、CISOとCSOの目から見れば、ランサムウェア攻撃が、組織として懸念すべき脅威のトップ3の1つに位置づけられる可能性が高いのです。これには、セキュリティリーダーが社内で担う役割が反映しているのかもしれません。他の関係者と違って、サイバーセキュリティやIT関連の職務においては、ランサムウェア対応は業務の中心に位置づけられるものであり、担当するCxOは、脆弱性をより強く実感している可能性があるからです。このことは、組織における重点課題の調整を行うために、経営幹部の間で情報共有の強化を図る必要性を裏付けるものです。

サイバーセキュリティの脅威と準備態勢
（上位3項目の構成比）



※世界平均27%との比較
質問2　今後12カ月間において、あなたの組織で最も懸念されるサイバーセキュリティの脅威を以下から選択してください（例：あなたの会社のブランドへのリスク、事業の喪失または事業への障害、コンプライアンス（上位3項目））。調査ベース：全回答者（4,042）
質問3　今後12カ月間において、あなたの組織で最も対応が遅れていると認識しているサイバーセキュリティの脅威を挙げてください（上位3項目）。調査ベース：セキュリティ分野およびCFO回答者（1,951）
出所：PwC「Global Digital Trust Insights 2025」

CxOへの警鐘

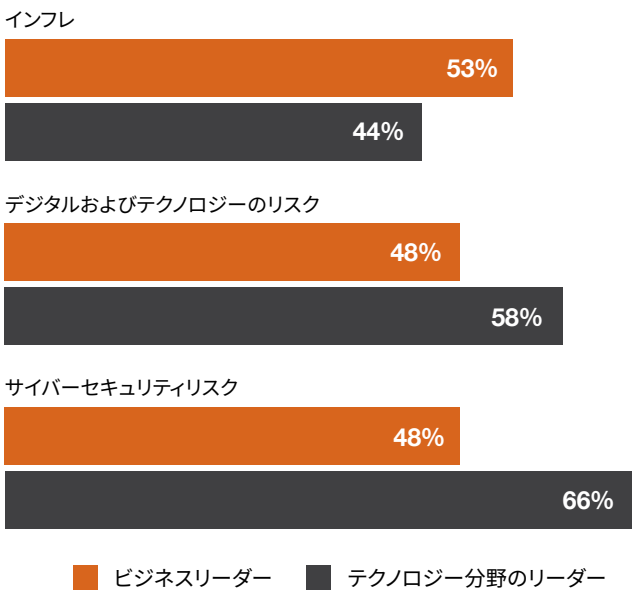
サイバーセキュリティ投資戦略の策定は、脅威を念頭に置いて行うことが重要です。喫緊のサイバーセキュリティリスクへの投資を最優先で実行しなければなりません。そして、人員、プロセス、ディフェンス能力のどこにリソースが配分されているか、よく見据えてください。

戦略面でのギャップ：ビジネスとセキュリティの優先度

ビジネスリーダーとセキュリティリーダーが重視するリスクは同じものではありません。ビジネスリーダーがインフレの進行をより強く懸念しているのに対し、セキュリティリーダーは、サイバーセキュリティリスクを最大の懸念項目に挙げています。それは、後者がサイバーセキュリティ上の脅威をより身近に実感できる環境にいるからなのかもしれません。とは言え、サイバーセキュリティリスクを懸念項目のトップ3の1つに挙げるビジネスリーダーが半数近くに上る事実からも、このリスクが極めて重要であることが裏付けられます。サイバーセキュリティリスクが両者に共通する懸念事項であるということは、CISOにとっては、サイバーセキュリティ上の課題を企業の経営課題に結びつける機会の存在を意味しています。

ビジネスリーダーとセキュリティリーダーが重視するリスク低減措置

（上位1位から3位までの項目の構成比%）



質問1　以下のリスクのうち、今後12カ月間で、あなたの組織が優先的にリスク低減措置を講じようとしているものを挙げてください（上位3項目）。調査ベース：全回答者（4,042）

出所：PwC「Global Digital Trust Insights 2025」

CxOへの警鐘

ビジネスリーダーとセキュリティリーダーは、今こそ、足並みを揃えねばなりません。組織の資産を保護し、レジリエンスを構築するには、サイバーセキュリティリスクと経済的な重圧との間で折り合いをつけて、優先すべき課題を決定する必要があります。組織横断的な診断を定期的に実施することにより、あなたの組織の戦略と優先課題とを整合させることができます。

データ漏洩のコストは世界平均で300万米ドル超

CxOの4分の1以上が、過去3年間で最も甚大な被害をもたらしたデータ漏洩のコストは100万米ドルを下らなかったと言っています。これは、組織の規模を問わず、また、大半の地域や業界において、昨年の調査結果を幾分下回っています。全体的に見れば、データ漏洩への対処費用は、平均で332万米ドルと推定されます。

過去3年間において、最上位の企業（高水準のサイバーセキュリティ対策が平常時に実行されている傾向があると回答した企業）は、いかなるデータ漏洩被害も受けにくかったことが示されています。最上位にあるこのような企業は、大抵の場合、より規模が大きく、急速な成長を遂げています。そして、翌年度のサイバーセキュリティ予算を15%以上増額する見込みであると回答しています。このことから、充実したサイバーセキュリティ計画と適切な予算配分が、レジリエンスの強化に関連していることがうかがえます。

> “サイバーセキュリティとレジリエンス強化の取り組みの手を休めてはいけません。犯罪者や国家のアクターは、IDおよびアクセス管理の弱点や、パッチを適用していないデバイス、不適切なセキュリティ設定など、保護されていない「縫い目」を見つけ出すスキルを高めています”
>
> Rob Joyce：PwC米国 Cyber, Risk & Regulatory Senior Fellow（前大統領特別顧問および国土安全保障代理アドバイザー）

CxOへの警鐘

リスクの予防、検知、対応や復旧を網羅する全体的なリスク低減戦略に重点的に取り組みます。データ漏洩の影響について、単に財務的な影響のみならず、より幅広い見地から認識し、実効的なレジリエンスを構築してください。

CxOに対する行動の呼びかけ

組織を取り巻く脅威が高度化する中で、現在および将来的なリスクを診断するために、CxOが連携して積極的な役割を果たすことが重要です。CxOは、より広範な経営目標の一環としてサイバーセキュリティ戦略を位置づけることによって、リスクの管理やレジリエンスの構築に向けた備えを強化することができます。

CISO：自社のビジネスを最も危うくする脅威について、他のCxOに明確に説明します。とりわけ、投資活動に軌道修正を要する場合に重要です。

CIOおよびCTO（最高技術責任者）：CROとの対話をもとに、ある脅威によって情報やインフラの全般的な安全にダメージが及ぶ可能性がどの程度あるか、また、レジリエンスの構築上、最大の障害となるのはどのような脅威であるかを見極めます。

CFO：CISOやCROとのコミュニケーションを通じて、サイバーセキュリティにおいて重点的に取り組むべきリスク管理と優先すべき投資対象に関する理解を深めます。

CEO：CROやCISOとの定期的な面談を通じて、当該分野のCxOが最も懸念する脅威ベクトルについて認識するようにします。脅威を低減するために現在実行している取り組みについて、定例報告を受けることが重要です。

取締役：組織が直面する最大のサイバーセキュリティリスクについて理解し、経営陣に対して厳しい質問を投げかけます。その内容は、「リスク低減に向けてどのような措置が講じられているのか」「先を見越したリスク対策の実行やインシデント発生時の対応のために、適切な計画と十分な予算配分がなされているか」などです。

生成AIと新たなテクノロジー：機会とリスクのバランス

67% セキュリティリーダーの67%が、昨年を通じて、生成AIによってアタックサーフェスが増大したと回答

78% 回答者の78%が、過去12カ月間で、生成AIに関連する投資を増額

72% 回答者の72%が、AIの管理において、リスクマネジメントのための投資を増額

生成AIの急速な進歩によって、幅広い産業で新しい機会が生み出されています。しかし、それと同時にサイバーセキュリティリスクも高まっています。生成AIなどの新技術の導入が進むにつれて、組織のCxOは、より複雑で予見が困難なさまざまな課題に直面しています。このような課題として、攻撃ベクトルや統合への障害に加え、生成AIがサイバーセキュリティにおいてディフェンスとオフェンスの双方の性質を有していることも挙げられます。このような状況の根本にはデータと法律の重大な問題があり、生成AIの導入と管理が困難になる可能性があります。

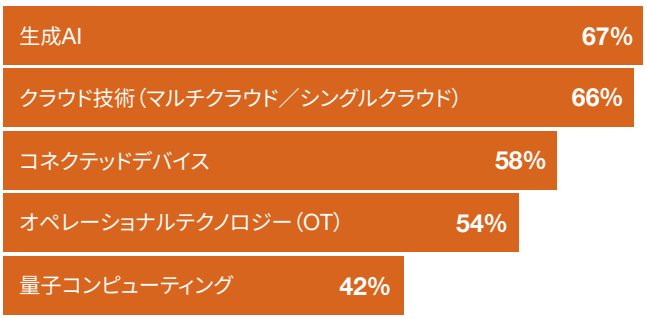
> “サイバーセキュリティは、多分にデータサイエンスの問題と言えます。サイバーディフェンダーにとって、生成AIと機械学習によってデータに近づき、タイムリーで即座に利用でき、最も重要な知見を活用できるようにすることが喫緊の課題となりつつあります”
>
> Mike Elmore：GSK社 Global CISO

アタックサーフェスの拡大

セキュリティリーダーの67%が生成AIについて、また66%がクラウド技術について、昨年を通じてサイバーセキュリティのアタックサーフェスの拡大をもたらす要因になったと回答しています。その結果、企業が高度な攻撃を受けやすくなったと指摘しています。また、生成AIによって、脅威アクターは、高度な技量がなくても、実効性のあるフィッシング攻撃や大規模なディープフェイクを容易に練り上げられるようになるかもしれません。これは、PwCが実施した第27回CEO意識調査で認められた方向性と一致しています。当該調査では、世界のCEOの64%が、生成AIにより、自らの組織のサイバーセキュリティリスクが増大すると予測しています。生成AIの利用によって、データの完全性、プライバシー、コンプライアンスに対する懸念も高まります。なぜなら、企業は、未だ発展途上にある規制上の義務に対処することになるからです。

生成AIのみならず、コネクテッドデバイスやオペレーショナルテクノロジー（OT）などの技術も、アタックサーフェス拡大の要因となっています。このことは、製造業、ヘルスケア、エネルギーなどの産業部門にも影響を及ぼすかもしれません。相互接続されるデバイスの増加につれて、このようなシステムの安全確保は一層困難になります。さらには、ようやく姿が見え始めてきた量子コンピューティングに関しても、セキュリティリーダーの42%が、既にその脆弱性への対応を余儀なくされていると回答しています。

アタックサーフェスに影響を及ぼす技術※



※「顕著に増加」「わずかに増加」回答の構成比（%）の合計値を表示
質問4　過去12カ月間において、あなたの組織のIT環境のサイバー・アタックサーフェスは、以下の各技術によってどの程度の影響を受けましたか。調査ベース：セキュリティ分野回答者（1,762）

出所：PwC「Global Digital Trust Insights 2025」

CxOへの警鐘

新たに発生する脆弱性を継続的に診断し、最新のセキュリティ対策に投資し、テクノロジー、セキュリティ、リスク対応および法務の各部門間の緊密な連携を現在以上に促進することが極めて重要です。このような脅威への準備態勢が日頃から整備されていれば、企業は最も重要な資産をより効果的に保護し、利害関係者のトラストをつなぎ止めることができます。

サイバーセキュリティディフェンスにおける生成AIの活用：機会と課題

生成AIに起因するサイバーセキュリティリスクのアタックサーフェスの拡大は大半の組織が経験していますが、CxOは、生成AI技術をサイバーセキュリティディフェンスの目的でも利用しています。生成AIの活用事例としては、脅威の検知と対応、脅威インテリジェンス、マルウェアフィッシング検知がトップ3を占めています。

このように、生成AIを活用する場はあるものの、組織のサイバーセキュリティディフェンス戦略に組み入れるには、いくつかの障害が存在しています。

既存のシステムやプロセスへの組み入れが困難（39%）

組織内関係者からの生成AIに対するトラストの欠如（39%）

内部統制とリスクマネジメントが不十分（38%）

生成AIの利用管理を目的とする内部ポリシーが標準化されていない（37%）

CxOへの警鐘

生成AIは、あなたの会社のサイバーセキュリティディフェンスに変革をもたらす可能性があります。しかし、そのためには、「責任あるAI」プラクティスを適用して、生成AIを実装し、信頼し、効果的に管理するという課題を克服しなければなりません。そうでなければ、脅威アクターとの「兵器開発競争」で、あなたの会社が後れをとってしまう恐れがあります。

サイバーセキュリティ投資の最重点は生成AI

サイバーセキュリティリスクの高まりに鑑み、CxOの78%が生成AIに対するサイバーセキュリティ投資を強化しています。特に注力しているのがガバナンスです。このような投資は、生成AIについて、機能とリスクの双方の管理が重要であることを裏付けるものです。

企業においては、量子コンピューティングへの体制固めを目的とする投資も始まっています。量子コンピューティングの実用化はまだ何年も先のことですが、将来この技術が悪用された場合の脅威に対抗すべく、既に、これに対抗できる技術や、量子コンピューティング実用化後のセキュリティ対策の追求が緊急課題となりつつあります。

CxOへの警鐘

生成AIへの投資は出発点に過ぎません。量子コンピューティングに対抗できるソリューションなど、他にも未開拓の技術を利用できないか検討を進め、あなたの会社のセキュリティディフェンスのスピードが脅威の進歩に勝るよう、もっとスピードを上げる必要があります。

CxOに対する行動の呼びかけ

サイバーセキュリティを取り巻く環境を新たな技術が塗り替えようとしています。CxOが連携して、このような革新がもたらす機会とリスクの両側面に自らの組織が適応できるよう、積極的に方向づけを行うことが極めて重要です。

CISO：テクノロジー資産全般にわたる標準化を進め、サイバーセキュリティディフェンスへのAIの実装を推進します。各々のユーザーに個別のアクセス権を付与することにより、潜在的な攻撃ベクトルを特定します。

CIOおよびCTO：投資と実装の実効性を最大化する投資項目についてビジネスリーダーを啓発できるよう、AIの影響診断を開発します。生成AIの利用増を念頭に、スケーラビリティを考慮したプラットフォームを設計します。

CFO：CISOと連携して、財務データの保護におけるセキュリティと機密性の確保に重点的に取り組みます。

CDO（最高データ責任者）：データ管理プロトコルを強化し、あなたの会社のデータプライバシーがプライバシー法や規制当局の指針に反していないか診断を行います。

CLO（最高法務責任者）およびGC（ジェネラルカウンセル）：リスクやコンプライアンスを担当する他部門と連携し、データの不正な二次利用や法的措置のリスクを防止します。

高度に規制されたサイバーセキュリティの世界：貴社の準備態勢は万全でしょうか

96% 回答者の96%が、サイバーセキュリティへの規制を受けて、過去12カ月間でサイバーセキュリティ関連の投資を増額

78% 回答者の78%は、このような規制がサイバーセキュリティに対する自らの姿勢を問い質し、改善し、強化する契機となったと認識

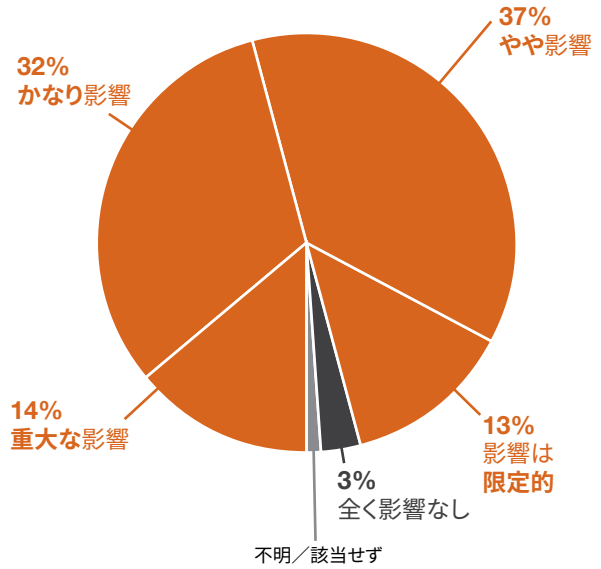
13% 回答者の13%は、AIやレジリエンス関連規制の遵守状況について、CISO/CSOとCEOとの間に自信のギャップがあると指摘

規制の枠組みで定められる要件は増加をたどっていますが、企業は速やかにこれに適合しなければなりません。デジタル・オペレーショナル・レジリエンス法（DORA）、サイバーレジリエンス法、欧州AI規制法（AI Act）、重要インフラに関するサイバーインシデント報告法（CIRCIA）、シンガポール・サイバーセキュリティ法をはじめ、新たな規制が次々と打ち出されています。こうした事実からも、組織における旧来の慣行を、高度化する要件に整合させることが急務とされている状況が分かります。企業がこのような要求に対処する際、自らの組織がこれらの要件を完璧に遵守できるか否かについて、CISO/CSOとCEOとの間で自信に顕著な相違が見られることがあります。規制に基づく監視と新たな脅威の双方に応えることができる、レジリエントで規制適合的なサイバーセキュリティ体制を整備するには、このような課題への取り組みが不可欠です。

ポジティブな変化を促進するサイバーセキュリティ規制

サイバーセキュリティ関連の規制が、サイバーセキュリティ投資の主たる牽引力となっていることが明らかになってきました。例えば、CxOの96%が、規制の要件を満たすためにセキュリティ対策を強化したと認識しています。さらには、規制の存在が、サイバーセキュリティに対する自らの姿勢を問い質し、改善し、強化する契機となったと考えるCxOが全体の78%を占めているのです。以上から、容易には遵守できない規制であっても、業界全般にわたるサイバーセキュリティ能力のレベルアップに貢献していることが分かります。

サイバーセキュリティ投資の増額に対するサイバーセキュリティ規制の影響度



質問16　過去12カ月間において、あなたの組織では、サイバーセキュリティ規制を契機にサイバーセキュリティ投資をどの程度増額しましたか（該当する場合）。調査ベース：セキュリティ分野およびCFO回答者（1,951）

出所：PwC「Global Digital Trust Insights 2025」

組織に対するポジティブな影響

サイバーセキュリティ規制は**78%**の組織にとって**有益**

24% 組織として、現行のサイバーセキュリティリスク・マネジメント・プログラム、プロセス、ガバナンス手法を強化する契機になった

20% 技術革新や変革に向けた取り組みにおける安全確保に役立った

19% 業界横断的な枠組みを管理することで、レジリエンスの強化に役立った

15% 規制の要件に取り組むために、サイバーセキュリティで管理するサービスを考慮するようになった

質問17　以下の選択肢から、過去12カ月間において、新たなサイバーセキュリティ規制があなたの組織に与えた影響として、最も当てはまるものを選んでください（もしあれば）。調査ベース：全回答者（4,042）

出所：PwC「Global Digital Trust Insights 2025」

CxOへの警鐘

規制の要件を取り入れることによって、組織におけるセキュリティの枠組みが強化され、新たな脅威に対抗し得る強力な体制が構築されます。規制の遵守は官僚的な確認作業に過ぎないと考えてはいけません。むしろ、長期的なレジリエンスを構築し、利害関係者とのトラストを築くチャンスと認識すべきです。

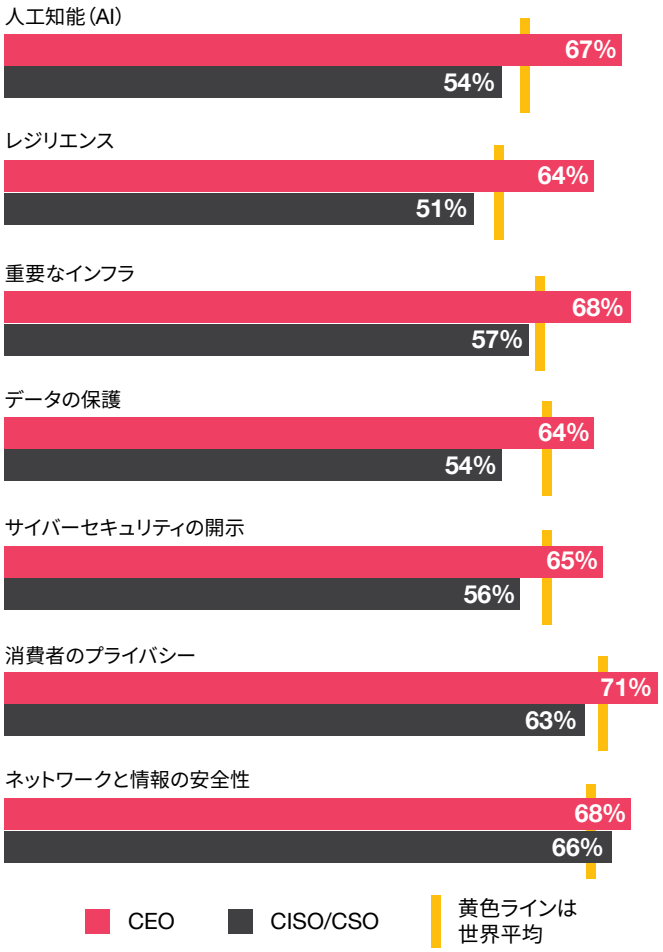
自信のギャップ：サイバーセキュリティの遵守能力に関して、CISOは、CEOほど自信を持っていない

サイバーセキュリティに関する規制は組織に有益であると確信している場合でも、自社がこのような規制をどの程度まで遵守できるかという点において、CEOとCISO/CSOとの間には、顕著な自信の相違が存在します。このような相違は、AI、レジリエンス、重要インフラの要件の遵守に関する認識で特に目立っています。サイバーセキュリティの最前線に立つCISOは、自らの組織がこのような規制の要件を満たせるかに関して、CEOよりも悲観的な見方をしています。

CISOは、日常的な運用上の問題、リソースの制約や潜在的な脆弱性など、サイバーセキュリティの遵守を阻害する恐れのある課題に、より敏感に接する立場にあります。それゆえ、組織のリーダー層との間で、このようなリスクに関するコミュニケーションをもっと効果的にとることは、極めて大きな意味を持っています。それを阻むものは何なのでしょうか。戦略的意思決定にCISOが参画できないことや、必要な規模のサイバーセキュリティリスク投資の根拠を提示できないことなどが、阻害要因となっている可能性があります。

組織の規制遵守に関する信頼度

遵守できると強く確信するCEOとCISO/CSOの構成比（%）



質問15　あなたの組織が活動する地域で以下の種類の規制が適用されることになった場合、あなたの組織はどの程度これを遵守できると思いますか。調査ベース：全回答者（4,042）

出所：PwC「Global Digital Trust Insights 2025」

CxOへの警鐘

このような自信のギャップを解消するには、セキュリティリーダーとCxOとの間でもっと綿密な調整を行い、コミュニケーションを活発化する必要があります。CEOは、CISOの意見をただ聴取するのではなく、規制の要件を遵守するために必要なリソースやサポートが行き渡るようにしなければなりません。CISOは、データに基づいた知見を提供し、コンプライアンスの強化を戦略的課題まで高めるビジネスケースを作成しなければなりません。

CxOに対する行動の呼びかけ

規制の要件によってサイバーセキュリティを取り巻く環境が形成されていく状況に変化はありません。こうした中で、CxO全体が、イノベーションのきっかけとして規制を活用しつつ、コンプライアンスの課題に先んじて取り組んでいくことが求められています。セキュリティチーム、リスク担当部門、経営幹部が横断的な調整を行うことは、規制を遵守できる体制を維持し、戦略的な強化策を推進していくために極めて重要です。

CISOおよびCRO：他の経営幹部に対して、各産業や担当地域のニーズに直接的な影響を及ぼす規制の動向に関する報告を頻繁に行います。また、テクノロジーの変化や規制改正の管理プロセスに係る業務を遂行します。

CFO：サイバーセキュリティリスク管理に関する全ての規制上の開示について、正確性、完全性、防御可能性を検証し、セキュリティ体制の計画を策定します。サイバーセキュリティリスク定量化を取り入れ、正確に診断し潜在的なリスクを周知することによって、サイバーセキュリティ・インシデントがもたらす重大性と具体的な影響について明確に理解できるようにします。

CEO：異なる事業部門にまたがる所要の調整を含め、コンプライアンスの取り組みを指導する監督責任について理解します。規制遵守に関する知識の格差を解消するために、CISOに対して問いかけるべき内容を特定します。

最高コンプライアンス責任者：規制遵守の要件に関する最新動向を常に把握します。また、CISOやCROと連携して遵守状況を定期的に確認すべく、先を見越したコンプライアンス対策やモニタリングを取り入れます。

CLOおよびGC：サイバーセキュリティ・プログラムの報告義務の遂行に必要とされる開示の程度について、透明性と秘匿性とのバランスを考慮しつつ決定します。

取締役：新たな規制の要件に関する最新の動向を把握し、新たな要件に対処するために経営陣が検討を進めている積極的方策について報告を求めます。サイバーセキュリティ・インシデントの診断と開示に対する経営陣の方針について理解します。

サイバーセキュリティリスク定量化の可能性を切り開く：貴社が躊躇している原因は?

15% サイバーセキュリティリスクがもたらす財務上の影響について、相当程度まで定量化できている組織は15%のみ

87% リスクが最も高い分野にリソースを配分することが最も重要であると87%が回答

44% サイバーセキュリティリスクの財務上の影響について定量化する際の最大の課題はデータの問題であると44%が回答

サイバーセキュリティの脅威は急速に範囲を拡大し、ますます巧妙になっています。こうした中で、サイバーセキュリティリスク定量化は、組織にとって看過できない必須のツールになっています。そのメリットは広く認識されていますが、データの質の問題やアウトプットの信頼性など、いくつかの課題も残されていることから、幅広く採用されるには至っていません。

サイバーセキュリティリスクの計測は不可欠ながら限定的

サイバーセキュリティリスクに関する重点投資分野の決定に当たりリスクの計測が不可欠とする回答が全体の88%、最もリスクの高い分野にリソースを配分するとの回答が全体の87%に達するなど、CxOの見解は大筋で一致しています。しかし、かなりの程度までこれらを実行（例：自動化および広範囲にわたるレポート作成による大規模なサイバーセキュリティリスク定量化）していると回答した組織は15%に過ぎません。

リスクの定量化を実行している組織では、CxOの10人中7人が、残存リスクの定量化に当たっては、脆弱性修復、ユーザー・アクセス・レビュー、トレーニング実施の遵守など、主要な管理が効果的になされているかを考慮しつつ、セキュリティ体制評価を利用していると回答しています。ただし、より全体的なサイバーセキュリティリスク定量化については、限定的な採用にとどまっています。

サイバーセキュリティリスク定量化のメリット

88% 優先すべきサイバーセキュリティ投資の特定が容易になる

88% リスク許容度の定義に沿ったサイバーセキュリティリスクの測定と伝達が容易になる

87% リスクが最も高い分野へのリソースの配分が容易になる

86% サイバーセキュリティリスク・マネジメント・プログラムの価値を実証できる

84% 同一条件の下で、脅威やインシデントを計測・比較できる

質問27　あなたの組織にとって、サイバーセキュリティリスクの測定を行う重要性はどの程度認められますか。以下の各項目について回答してください。調査ベース：サイバーセキュリティリスクが財務上にもたらす影響度について計測を行っているセキュリティリーダー、CEO、取締役、CFOおよびCRO回答者（1,899）

出所：PwC「Global Digital Trust Insights 2025」

CxOへの警鐘

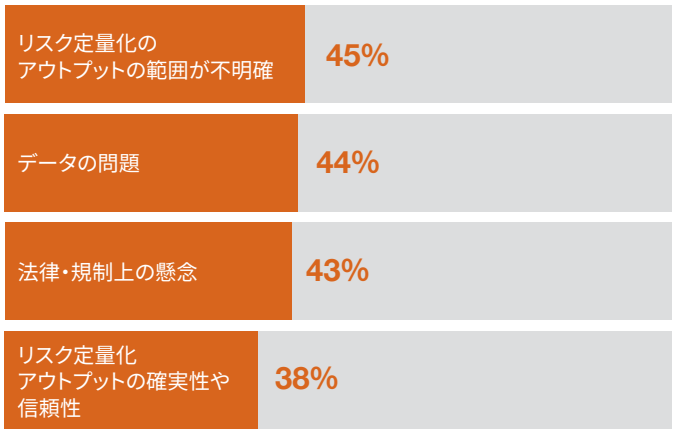
サイバーセキュリティリスク定量化の潜在力を最大限に実現すべき時期が到来しています。有用性が認識されているにもかかわらず実装が進まない現状は機会の喪失にほかならず、もはや看過することはできません。サイバーセキュリティリスクの計測を実施していないか、この潜在力を十分に活用していない組織は、特に取締役会への報告や資金配分の観点からすれば、この極めて重要なインテリジェンスを棚上げしていると言えるのです。

実装を阻害している要因は？

サイバーセキュリティリスク定量化の実用化を阻む要因の上位には、データの問題、範囲の不確実性、法的な課題が挙げられます。もう1つの要因は、定量化されたアウトプットの質に対するトラストが低いことにあります。サイバーセキュリティリスクの定量化を進めるに当たり、セキュリティ分野のCxOは、事業リスク許容度との折り合いをつける必要があります。CxOが期待する内容とCISOが開示する内容とに落差があることが、この技術の採用を一層困難にしています。

サイバーセキュリティリスクがもたらす財務上の影響の定量化における課題

（上位1～3位の項目の構成比%）

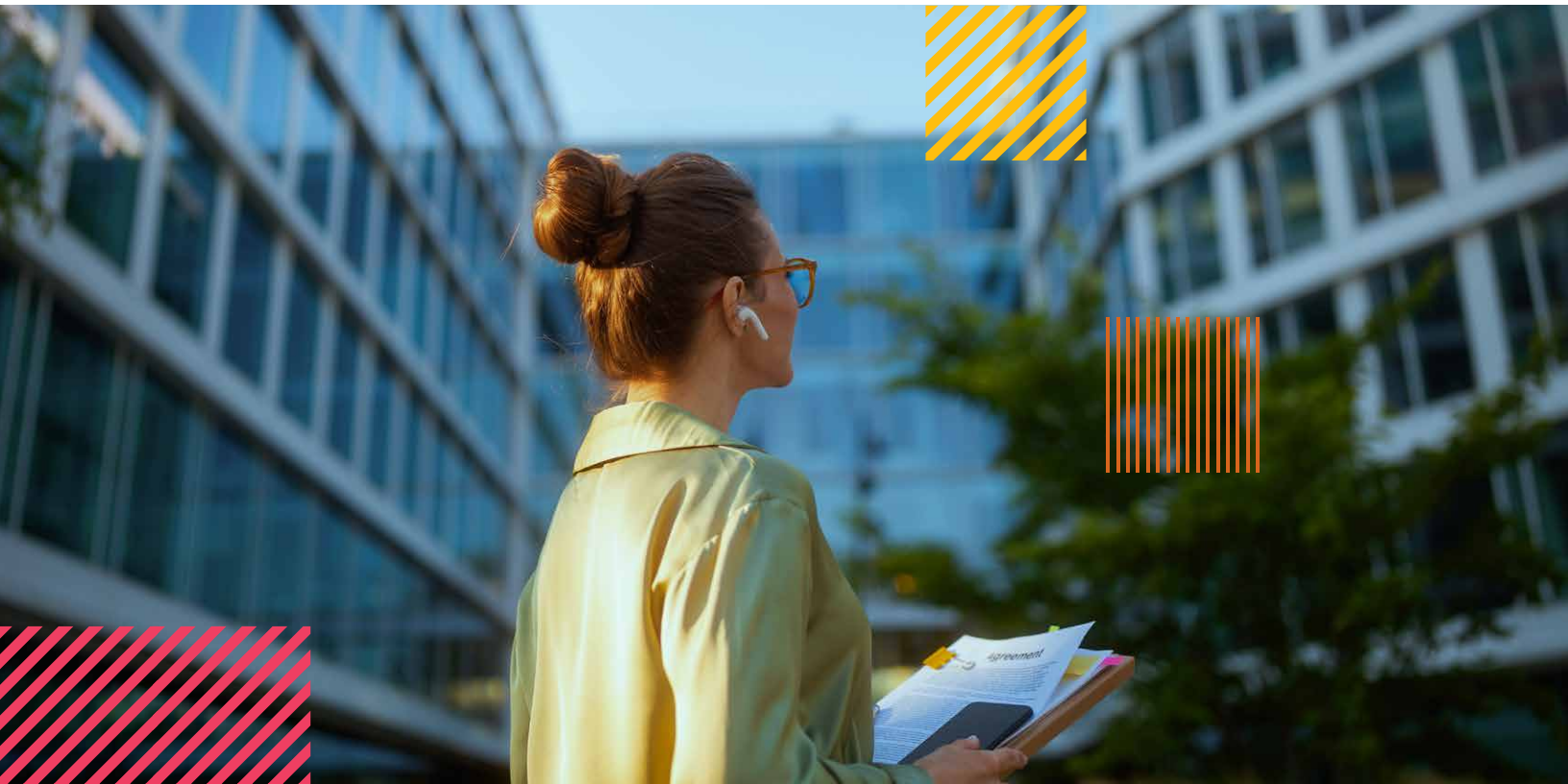


質問26　あなたの組織では、サイバーセキュリティリスクにより財務上懸念される影響を定量化するに際して、どのような困難がありましたか（もしあれば）。上位3項目を挙げてください。調査ベース：サイバーセキュリティリスクが財務上にもたらす影響度について計測を行っているセキュリティリーダー、CEO、取締役、CFO、CRO回答者（1,899）

出所：PwC「Global Digital Trust Insights 2025」

CxOへの警鐘

サイバーセキュリティリスク定量化の採用と活用の間に障害が横たわっていることから、この技術の進歩が頭打ちになっています。組織にとって、このような問題のために、最重要な意思決定を遅らせる余裕は最早ありません。障害に真正面から取り組み、サイバーセキュリティリスク定量化に対するトラストを確立し、あなたの会社の戦略的プロセスに完全に組み入れてください。



CxOに対する行動の呼びかけ

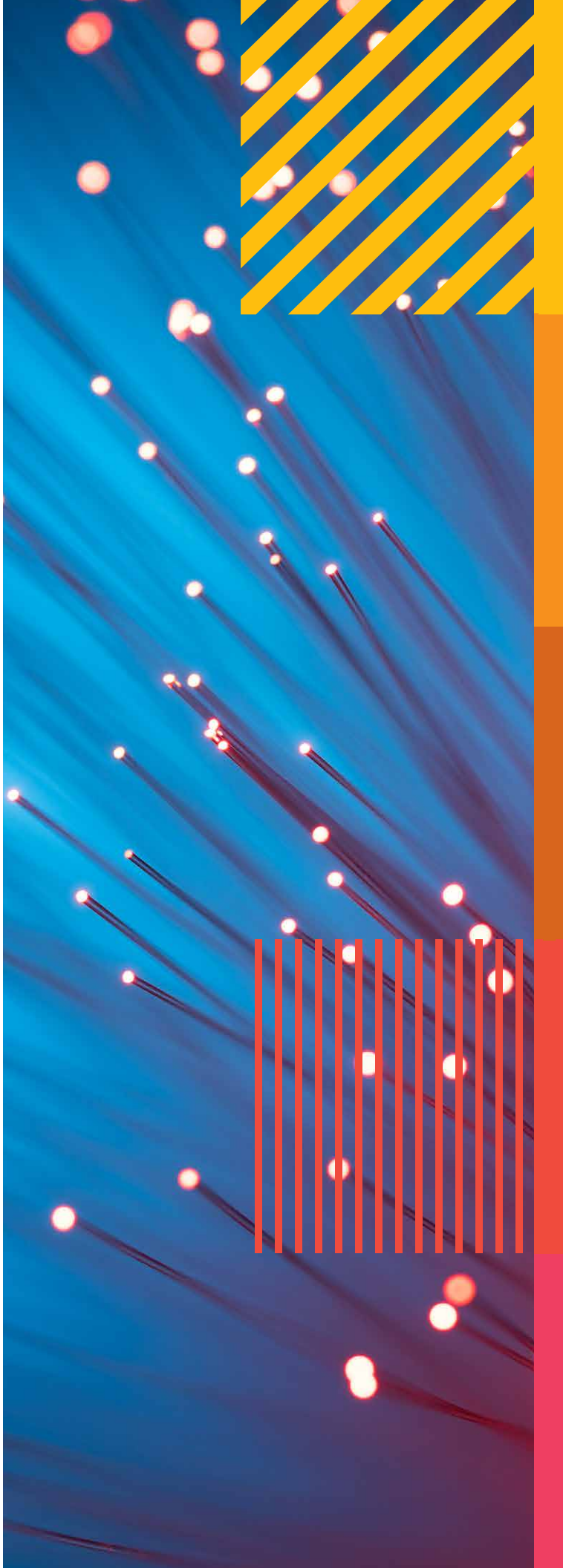
情報に基づく意思決定と戦略的投資分野の優先順位付けには、トラストのあるサイバーセキュリティリスク定量化システムの確立が不可欠です。リスクを正確に計測すれば、サイバーセキュリティの取り組みを、より広範な事業目標に合致させることができます。

CISO：具体的なアウトプットを念頭に置きながら、手の届くところからスタートするよう心がけます。あなたの組織内で入手可能な情報を有効活用します（例：コントロールの有効性、成熟度、インシデントや損害のデータ）。新しいツールがリスクの定量化に役立つことがありますが、これは必要条件ではありません。自らの計画を定義して、そのプランの実現に役立つ技術を探求します。

CISOおよびCRO：定量化ツールや定量化業務から得られる財務リスクの測定結果の中で、最も影響が大きいものをCxOに提示します。このような事例を挙げることは、最もリスクが高い分野に適正なリソースを重点的に配分するよう、組織のリーダーを説得するために有用です。

CEO：CISOやCROとの共同作業を通じて、サイバーセキュリティリスク定量化が会社の事業にもたらす価値、その潜在的なコスト、リスクを計測しないことで失われる機会についての理解を深めます。

取締役：サイバーセキュリティリスクの診断を行うためにあなたの組織で現在利用されている方法について理解します。経営陣に対して、もっと広範なリスク定量化計画を実行して、あなたの企業のサイバーセキュリティリスク体制に関する診断をより的確に行い、報告するよう求めます。



レジリエンスへの投資によるトラストの構築

77% 回答者の77%が、来年度のサイバーセキュリティ予算の増額を予想

48% ビジネスリーダーの48%が、来年度におけるサイバーセキュリティ投資の最重点はデータの保護とデータのトラストであると回答

34% セキュリティリーダーの34%が、来年度におけるサイバーセキュリティ投資の最重点はクラウドセキュリティであると回答

事業において看過し得ない重点項目として、サイバーセキュリティの位置づけは上昇し続けています。また、組織では、サイバーセキュリティは差別化の秘訣であり、企業の評判とトラストを向上させる手段としての可能性を有していると考えられ始めています。これに備えて、特にデータの保護とデータのトラストを中心に、多くの組織がサイバーセキュリティ予算を増額しています。このような分野に戦略的な投資を行うことで、企業はレジリエンスを強化するだけではなく、顧客とのポジティブな関係性も築いているのです。

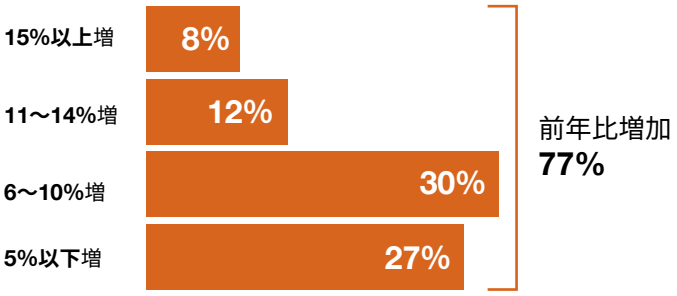
> “多方向から脅威が押し寄せ、物理的環境とデジタル環境の双方が脅かされるなど、組織を取り巻く脅威の状況は、ますます予見し難くなっています。物理的なセキュリティとサイバーセキュリティの強化を目指して、統合対応と復旧のためのリソースに投資しています。
> 脅威アクターは攻撃対象を選びません。事業の継続性とレジリエンス計画のあらゆるレベルで、攻撃への備えができていなければなりません”
>
> Georg Stamatelopoulos博士：EnBW社 CEO

来年度はサイバーセキュリティ予算の増額を予想

サイバーセキュリティ予算は昨年と同様の傾向を示しています。すなわち、比較的小規模な組織の方が、より規模の大きな組織に比べて、予算全体に占めるサイバーセキュリティリソースの割合が高くなっています。この調査結果には、既に大企業が重点的な投資を一巡させた分野で、より小規模な企業が大企業にキャッチアップしようとしていることが反映されている可能性があります。大規模な組織も新たな脅威やレジリエンスに関する懸念を表明していますが、投資については抑制的な姿勢を維持しています。大規模な組織では、セキュリティ体制が既に確立されているからかもしれません。

CxOの4分の3が、自らの組織では、来年度のサイバーセキュリティ予算が増額されるものと予想しています。この比率は、北米のテクノロジー・メディア・情報通信（TMT）業界でより高く（82%）なっています。

サイバーセキュリティ関連予算
(2025年度の前年比増減率)



質問7　2025年度におけるあなたの組織のサイバーセキュリティ予算は、前年度比でどのような変化がありますか。調査ベース：全回答者（4,042）

出所：PwC「Global Digital Trust Insights 2025」

CxOへの警鐘

2年ぶりに増額が計画されている来年度の予算は、現在と将来のリスクに見合うものでなければなりません。すなわち、レジリエンスの強化や、進化を続ける脅威の環境に組織として備えるために、配分される全ての資金が確実に充当されることが重要です。

最も問題の多い分野に投資：クラウドとデータのトラストは密接に関連

各組織では、今後12カ月にわたり、他のサイバーセキュリティ投資に優先して、データの保護・トラストとクラウドセキュリティに注力してきました。ステークホルダーの信頼とブランドインテグリティを維持するためには、センシティブ情報の保護が不可欠であると認識されています。

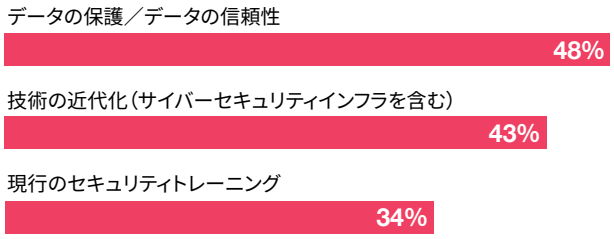
ビジネスリーダーやセキュリティリーダーは、その職務に応じて具体的に取り組むべき項目の優先順位を整理しています。

ビジネスリーダーの**48%**は、サイバーセキュリティ投資における最重点項目はデータの保護やトラストであると回答。これに次いで、技術の近代化や最適化とする回答が**43%**

他方、セキュリティリーダーについては、昨年の傾向と変わらず、クラウドセキュリティが**34%**で最上位。次いで、データの保護とトラスト（**28%**）

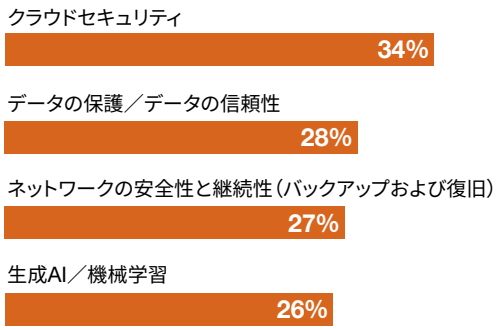
ビジネスリーダーが重視するサイバーセキュリティ投資

（上位1～3項目の構成比%）



セキュリティリーダーが重視するサイバーセキュリティ投資

（上位1～3項目の構成比%）



質問8a　今後12カ月間において、あなたの組織でサイバーセキュリティ予算を配分する場合、以下に挙げる投資対象のうち、あなたが重視する上位3項目を挙げてください（もしあれば）。調査ベース：サイバーセキュリティ予算の見直しについて認識している全ビジネスリーダー回答者（1,867）

出所：PwC「Global Digital Trust Insights 2025」

質問8b　今後12カ月間において、あなたの組織でサイバーセキュリティ予算を配分する場合、以下に挙げる投資対象のうち、あなたが重視する上位3項目を挙げてください（もしあれば）。調査ベース：サイバーセキュリティ予算の見直しについて認識している全テクノロジー分野回答者（2,092）

出所：PwC「Global Digital Trust Insights 2025」

サイバーセキュリティ投資と重点項目

クラウドセキュリティに注意すべき状況が変わらないのはなぜでしょうか。何年にもわたって投資が継続してきたにもかかわらず、クラウド技術の急速な広まり、クラウドハイパースケーラーの統合、ハイブリッドクラウド環境やマルチクラウド環境の拡大に伴い、クラウド環境にリスクが集中するようになっています。このようなリスクの集中によって、データアクセス構成の誤りやデータ侵害、統合の難しさによる悪影響がもたらされる可能性が高まります。脅威アクターが進化する中、クラウドセキュリティ戦略もまた進化を続けなければなりません。すなわち、このように増大するリスクの低減を目的とする投資を継続して行うことが不可欠なのです。

CxOへの警鐘

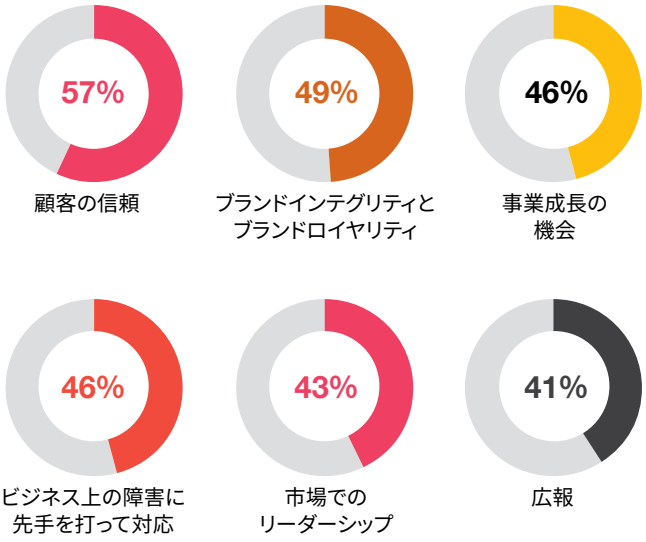
サイバーセキュリティへの投資は、トラストへの投資を意味します。あなたの組織が目指すものがクラウドの安全性、データの安全確保、新たなリスクへの対処のいずれであったとしても、このような分野に取り組んでいるという事実がステークホルダーの信頼を獲得し、あなたの組織のレジリエンス強化に結びつくのです。

サイバーセキュリティとトラスト：新たな競争力の源泉

サイバーセキュリティは、より多くの組織で、競争上優位に立つための差別化の重要な手段であると見なされるようになっています。例えば、影響をもたらす要素として、CxOの57%が顧客の信頼を、また49%がブランドインテグリティとブランドロイヤリティを挙げています。サイバーセキュリティの脅威がエスカレートする中で、強力なサイバーセキュリティ体制を構築することは、単なる防護の強化にとどまるものではありません。それは、顧客や利害関係者から頼りにされる評判を築くことでもあるのです。トラストが不可欠とされる今日、サイバーセキュリティを重視する企業は、安全性と完全性の双方において傑出した存在であることをアピールできる立場にあります。

競争上のアドバンテージとしてのサイバーセキュリティの位置づけ

（「かなりの程度」を選択した回答者の構成比%）



質問19　あなたの組織では、このような分野での競争上のアドバンテージとして、サイバーセキュリティをどの程度高く位置づけていますか。調査ベース：全回答者（4,042）

出所：PwC「Global Digital Trust Insights 2025」

CxOへの警鐘

サイバーセキュリティは、単にデータの安全を確保するだけでなく、組織のブランドの安全を確保することでもあるのです。厳しい競争環境の中で、全てを決するのはトラストです。今こそ、あなたの組織のセキュリティ対策を強化し、データインテグリティにおけるリーダーとしての地位を確固たるものにしましょう。

CxOに対する行動の呼びかけ

サイバーセキュリティ投資の増額に向けた体制が整った状況において、CxO全員が、自らの戦略を、組織が直面する最も切迫したリスクに整合させなければなりません。CxOは、現時点の脆弱性に対処するための投資に加え、トラストとレジリエンスを構築するための投資も行うべきです。

CIO、CTO、CISO：主な成果のビジネス価値（例：ミッションクリティカルなデータの復旧に要する時間の短縮、システムのパッチング）に基づいて、データ保護とクラウドセキュリティにおける重点投資項目に係るビジネスケースを、分かりやすくCFOに説明します。

CFO：利害関係者のトラストを獲得するとともに、より情報に基づいた形でサイバーセキュリティ投資に係る意思決定を行い得るように、データ保護やクラウドセキュリティがどの程度のビジネス価値を有するか決定します。

CDO：テクノロジー、セキュリティ、財務の各分野のCxOと連携して、データの安全性と完全性において最も重視すべき項目を絞り込み、情報投資やクラウドセキュリティ投資戦略の指針とします。セキュリティ投資を増額するには、データの質や体制の整備状況を確認する必要があります。

貴社のサイバーセキュリティ戦略とリーダーシップは、レジリエンス強化を効果的に推進できているでしょうか

2% 調査対象の全分野について、組織全体を通じてサイバーセキュリティレジリエンスのための活動を行っている組織は、全体のわずか2%

21% 最大のリスクにサイバーセキュリティ予算が通常配分されている組織は、全体の21%のみ

50% サイバーセキュリティ投資関連の戦略計画の策定に相当程度参画しているCISOは、全体の半数

将来の脅威に対処するには、投資を行うだけでは十分とは言えません。組織におけるサイバーセキュリティ戦略への取り組み方やリーダーシップの見直しも必要です。レジリエンス強化の取り組みは停滞し、戦略的意思決定へのCISOの参画も進捗していません。このことからも、戦略的な調整を必要とする分野が残されていることは明らかです。レベルアップを図るには、サイバーセキュリティの最先端を走る組織において実行されている手法を取り入れるべきです。さらに、既知の脅威に対処するにとどまらず、アジャイルでセキュア・バイ・デザインの手法をビジネスに取り入れることにより、トラストを構築し、永続的なレジリエンスを目指すことが重要です。

> “組織に内在する脅威について説明し、このような脅威を組織の脆弱性と結びつけることは、CISOの責務です。これは、既に企業として対処する備えができている脅威とそれ以外のものについて、関係者を啓発することを意味します。教育推進型のアプローチをとることにより、組織全体にわたって連携が強まる傾向があります”
>
> David Bruyea：Moneris社 CISO

部分的な実装だけでは不十分

サイバーセキュリティリスクに対する懸念は高まっているものの、自社の主要な活動全体をカバーするサイバーセキュリティレジリエンスを完全に実行することは、多くの企業にとって依然として容易ではありません。関係者、プロセス、テクノロジーの全般をカバーする12項目のレジリエンス活動について実施した調査において、自らの組織ではこのような活動のいずれか1つを完全に実行していると回答したCxOは全体の42%（またはそれ以下）にとどまりました。さらに懸念されることは、この12項目のレジリエンス活動が組織全体にわたって完全に実行されているという回答がわずか2%しかないことです。このような状況から、顕著な脆弱性が手つかずのまま残されていることがうかがえます。すなわち、企業全体をカバーするレジリエンスがなければ、活動の全てを危険に陥れかねない脅威の増大という、憂慮すべき事態に晒され続けるということです。

以下に例示するのは、組織横断的に検討すれば効果が高いと期待される主な分野です。

レジリエンスチームを編成（組織横断的にこれを実行していると回答したCxOは、全体の**34%**のみ）

ITロスの可能性に備えたサイバー・リカバリー・プレイブックの作成（組織横断的に実行しているとの回答は全体の**35%**のみ）

テクノロジー依存状況のマッピング（組織横断的に実行しているとの回答は全体の**31%**のみ）

組織全体をカバーするサイバーセキュリティレジリエンス活動の実行

全ての分野で、組織横断的に実行している回答者は**わずか2%**

関係者

- 外部の利害関係者（規制当局、投資家）への報告 35%
- 事業継続、サイバーセキュリティ、危機管理部門のメンバーで構成するレジリエンスチームの設立 34%
- 分析や事故対応を行うために、地元の法務当局との関係を構築 31%

プロセス

- 重要なビジネスプロセスの特定 42%
- 「ITロス」の可能性に備えたサイバー・リカバリー・プレイブックの作成 35%
- 主要なテクノロジープロバイダーとの間で、インシデント対応を調整するためのプロトコルの確立 35%
- 机上演習やシミュレーションの実行 33%
- 公式なプロセスを通じて同業者と情報共有し、システミックリスクを回避 32%

テクノロジー

- サイバーセキュリティ復旧ソリューション（イミュータブルバックアップを含む）の実装 39%
- テクノロジー依存のマッピング 31%
- オペレーショナルテクノロジー（OT）資産の可視化を容易にするツールの実装 31%
- サイバーセキュリティディフェンスとレジリエンスを目的とする量子コンピューティングの導入 23%

質問10　あなたの組織では、以下のサイバーセキュリティレジリエンス活動をどの程度実行（または実行を計画）していますか。調査ベース：全回答者（4,042）

出所：PwC「Global Digital Trust Insights 2025」

CxOへの警鐘

サイバーセキュリティレジリエンスで後手に回れば、あなたの組織はリスクに直面します。テクノロジー、プロセス、関係者の全てをカバーする全社横断的な行動を起こすことによって、あなたの組織のディフェンスに変革をもたらし、将来の課題に備えることができます。

サイバーセキュリティレジリエンスは最優先すべき分野です。この最重点分野において、多くの企業が後れを取っているのはなぜでしょうか？

主要なサイバーセキュリティ活動の実行面では、依然として多くの企業が後れを取っています。このような活動が日常的に行われていると回答したCxOは、およそ5人に1人に過ぎません。例えば、将来のサイバーセキュリティリスクを常に予測しているCxOは20%に過ぎず、組織が直面する最大のリスクにサイバーセキュリティ予算を概ね配分しているものは21%にとどまっています。このような停滞には、いくつかの要因が考えられます。例えば、戦略的に先を見通せないこと、リソースが不十分なこと、そして、サイバーセキュリティに対して受動的な対応にとどまり、先手を打てないことなどです。

組織においてサイバーセキュリティチームが「通常」行っている活動

（常時81～100%）

- サイバーセキュリティ上の重大な障害に耐えられるように、制御を行い、脅威に迅速に対処 26%
- 組織のサイバーセキュリティ体制に影響力のある他の事業部門と連携 22%
- サイバーセキュリティリスク環境の変化や規制の改正、低減手段の変更に関する知見をCEOや取締役と共有 22%
- 組織において最もハイリスクの分野にサイバーセキュリティ予算を配分 21%
- マクロ環境や新たなテクノロジー、事業戦略を前提条件として、将来のサイバーセキュリティリスクを予測 20%

質問28　最後に、あなたの組織のサイバーセキュリティチームは、どの程度一貫して以下の各項目を実行していますか。調査ベース：全回答者（4,042）

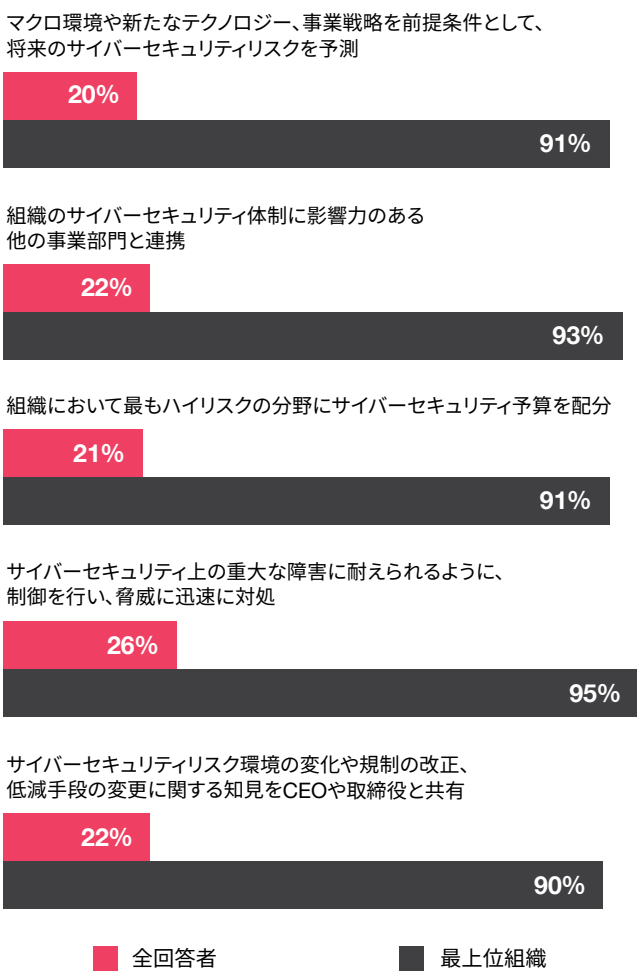
出所：PwC「Global Digital Trust Insights 2025」

最先端の企業は、一貫して他を大きく凌いでいます

PwCでは、この疑問をさらに解明すべく、このような行動を「常々」とっているという、最も先進的なCxOの一群を割り出してみました。先端を走る最上位の企業と世界平均的な企業との間には、あらゆる行動において69ポイント以上の差があります。最上位にある企業は、自らの組織の規制遵守能力について、より強い自信を持っている傾向が見られ、組織全体にわたって主要なレジリエンス活動が行われています。

最上位組織とその他組織の間に見られるサイバーセキュリティチームの活動状況の相違

「通常（全体の81～100%）」回答の構成比



質問28　最後に、あなたの組織のサイバーセキュリティチームは、どの程度一貫して以下の各項目を実行していますか。調査ベース：全回答者（4,042）、最上位組織回答者（222）

出所：PwC「Global Digital Trust Insights 2025」

CxOへの警鐘

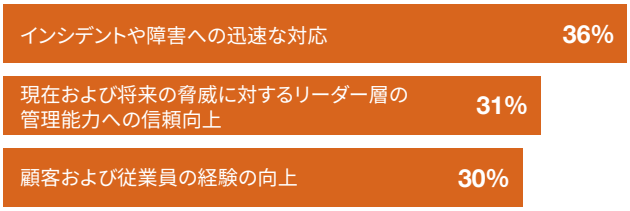
格差を解消するには、組織のサイバーセキュリティ戦略を、受け身から攻めの姿勢に転換する必要があります。例えば、リスク予測の精緻化、より戦略的な予算配分、改善に向けた継続的な取り組みなどがこれに該当します。

戦略的な重点項目：スピード、トラスト、ステークホルダーの安全確保

CxOの3分の1以上が、今後12カ月間に、インシデントや障害への対処に要する時間の短縮に向けた取り組みを予定しています。その他の重点目標としては、リーダー層の脅威管理能力に対する自信の向上に加え、顧客と従業員の双方に経験を積ませることなどがあります。このような目標は、リスク低減の迅速化を図るだけでなく、トラストの構築や、顧客・従業員の安全確保といった、より幅広い取り組みでもあります。

サイバーセキュリティとプライバシーに対する組織の目標

（上位1～3位の構成比%）



質問23　サイバーセキュリティとプライバシーとの関連において、あなたの組織は、今後12カ月間に、どのような戦略や、関係者と投資の目標を有していますか（もしあれば）。上位3項目を挙げてください。調査ベース：全回答者（4,042）

出所：PwC「Global Digital Trust Insights 2025」

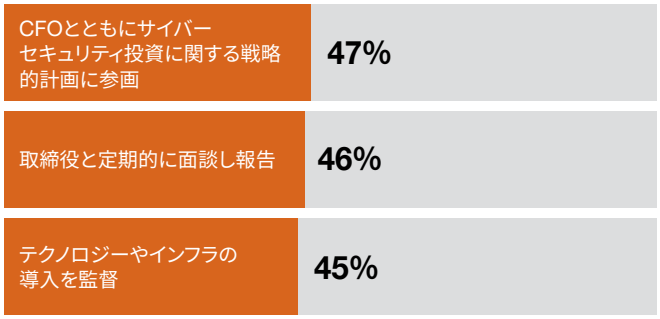
CxOへの警鐘

迅速な対応は、単なる目標ではなく必要条件です。脅威への対応が遅れれば、費やされた時間以上にコストが嵩む可能性があります。そして、トラストの低下と、事業の著しい混乱につながる恐れがあります。リーダー層が自信を持って迅速に対処することは、議論の余地のない優先課題です。

CISOの地位の向上：戦略とセキュリティの整合化

組織の重要な取り組みにCISOを十分に参画させていないことにより、多くの組織が、またとない機会を逃しています。サイバーセキュリティ投資に関する戦略的な計画の策定、取締役会への報告、テクノロジーの導入管理にCISOが概ね参画していると回答したCxOは、全体の半数を下回ります。このような齟齬が存在すると、組織における戦略の整合性が損なわれ、セキュリティ体制の弱体化につながります。

事業活動にCISOが「かなりの程度」参画



質問21　あなたの組織では、以下の各分野において、CISOが積極的な役割を果たすためにどの程度まで参画していますか。調査ベース：CISOを除く全回答者（3,640）

出所：PwC「Global Digital Trust Insights 2025」

CxOへの警鐘

CISOが意思決定のテーブルにつくことを認めましょう。企業が直面する中心的なリスクであるサイバーセキュリティに関して先を見越した対策を講じるために、CISOの知見は欠かせません。組織の最上層部にCISOを参画させることによって、組織にとって極めて重要な資産の安全確保と、レジリエンス強化の取り組みとの整合化を行うことが容易になります。

CxOに対する行動の呼びかけ

サイバーセキュリティにおける強力なリーダーシップには、組織全体を見渡す戦略的なビジョンと調整を必要とします。このような調整を進めることは、各々のエグゼクティブの責務です。それには、CISOを重要な意思決定に参画させることから、レジリエンスを最重点項目に据えて取り組むことまでが含まれます。

CISO：他のCxO向けのビジネスケースを作成し、サイバーセキュリティリスクの低減を目的とする戦略、計画および監督、ならびにレジリエンス戦略にCISOが参画することが不可欠である理由を説明します。

CEO、CFO、CIO：サイバーセキュリティレジリエンスの診断とその演習に参画し、主要な活動、基準および管理の統合を進めるに当たってCISOが直面することが想定される齟齬やその手法に関する理解を深めます。

取締役：あなたの組織のサイバーセキュリティリスクや組織が直面する脅威をはじめとして、サイバーセキュリティリスク計画の策定に関する情報を常に入手し、拡大する監督・管理責任に応えられるようにします。

本調査について

「Global Digital Trust Insights 2025」は、2024年5月から7月にかけて、ビジネスリーダーおよびセキュリティリーダー4,042名を対象に実施した調査です。

回答者の4分の1は売上高50億米ドル以上の大企業のCxOです。回答企業の業種は、製造・サービス業（21%）、テクノロジー・メディア・通信（20%）、金融サービス（19%）、小売・消費財（17%）、エネルギー・ユーティリティ・資源（11%）、ヘルスケア（7%）、政府・公共サービス（4%）と多岐にわたっています。

回答者は77カ国に拠点を置いており、その地域別分布は、西欧（30%）、北米（25%）、アジア太平洋（18%）、中南米（12%）、中・東欧（6%）、アフリカ（5%）、中東（3%）となっています。

「Global Digital Trust Insights」調査は、以前は「グローバル情報セキュリティ調査（GSISS）」として知られていたものです。今年で27年目を迎える本調査は、サイバーセキュリティの動向に関する年次調査として最も長い歴史を有しています。また、サイバーセキュリティ業界で最大規模の調査でもあり、セキュリティリーダーだけでなく、シニアビジネスリーダーの参画を得ている調査としても他に類を見ないものです。

本調査は、PwCで世界の市場調査とインサイト提供を担当するCentre of Excellenceである PwCリサーチが実施しました。

本レポートに関するお問い合わせ

Sean Joyce
Global Cybersecurity & Privacy
Leader US Cyber, Risk & Regulatory
Leader PwC US
sean.joyce@pwc.com | LinkedIn

日本のお問い合わせ先

PwC Japanグループ

www.pwc.com/jp/ja/contact.html

pwc

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12,700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、社会における信頼を構築し、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界149カ国に及ぶグローバルネットワークに370,000人以上のスタッフを擁し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細は www.pwc.com をご覧ください。

本報告書は、PwCメンバーファームが2024年10月に発行した『Global Digital Trust Insights 2025』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。
オリジナル（英語版）はこちらからダウンロードできます。
https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html

日本語版発刊年月：2025年2月　　管理番号：I202410-11