KPMG

KPMG サイバートラストインサイト2022

サイバーセキュリティとプライバシー保護による
信頼の構築

コンテンツ

概要

サイバーセキュリティとプライバシー保護による信頼構築のために重要な5つのステップ

ビジネスにおいては「信頼」がすべてです。不確実で絶えず変化する環境のなかで、顧客や従業員、投資家は信頼できる組織を求めています。そして、信頼を築き守るためには、組織全体が連携して一貫した統一ビジョンを提供することが必要です。

デジタル化された世界ではいずれのビジネスにおいても、情報の収集と処理における公正さ、誠実さ、透明性が成功のカギとなります。そのため、組織はレジリエントで信頼性が高く、混乱に直面しても迅速に対応できなければなりません。安心して取引したいと思う顧客やクライアントにとっても、取引先、投資家、規制当局、社会といったあらゆる組織を取り巻く幅広いエコシステムの一部にとっても、デジタルトラスト（デジタル技術の活用への信頼）は重要です。

デジタルトラストを築き維持するためには、サイバーセキュリティとプライバシー保護が不可欠です。企業はデータ収集を強化し、人工知能（AI）や機械学習（ML）技術の利用を拡大し、環境・社会・ガバナンス（ESG）の課題解決に取り組んでいますが、これらに関連する規制・基準はますます厳しくなっています。

「KPMGサイバートラストインサイト2022」では、約1,900人の上級管理職を対象に調査するとともに、世界中の企業リーダーや専門家と議論を重ね、経営層がどの程度これらの状況や課題を認識しているか、どのように課題に取り組んでいるか、次に何をすべきかを分析しました。また、最高情報セキュリティ責任者（CISO）が果たすべき重要な役割についても調査しました。

これらの調査により、サイバーセキュリティを通じて信頼を築くための5つの重要なステップ、**1）サイバーセキュリティやプライバシー保護をビジネスと結びつけて扱うこと、2）社内の協力関係を築くこと、3）CISOの役割を再認識すること、4）経営層の支持を得ること、5）エコシステムを頼ること、**を特定しました。

主な調査結果

データの洪水

企業は大規模なデータマイニングを行っており、データ保護・利用・共有の方法に関する懸念が高まっています。

回答者の大多数は、過去1年間に顧客データの広範な収集や分析に取り組んだと回答しています。

組織にとって、**データドリブン型の活動に対する投資**の優先度が高まっています。

AIやMLの挑戦

AIやML（機械学習）をビッグデータの分析に活用することに対し、倫理、サイバーセキュリティ、プライバシー保護の観点で社会的にもビジネスの面でも懸念が高まっています。

78% の回答者が「AI/MLの導入はサイバーセキュリティの課題をもたらす」と回答しています。

4人に3人 の回答者が「AI/MLの導入は、基本的な倫理の課題をもたらす」と回答しています。

価値と信頼

信頼はかつてないほど重要になっており、その影響を受けるのは組織の評判のみにとどまりません。信頼を向上させることで、競争優位性の獲得や、利益の拡大が可能となります。

3分の1以上 の組織は「信頼を向上させることで収益性を向上できる」と回答しています。

65% の回答者が、一方で情報セキュリティは「長期的な戦略というより、コンプライアンス面での必要性による」と回答しています。

規制の厳格化

規制当局はこれらの問題に大きな関心を寄せており、多くの企業は複雑化するグローバルな規制環境に太刀打ちできるか不安を感じています。

36% の回答者が「デジタルサービスプロバイダーに業務を委託する場合、サイバーセキュリティに関する既存または新規の規制に準拠しているかどうか懸念している」と回答しています。

34% の回答者は「サイバーセキュリティに関連する企業報告書の開示について懸念している」と回答しています。

信頼されるコミュニティ

過度に接続されたエコシステムを成功させるには、外部との連携が欠かせません。しかし、実際にはさまざまな障壁が連携を阻んでいます。

79% の回答者が「効果的なサイバーセキュリティにはサプライヤーの建設的な関与が不可欠」と述べているにもかかわらず、「その実現に向けて実際に協力している」と答えた回答者はわずか42%にすぎません。

60% の回答者が「サプライチェーンの脆弱性によって攻撃される可能性がある」と回答しています。

CISOの役割の変化

デジタルトラストの構築に向けて組織全体で取り組む際にCISOが果たすべき役割について、組織は認識しているでしょうか？

2人に1人 の経営層が取締役会とCISOの関係が「高い信頼」によって成り立っているか、疑問に感じています。

3人に1人 の回答者が、「CISOは重要な幹部としてみなされていない」または、「CISOは組織とそのデータを守るために必要な影響力を持っていない」と回答しています。

信頼されるパーパス

企業はデジタルトラストとESGの課題とのつながりを認識しているのでしょうか？

5社に1社未満

が「CISOのチームはESGチームにとって不可欠な要素」と回答しています。

50% の回答者が「CISOのチームはESGへの取組みに関し、非常に限られた役割のみ、またはまったく関与していない」と回答しています。

＊本レポートでは、少数点第1位で四捨五入しているため、図表のパーセンテージ合計は100%とならない場合があります。

1

デジタルの進化

信頼への投資がなぜ必要なのか

信頼とは何か？

信頼の定義を明確にすることで、企業は信頼度合いを測り、高め、潜在的な利益を顕在化することができます。

デジタルトラストとは、ステークホルダーの利益を守り、社会からの期待に応え、企業価値を維持するという目的に向けて、デジタル技術を活用する組織に対し、ステークホルダーが抱く信頼のことです。

組織によって、優先順位や構成要素が異なりますが、一般的にデジタルトラストは、以下の概念を指しています。

セキュリティと信頼性

組織の持つ技術やデータを計画通りに運用しつつ、それらを適切に保護すること

包括的かつ倫理的で、責任感を持った活用

組織が人、社会全体、環境やステークホルダーに配慮し、技術やデータを確実に設計、構築、運用すること

説明責任と監視

組織が信頼性についての役割を明確に定義し、それを社内で適切に割り当て監視すること

「なぜ信頼が重要か」が利益と顧客ロイヤルティ向上へのカギ

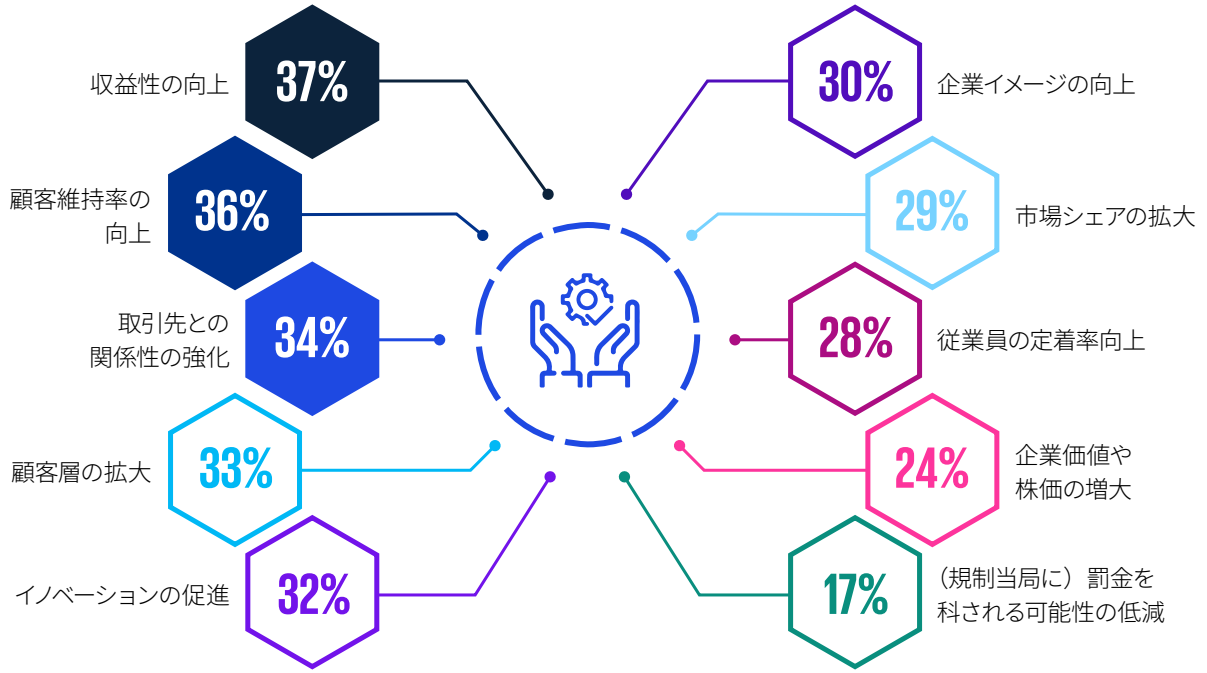
回答者は、信頼性の向上がもたらす効果として以下の項目を上位に挙げました。

1. 収益性の向上
2. 顧客維持率（カスタマーリテンション）の向上
3. 取引先との関係性の強化

そのほか、イノベーションの促進、従業員の定着率向上、市場シェアの拡大といった効果も期待できます。

信頼性の向上による主なメリット

各選択肢を上位3つに選んだ回答者の割合



データに投資し、カスタマーエクスペリエンスに注目する企業

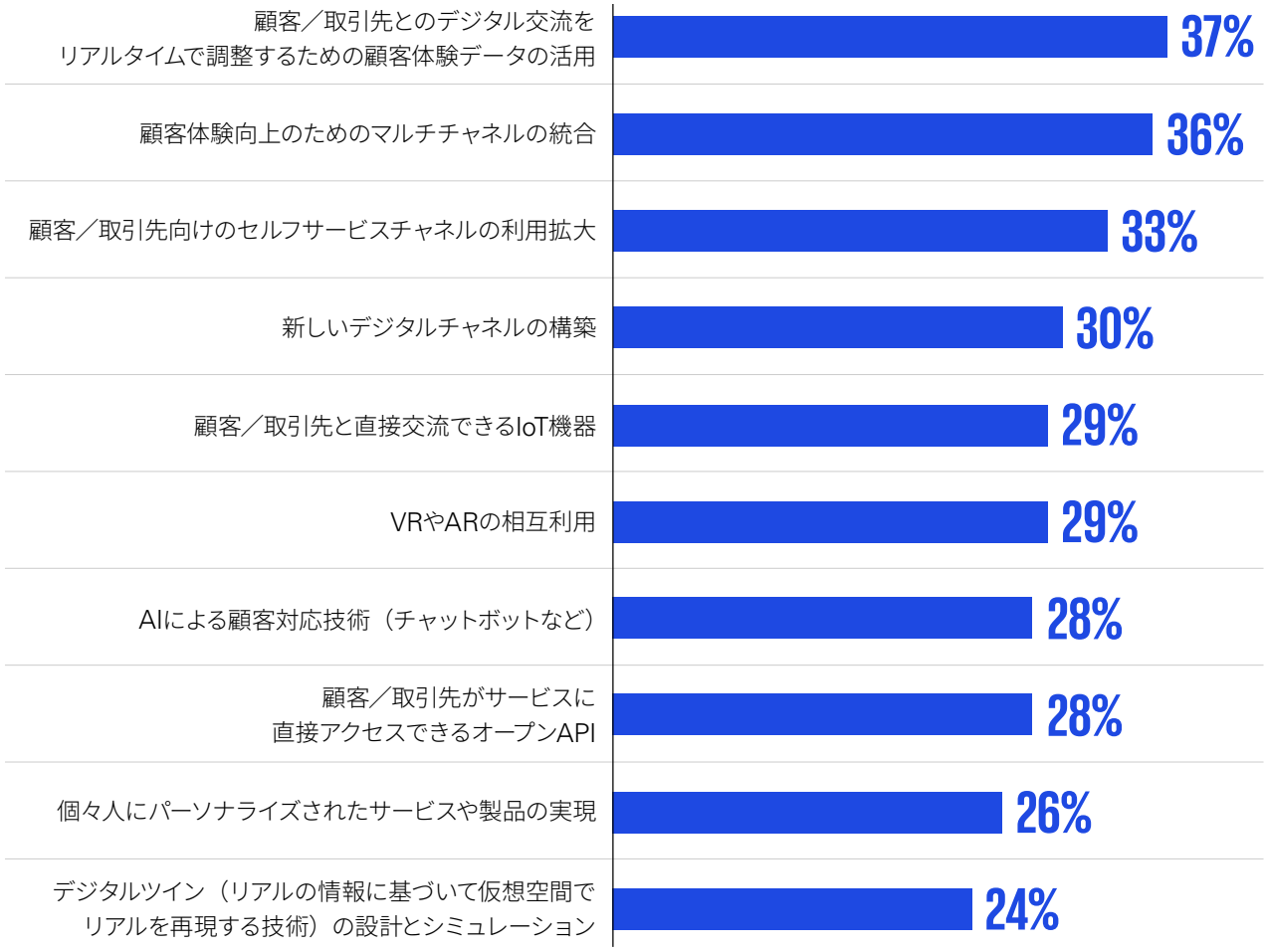
デジタルトランスフォーメーション（DX）は本格化してきています。さまざまな業界の企業が、テクノロジーを見直し、高度なデータ分析を業務の中心に据えようとしています。今後3年間で、企業は成長を加速させるためにデジタルツールに継続的に投資を行う予定であり、顧客や取引先とのやり取りの最適化や、業務の効率化、集めたデータからの新たな価値の創出を目指すでしょう。ただ、新しいデータ活用を開始するたびに、企業は潜在的な脆弱性と評判低下のリスクにさらされるため、防衛策を講じて信頼の維持に取り組む必要があります。

KPMGグローバルテクノロジーレポート2022では、顧客チャネルのデジタル化は、ハイブリッドな働き方の導入に次ぐ重要なサイバーセキュリティ課題とされています。本調査では、デジタルエクスペリエンスのどの分野に投資しているか、という問いに対して、37%の企業が「デジタル交流をリアルタイムで調整するために顧客体験データの活用に力を注いでいる」と回答し、36%が「顧客体験向上のために、マルチチャネルの統合に投資している」と回答しています。

このようなトレンドが各業界で加速するなか、顧客のプライバシーに対する要請も変化しています。ユーザーはデバイスやチャネルごとにプライバシー管理をカスタマイズできることをますます望むようになっており、企業は今後設計する製品やサービスに、柔軟なプライバシー管理機能を組み込むことが求められています。

デジタルエクスペリエンスへの投資対象として上位の分野

各選択肢を上位3つに選んだ回答者の割合



サイバーセキュリティとプライバシー保護への当社の投資は、顧客の信頼に応えるためです。

Bashar Abouseido氏
SVP and CISO, Charles Schwab

サイバーセキュリティは変化し、データはこれまで以上に重要となる

このような状況で、企業には信頼を確立するために不可欠な領域でのセーフガードの強化が求められています。回答者の80%以上が、データ利用に関する透明性向上など「サイバーセキュリティとデータ保護の改善が重要」と認識しています。また、51%の回答者が「サイバー攻撃からIT資産を保護することが大切」とみています。

組織がDXを進める過程で、サイバーセキュリティとプライバシー保護への投資は、戦略的イニシアティブの達成に必要不可欠なものとみなされるようになりました。Shell社のCISOであるAllan Cockriel氏は、「変革型デジタルサービスの成功は、組織がセキュリティとプライバシー保護をそのサービスの設計と実装に織り込めるかにかかっています」と述べています。さらに、「我々は技術を構築する際に『セキュリティ・バイ・デザイン・スタンダード』に重点を置いています。当社の義務は、信頼を維持・向上させることであり、顧客に対し透明性の高い基準を掲げたいと考えています」と続けています。

また、Charles Schwab社でSVP兼CISOを務めるBashar Abouseido氏は「顧客の信頼に応えることが、サイバーセキュリティとプライバシー保護への当社の投資の原動力です。プライバシー管理とデータ保護の透明性について、積極的かつ継続的な改善を通じ、顧客から期待される以上のことにも取り組んでいます」と述べています。

KPMGの視点：先端技術の成功に向け、信頼は必要不可欠に

分散型台帳技術（DLT）、量子コンピューティング、5G、AIやML、ARやVRのような最先端テクノロジーの開発が急速に進められており、これらがビジネスのあり方を変えることは論をまちません。

ただ、これら最先端技術によって今後生まれるアプリケーション（コネクテッドエコノミー、スマートシステム、NFT、メタバース等）の成功は、さまざまな側面で信頼を獲得できるかにかかっています。言い換えれば、透明性、信頼性、誠実性を伴ったサイバーセキュリティおよびプライバシー管理を組み込む必要があるということです。

Atul Gupta
Partner and Head of Digital Trust and Cyber Security Services
KPMGインド

2

デジタルトラストの動向

信頼を構築するのは何か

AIの倫理的課題に向き合う

多くの企業でAIやMLの利用が進むにつれ、新たな（いまだ誤解されている）信頼問題が生じています。KPMGの調査では、多くの企業がAIとMLを導入する方針を決め、効率性・生産性の向上から顧客・市場の予測能力の向上まで多岐にわたる効果が期待されていることがわかりました。

これらの技術は、取扱いを間違うと、サイバーセキュリティやプライバシーのリスクを高め、風評被害や規制当局の制裁を受ける可能性があるという危険性をはらんでいます。

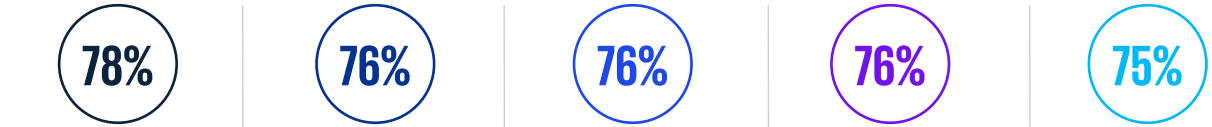
組織はこういったリスクを認識し始めています。回答者の4分の3以上（78%）が「AIとMLが特別な注意を必要とするサイバーセキュリティの課題をもたらす」と回答しています。大多数が「これらのテクノロジーを導入する際には解決すべき基本的な倫理的課題がある」と考えており、これらの課題への対応について「組織は一段とオープンに開示していく必要がある」と答えています。

これらの事実は、倫理的な議論の形成とリスク管理を支援するうえで、サイバーセキュリティとプライバシーのチームが果たす重要な役割を明確に示しています。

Microsoft社 Security Business Developmentのコーポレートバイスプレジデントであるann Johnson氏は、「我々がデータポイズニング、マシンドリフト、AI攻撃といった敵対的AIへの対応を重視しているのは、これらが次の攻撃の波になると考えているからです」と述べています。

AIとMLが情報セキュリティチームにもたらす新たな課題

各選択肢において、「少しそう思う」「非常にそう思う」と回答した人の割合



KPMGの視点：倫理的なAI

組織はデータドリブン型にならなければ、判断を誤る恐れがあることを知っています。多くの企業はデータドリブンによる意思決定を自動化するためにAIを導入していますが、AIは組織のブランドと収益性に新たなリスクをもたらします。AIは不平等を助長し、プライバシーを侵害し、自律的で個人的な意思決定の能力を制限する可能性があります。

望ましくない結果について、AIシステム自体を責めることはできません。信頼できる倫理的なAIは決して「ぜいたく品」ではなく、ビジネス上必要なものです。このことを認識するビジネスリーダーは増えていますが、努力や挑戦なしに信頼が確保されるわけではありません。

特に、ある分野や領域では「倫理的で信頼できる」と考えられていることが、別の分野では通用しないことがあります。万能の解決策はなく、既存のフレームワークをコピーしても効果はありません。信頼できるAIは、全体論的かつ技術にとらわれない、意識やAIガバナンス、リスク管理に対して広く支持されているアプローチによって実現されます。

たとえば、以下の対策はすべて、イノベーションを阻害することなく実施しなければなりません。

- AIによる影響の評価では、適切なステークホルダーを巻き込みリスクを特定する
- AIの価値観と、組織やステークホルダーの価値観を一致させる
- 組織は、法律や規制へのコンプライアンス、AIの投資収益率を慎重に評価する
- 意思決定は追跡および監査を可能とする

Sander Klous
Partner, D&A Business Development
KPMGオランダ

> **我々が敵対的AIへの対応を重視しているのは、これらが次の攻撃の波になると考えているからです。**
>
> **Ann Johnson氏**
> Corporate Vice President
> Microsoft Security Business Development

規制の見通し

デジタルトラストに対する社会的な関心が高まるにつれ、法律家や規制当局の関心も向上し、透明性と監視に対する要求も高まっています。本調査によると、

36%

の回答者は、デジタルサービスプロバイダーに業務を委託する場合、サイバーセキュリティに関する既存または新規の規制に準拠しているかどうか懸念しています。

34%

の回答者は、サイバーセキュリティに関連する企業報告書の開示について懸念しています。

31%

の回答者は、英国やEU、米国で規制強化の対象となっている、重要インフラに関する要求が高まっていることを懸念しています。

これらに加え、国際的な組織は、ますます複雑化・多様化し、時には矛盾する領域外の規制に対処しなければなりません。「CISOにとっての課題の1つは、同じ規制でも地域によってステークホルダーの解釈が異なることです」と、欧州の大手ITプロバイダー、Bechtle社のCIOであるUlrich Baisch氏は述べています。彼の言葉を借りれば、「何ができていて何ができていないのか、明確な考えを持つことが必要」です。

KPMGの視点：厳格化する世界の規制

世界的にみると、サイバーセキュリティとプライバシー保護に関する規制の強化が加速しています。2022年10月時点で、137ヵ国以上の国々が何らかの形でデータ保護制度を設けており、多くの場合、その国で提供されるサービスや国民のデータに対する治外法権（域外管轄権）を主張しています。プライバシー保護制度は強化の一途で、テクノロジーの導入が引き起こす新たな課題に直面しながらも、次世代の規制へと移行しています。AIの規制に関する議論は、現在、法律案として形になるほどになっています。

さらに、産業用制御システムに対する攻撃への懸念が高まるなか、各国は重要インフラのサイバーセキュリティに関する規制を一段と厳しくしています。これらの規制は、インシデント報告や外部監査の義務付けなど、自己評価型から、より指導的な管理型へと移行しつつあります。

規制当局も、統制の枠組みをより厳格にする一方、CISOの独立性と内部統制基準の設定におけるCISOの役割を強化しようとしています。金融などの分野では「極端ではあるものの起こり得るシナリオ」での事業回復に焦点を当てた、より全体論的なレジリエンス要件も現れてきています。

サイバーリスクの透明性に関する企業要件は、ランサムウェアインシデントの開示に関する要件の増加とともに、議論が進んでいます。企業はコンプライアンスの監視と報告を自動化するために投資し、規制環境のモニタリングを続け、新しいサービスや製品を開発する際にはプライバシーやセキュリティに関する規制の動向を考慮に入れる必要があるのです。

David Ferbrache
Global Head of Cyber Futures
KPMGインターナショナル

規制の先を見据える

デジタルトラストはESG戦略の一部であるべきで、サイバーセキュリティとプライバシー保護についても同様です。「ESGはビジネス全体にとって必要不可欠な観点です。特に社会やガバナンスに関連する問題については、CISOが重要な役割を担っています」とBechtle社のUlrich Baisch氏は述べています。

デジタルトラストをESGに組み込むためには、さらなる取組みが必要です。ESGチームにとってセキュリティは不可欠な要素であるとみなしている企業は5社中1社に満たず、大多数の企業は「セキュリティの役割は非常に限定的」と回答しています。組織はこれらのテーマに関する社会的要請と期待の高まりを認識する必要があり、ESGの担当者はサイバーセキュリティ（多くの場合、CISO）やデータプライバシー（多くの場合、データ保護責任者（DPO））の担当者と協力する必要があります。

> **ESGはビジネス全体にとって必要不可欠な観点です。特に社会やガバナンスに関連する問題については、CISOが重要な役割を担っています。**
>
> **Ulrich Baisch氏**
> CIO, Bechtel

KPMGの視点：ESGと社会的責任

ESGに真摯に向き合っている組織は、顧客の信頼を獲得し、ブランドを強化することができます。現在のデジタルな世界では、役員会、投資家、規制当局、顧客、一般市民が、組織のサイバーセキュリティとプライバシー保護について透明性の高い報告を求めています。ステークホルダーは「取締役会や経営層が情報を保護しつつ、重要なサービスのレジリエンスと誠実性を確保するために努力することの社会的意味を認識している」との確信を持ちたいと考えています。

ステークホルダーが考慮している点は以下のとおりです。

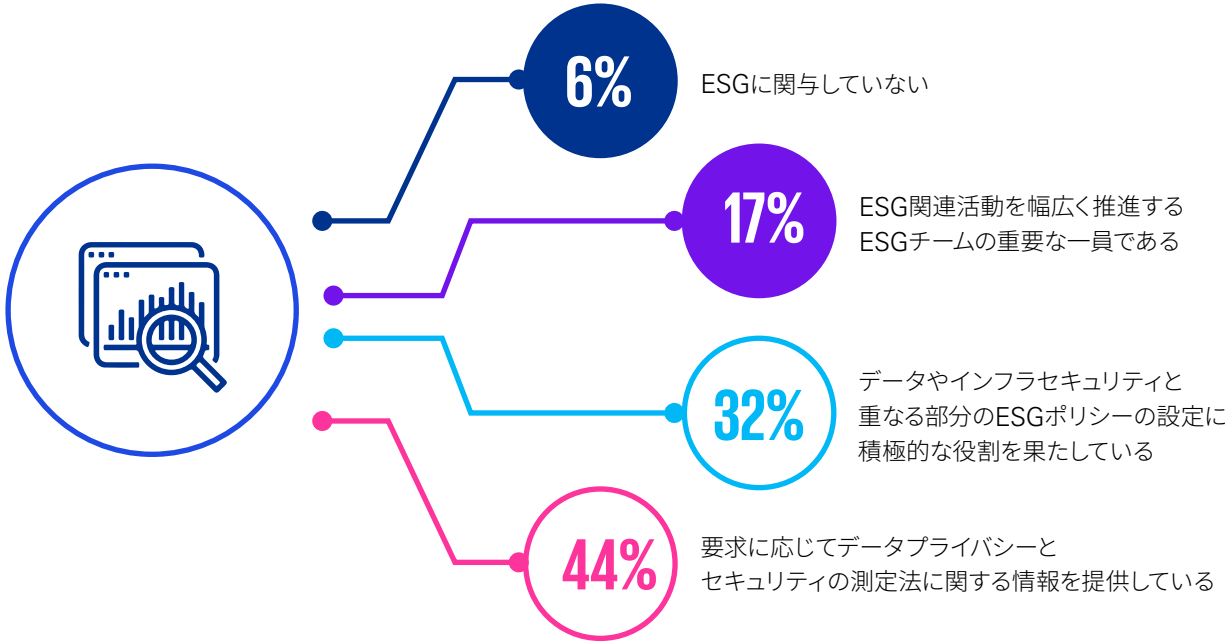
- デジタル資産を積極的に監視し、「フェイクニュース」や「ディープフェイク」によるオンライン搾取や情報の武器化が進むなか、安全で信頼性の高いコンテンツへのアクセス確保を支援していること
- サイバー空間で可能になった詐欺や個人情報盗難に対し、特に「サイバー貧困ライン（サイバーセキュリティを十分に考慮できる顧客とそうでない顧客の境界線）」を下回っている顧客の保護を支援していること
- 顧客データを収集・分析するAIやMLなどの技術について、倫理的な導入を目指していること
- 社会にとって不可欠なデジタルサービスの信頼性、誠実性、可用性を維持していること
- サプライヤーのエコシステム内外で、サイバーに関するスキルと能力を高めるための幅広いコミットメントを示していること

Srinivas Potharaju
Partner, Digital Trust
KPMGインド

Siddharth Durbha
Director, Digital Trust
KPMGインド

大半のCISOは、ESGポリシーやその活動に受動的にしか関与していない

自社のCISOと情報セキュリティチームのESGの役割について、各選択肢を「非常に当てはまる」と回答した人の割合



KPMGの視点：規制の最低基準を超えることで信頼を高める

先進的な企業は、ESG報告フレームワークにデータプライバシーに関する指標を組み込んでいます。

これにより、規制要件が最低限満たされていることを確認し、信頼を構築することができます。多くの組織は、より強い信頼を得るため、積極的に規制の最低基準を超えようとしています。その結果、法的な観点だけではなく、組織が明示した「ESGのシナリオ」に合致しているという観点からも、個人情報が適切に収集、使用、開示されていると、ステークホルダーは確信を持つことができるのです。

Sylvia Klasovec Kingsmill
Global Privacy Lead
KPMGインターナショナル
Partner
KPMGカナダ

3

信頼できるコミュニティの構築

コラボレーションとパートナーシップの力

デジタル化によって企業活動は、孤立して行われるのではなく、広範なパートナーシップやコラボレーションのなかで行われることが多くなっています。このことは、サイバーセキュリティチームが直面する課題をさらに難しくしています。取引先等との協力により相互の信頼を確保することで、組織が存在しているエコシステムへの信頼を築かなければなりません。最終的には、エコシステム全体への信頼確立を目指す必要があります。

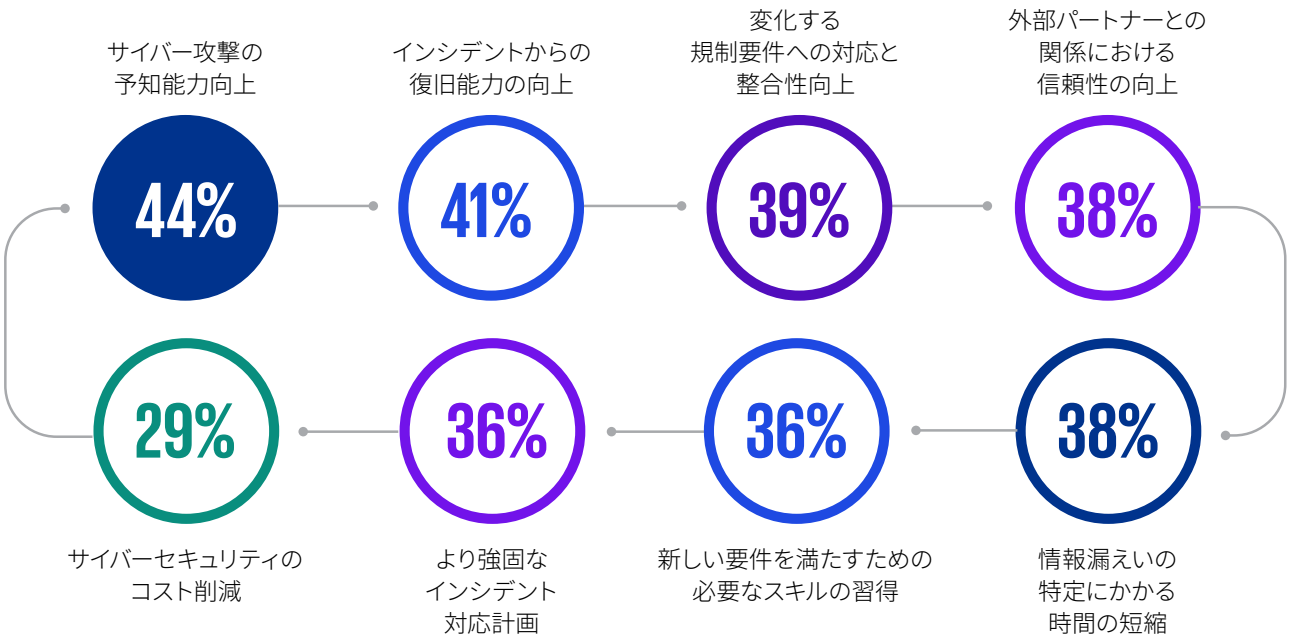
数字は説得力を持っています。本調査では、回答者の44%が「より広範なエコシステムでサイバーセキュリティに関して協力することが、サイバー攻撃の予知能力向上に役立つ」と回答しています。

コラボレーションは望ましいことですが、必ずしも一筋縄ではいきません。回答者の38%が、プライバシーに関する懸念が外部とのサイバーセキュリティパートナーシップの妨げになっていると答え、36%が、自社のセキュリティ体制について開示しすぎないかためらっています。また、規制による制限、経営層のサポートの欠如、リソースの不足などの課題が挙げられます。

『基準を定めること』と、『自社のファイアウォールがその基準を満たしていると言うこと』はまったく別の話です。一般的に、複雑な詳細を明らかにしなくとも、信頼獲得に役立たせることができます。

Mark Thompson氏
Chief Strategy Officer, International Association of Privacy Professionals (IAPP)

より広範なエコシステムでサイバーセキュリティに協力することは、攻撃を予期し、被害から立ち直るために役立つ
協力するメリットとして、各選択肢を上位3つに選んだ回答者の割合



国際プライバシー専門家協会（IAPP）の最高戦略責任者（CSO）であるMark Thompson氏は、現実的な解決策について次のように述べています。「もし私がファイアウォールのルールのパラメータを公開した場合、脆弱性や抜け穴を指摘される可能性がありますが、『基準を定めること』と、『自社のファイアウォールがその基準を満たしていると言うこと』はまったく別の話です。一般的に、複雑な詳細を明らかにしなくとも、信頼獲得に役立たせることができます。」

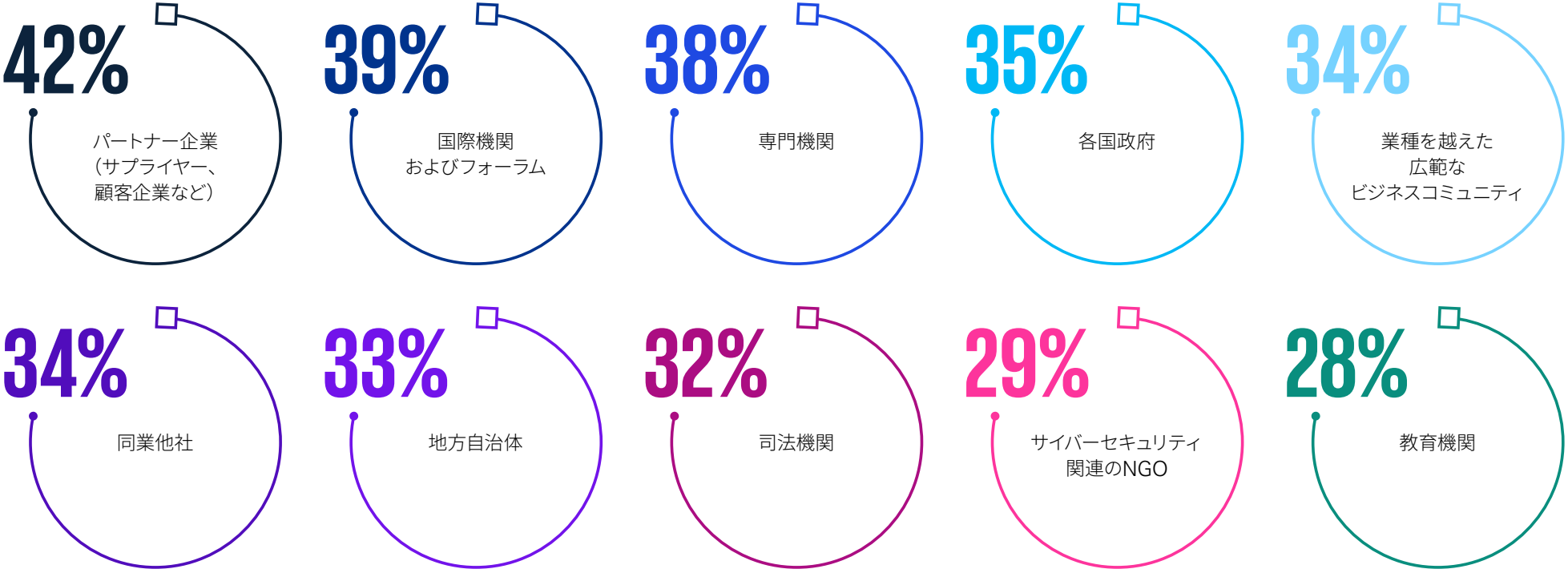
重要なパートナーとの協力や情報交換を行っている企業が半数以下にとどまっている理由の1つに、情報共有に関する基準やベストプラクティスが未成熟であることが挙げられるかもしれません。79%の回答者が「効果的なサイバーセキュリティにはサプライヤーの建設的な関与が不可欠」と述べているにもかかわらず、「その実現に向けて実際に協力している」と答えた回答者はわずか42%にすぎません。

こういった消極的な姿勢は重大な弊害をもたらす可能性があります。半数以上の企業が「攻撃者による調達やサプライチェーンの脆弱性の悪用を阻止するうえで、自社の防御が十分に強固であるかわからない」と認めています。

対策を自らの組織のみで行う限定的なアプローチでは、個々の組織やそのエコシステムを十分に保護することができず、組織やエコシステムへの信頼が損なわれてしまうため、コラボレーションを継続することはできません。回答者の半数以上（53%）は、自組織がサイバーセキュリティのコラボレーションに積極的ではないことを懸念しており、その懸念は正しいと言えるでしょう。

エコシステム全体でより多くのサイバーセキュリティパートナーシップが必要になっている

サイバーセキュリティを強化するために協力や情報交換を行う組織として、各選択肢を選んだ回答者の割合（複数回答）



KPMGの視点：団結の価値

サイバーセキュリティの課題に対処するためには、効果的なコミュニティの構築が不可欠で、各組織は協力し合うべきです。ただ、リスク管理、評判、法律、戦略などに関する大きな懸念が、依然としてその目標を妨げている可能性があります。

どのような組織も単独ではこれらの課題に対処できないため、リソースを組み合わせ、いくつかの組織を効果的に調和させることが重要です。公共機関や民間企業が協力することで、さらなる効率性、視点、リソースを手に入れることができます。

信頼とコミュニティを構築するためには、各当事者は、何が可能で、どこに障壁があり、それをどのように克服するかを認識する必要があります。たとえば、米国国立標準技術研究所（NIST）のサイバーセキュリティフレームワークなどの既存の基準を使用して、他の組織と提携する際の共通言語や用語を作成している組織もあります。また、機密情報を組織内に保持するための方法に着目している組織もあります。共通の運営原則に基づく協力協定は、組織のプライバシーを保ちパートナー間の相互信頼を強化しつつ、組織同士が関係を深めることや、デジタルインフラの構築を手助けしてくれます。

このように組織同士が連携した状況では、従来のセキュリティのパラダイムはあまり意味をなさないことを認識すべきで、レジリエントな思考に焦点を当てるほうが理にかなっています。システムを分離して制御することによって悪意あるアクターを打ち負かそうとするのではなく、より協調的・協力的なアプローチが求められています。

Prasad Jayaraman
Principal, Cyber Security Services
KPMG米国

4

CISOの進化

信頼の構築に貢献するCISO

CISOの登場

CISOは革新と成長に向けた取組みにブレーキをかける存在とみられがちですが、今や成功要因として重要な役割を果たす立場にあります。CISOは、組織の信頼を守る最高の守護者として活動することで、組織の成功の原動力となることが可能です。

IAPPのMark Thompson氏は「CISOは信頼を高め、向上させることができますが、一般的にCISOの活動は組織の優先順位に左右されがちです。組織がダイナミックに活動できるよう、組織の信頼を守ることを優先して取り組む必要があります」と述べています。

CISO自身も、何が喫緊の課題なのかを認識しています。回答者の4分の3以上（77%）が、信頼の向上がサイバーリスク問題の重要な目的であると回答しています。

また、組織は自社のサイバーセキュリティ能力を高く信頼しています。回答者の74%が「過去12ヵ月の間にサイバーセキュリティが改善された」と回答しており、4人に1人以上が「おおいに改善された」と回答しています。この自信は、CISOの重要な任務を遂行する能力に対する強い信頼と結びつきます。

一方で、CISOはその期待に応えられていると感じているのでしょうか。

組織がCISOに寄せる信頼は高い

各項目において、自組織のCISOや情報セキュリティチームが「効果的な役割を果たしている」と評価した回答者の割合

- **80%** サイバーセキュリティとデータ保護に関して企業が直面する法的要件への対応
- **80%** サイバー攻撃から顧客／取引先のデータを効果的に保護するためのテクノロジーの導入
- **80%** サイバー攻撃からIT資産を保護するためのテクノロジーの導入
- **79%** サイバー攻撃や情報漏えいの調査および影響の軽減
- **79%** データ利用およびプライバシー／データ保護に関する透明性の向上
- **78%** サイバーセキュリティに関する教育・啓発の推進
- **78%** 規制当局との相互信頼関係の構築
- **78%** サイバーインシデント発生時のステークホルダー・広報対応
- **78%** 社内パートナーの業務改革支援
- **77%** サードパーティおよびサプライチェーンのサイバーセキュリティの強化

興味深いことに、多くのCISOは、目標を達成するための権限を確保することに苦労しているようです。Microsoft社のAnn Johnson氏は「しばしば難しい会話がなされます。どのようなデータを共有するのか。どのようなデータを保存するのか。AI/MLの観点からどのようにデータを利用するのか。そしてどのようにデータを保護するのか。CISOは、こうした議論の一つひとつに参加を求められますが、それは簡単なことではありません」と話しています。

回答者のほぼ3分の2 (65%) が「情報セキュリティはビジネスを実現するものというより、むしろリスク低減のための活動として捉えられている」と回答しています。回答者の57%が「経営層は情報セキュリティの強化による信頼性の向上がもたらす競争上のメリットを十分に理解していない」と回答しています。このような認識の「ズレ」は、CISOが経営層に対し、サイバーセキュリティの現実に関する見識を改めてもらうよう、働きかける必要があることを示唆していると言えます。

経営層との関係構築

CISOがサイバーセキュリティとデータプライバシーの信頼に関する議題を単独で推進することを期待するのは、非現実的かつ不公平でしょう。最高データ責任者 (CDO) や最高プライバシー責任者 (CPO) といった同僚との連携が、極めて重要になるはずです。効果的に協力すれば、この「トリオ」は信頼を高めるために実用的な変革を起こし始めることができます。

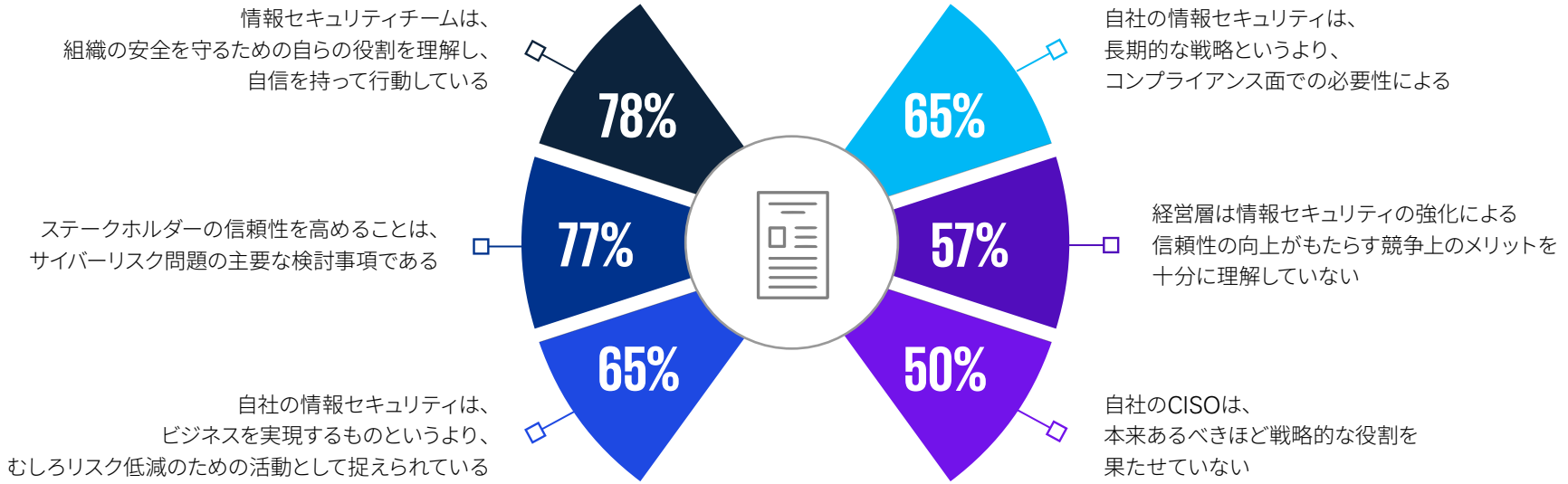
組織で最も影響力のあるリーダーが「CISOとサイバーセキュリティ部門は、早い段階から変革に関与すべきだ」と考えていることは、良い傾向です。

経営層の回答者の45%は、CISOを重要な幹部とみなしており、CISOの役割は、デジタル変革、サイバー犯罪の増加、規制の厳格化などを背景に、過去5年間で急速に拡大しています。

CISOへの見方を変えるための方法の1つは、技術的な問題から焦点を移すことかもしれません。結局のところ、経営層の回答者の半数以上は「取締役会は、CISOから提示された技術的な詳細を理解していない」と答えています。戦略的役割に踏み込むための課題は、CISOに残されています。企業は、CISOが管理職を巻き込みビジネスにおけるニーズに注力し、サイバー領域をビジネス戦略、計画、投資、実現のあらゆる側面から推進する役割を担うことを期待しています。

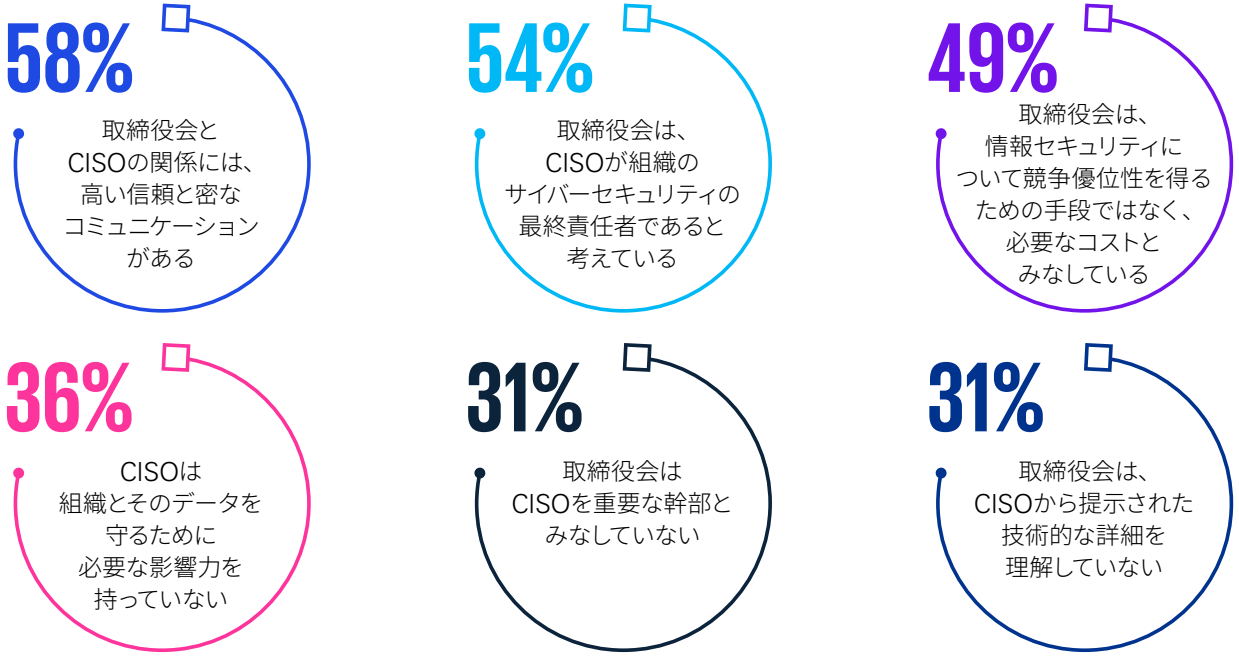
CISOはステップアップする準備ができていますが、それは許されることなのでしょうか

各選択肢において「少しそう思う」「非常にそう思う」と回答した人の割合



取締役会の見解が分かれる「CISOの影響力」

取締役会とCISOの関係について、各選択肢を「当てはまる」と回答した人の割合



リスクの定量化という課題

多くの組織で、分析が難しい領域におけるリスクモデリングとリスクアセスメントが順調に進んでいます。

4分の3の組織が「サイバーリスクを定量化し、取締役会へ視覚的に報告するためのリスクモデリングを導入した」と回答しています。一方、サイバーリスクを定量化する自社のアプローチを「強固」と言いきることができ、「サイバーリスクのシナリオがビジネスニーズに適合している」と考えている回答者は58%にすぎません。

より前向きな言い方をすると、回答者の3分の2以上（69%）が「デジタルトラストを単なる抽象的な概念として捉えるのではなく、それを評価する強固なアプローチを自社が持っている」と考えています。また、回答者の65%が「リスクモデリングがプロジェクトとリスク軽減の間に明確な関連性を持たせ、サイバーセキュリティへの投資を促進する」と回答しています。

そのため、CISOは現在行っていることをさらに進めるとともに、その仕事の性質が進化することを認識し、組織内外の信頼を高めるために役立つ可能性がある分野にまで手を広げる必要があります。

KPMGの視点：サイバーリスクの定量化に対する称賛

慎重なモデリングと定量化作業は、組織がどの程度サイバーリスクにさらされているかを認識し、意思決定者の理解に役立ちます。これにより経営層は、どのような制御が特定のサイバーリスクの削減に最も貢献するかを把握することができ、最もリターンの大きい分野にリソースを集中することが可能になるのです。

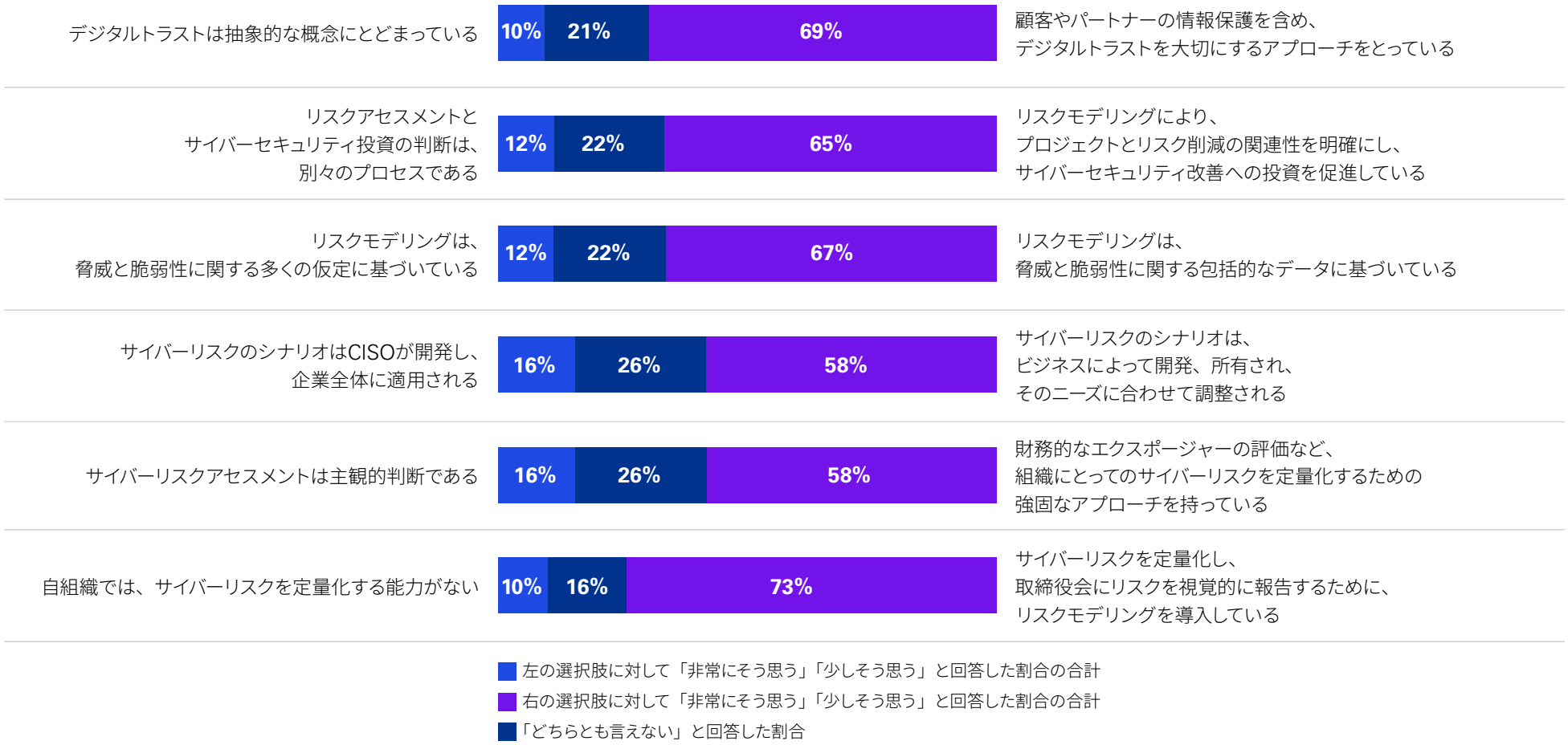
これを実現するためには、組織は次の5つの原則に従う必要があります。

1. リスクモデルと組織のリスクのフレームワークとの整合性を確保する
2. サイバーリスクの定義をビジネスに対する潜在的な損失対象とし、一貫性を持たせる（シナリオが有効）
3. モデル化にあたっては攻撃者目線のアプローチをとり、攻撃経路のモデリングによってこれらのリスクがどのように顕在化するかを明確にする
4. 計算には実際のデータを使う。つまり、発生可能性と影響度の見積もりは、社内外の実際のデータを用いる
5. モデルの利点と限界を理解し、それらについて透明性を保つ

James Hanbury
Director, Cyber Security Services
KPMG英国

多くの組織がサイバーリスクのモデル化と評価に苦慮している

取締役会にサイバーリスクを説明するための自組織におけるアプローチとして、各選択肢に対し、「少しそう思う」「非常にそう思う」「どちらとも言えない」と回答した人の割合



5

ミッションの達成

CISOを中心にどのように「信頼」を構築するか

経営者は、組織とそのエコシステムに対する信頼を高めることが重要であると認識しており、CISOが守護者の1人として役割を果たすことを期待しています。サイバーセキュリティとプライバシー保護は、企業の信頼を高めるためのカギとなる要素であり、ESGへの責務を通じて、顧客や規制当局、国民の心を掴むことができます。

CISOは自身が企業の目標を達成するための推進役を担っていることを認識しており、それはほかの部署の同僚も同じです。ただ、私たちの調査によると、多くのCISOがこの責任を果たすことに苦労しています。おそらく、デジタルトラストの本当の意味とその達成における自身の役割について明確なビジョンを持っていないことが原因でしょう。

これはCISOが1人で解決できる問題ではありません。経営層からの強力なサポート、他部門からの協力、外部パートナーやサードパーティとの生産的な協力が必要です。

ただ依然として、CISOの役割は非常に重要です。信頼を明確に定義することは良い出発点となり、サイバーセキュリティとプライバシー保護を組織の信頼を強化する方法として利用することで、あらゆる競争優位性をもたらすことができます。

では、どのように取り組めば良いのでしょうか。

サイバーセキュリティとプライバシー保護を通じた信頼構築のための重要な5つのステップ

01

サイバーセキュリティやプライバシー保護をビジネスと結びつけて扱うこと

サイバーセキュリティとプライバシー保護を、組織のビジネスプロセス、ガバナンス、文化に組み込むことで、コンプライアンス主導の間接的なものというより、ビジネスに不可欠なものにする。

02

社内の協力関係を築くこと

CDOやCPOなどの同僚と協力し、デジタルトラストの確立、定着、維持に貢献する。

03

CISOの役割を再認識すること

より幅広い課題を受け入れ、ESGからAI倫理に至るまで、幅広い貢献ができることを認識する。

04

経営層の支持を得ること

CISOは、経営層や取締役会の支持を得ることで、信頼に関する課題の推進に貢献しやすくなると思われる。これは、CISOを狭い意味での技術的役割から、組織の戦略的キーパーソンへと変貌させることを意味する。

05

エコシステムを頼ること

組織のエコシステム内の主要なパートナーを特定し、それらのパートナーと密に連携して、信頼とレジリエンスの向上に貢献する。

6

日本の特徴

CISO／セキュリティチームが取り組むべき課題

日本の特徴

本調査（KPMGサイバートラストインサイト2022）は、2022年5月から6月にかけ、日本を含む世界各国の上級管理職約1,900名を対象に、サイバーセキュリティとプライバシー保護が信頼の構築と維持に果たす役割を調査する目的で実施されました。

日本においてもサイバーセキュリティは重大な問題と捉えられており、他国と同様、多くの設問項目において、セキュリティと真摯に向き合う傾向が顕著でした。

グローバル全体と比較して、日本の取組みが進んでいた点は「リスクモデリングによるサイバーリスクの定量化と取締役会への視覚的な報告」で、グローバル全体よりも10ポイント以上高い結果でした。

一方、課題も山積しており、以下の項目で日本企業の取組みの遅れが目立ちました。

- 取締役会でのセキュリティコストの理解促進
- CISOの影響力の向上
- 社内外でのセキュリティ連携強化
- デジタルトラスト獲得のための社内支援
- サプライチェーン攻撃への対応強化
- サイバーセキュリティコミュニティの構築

図表1：リスクモデリングによってサイバーリスクを定量化し、取締役会にリスクを視覚的に報告していますか

「非常にそう思う」と回答した人の割合

自組織で完結しない サイバーセキュリティを目指して

2022年、メールで拡散する世界的なマルウェア（悪意あるプログラム）のEMOTET（エモテット）が、日本で多く検出されました。日本独自のPPAP（暗号化したファイルをメール送信し、復号パスワードを別送する手順）によって暗号化されたEMOTETファイルが、ウイルスソフトで検疫できないことを逆手に取られたことが要因となり、サイバー攻撃の拡大を招きました。

サイバー攻撃グループは、グローバルで「Weakest Link（最も脆弱な箇所）」を探し、ひとたびターゲットをみつけるとAIやMLを駆使して徹底的に攻撃します。そのような攻撃を自組織だけで防衛することは不可能なため、親会社・子会社間、本社・海外子会社間、パートナー企業間、同セクター企業間などのコミュニティを形成し、サイバーセキュリティに関する情報交換を活発に行い、集団の力で対抗する必要があります。

本調査では、日本企業において取締役会からのサポートや社内外とのセキュリティ連携不足により、孤軍奮闘するCISO／セキュリティチームの姿が浮き彫りになりました。社内外に味方を作り、「衆力功をなす」でサイバー攻撃に対抗できるよう、本調査を社内外の連携推進の参考としてご活用いただければ幸いです。

取締役会メンバーのセキュリティ技術への理解が不可欠

2015年に経済産業省が「サイバーセキュリティ経営ガイドライン」を公表し、日本においても「サイバーセキュリティは経営課題」という認識が定着してきました。ただ、本調査において、取締役会でのサイバーセキュリティの取扱いについて、他国と比較して一層の進展が必要なことが明らかになりました。

グローバル全体で、約半数が「取締役会は情報セキュリティを必要なコストとみなしている」と回答したのに対し、日本は43%にとどまり、特に北米（52%）との差は顕著でした。昨今のサイバー攻撃は、より安易にマネタイズできるかが重視されており、セキュリティ投資への遅れが日本を標的とした攻撃を増加させる一因となっています。

変化がめまぐるしいマーケットへの対応を加速するためにデジタルトランスフォーメーション（DX）が進むなか、製品のIoT化やスマートファクトリーなど、サイバー攻撃からの保護対象が急速に広がっています。半面、「取締役会がCISOから提示された技術的な詳細を理解していない」との回答がグローバル全体では31%だったのに対し、日本では37%に達しました。

適切なタイミングで適切なセキュリティ投資がなされるよう、取締役会で十分な議論をするためには、セキュリティ関連の技術的詳細への理解が不可欠です。CISOは、投資の必要性だけでなく、現在のサイバー攻撃のトレンドや、攻撃にさらされる要因などを取締役会で説明し、投資判断を後押しする役割を担うことが求められています。

CISOの影響力の向上

『KPMGサイバーセキュリティサーベイ2022』では、CISOもしくはサイバーセキュリティの責任者を設置している日本企業は58.6%にとどまりました*。

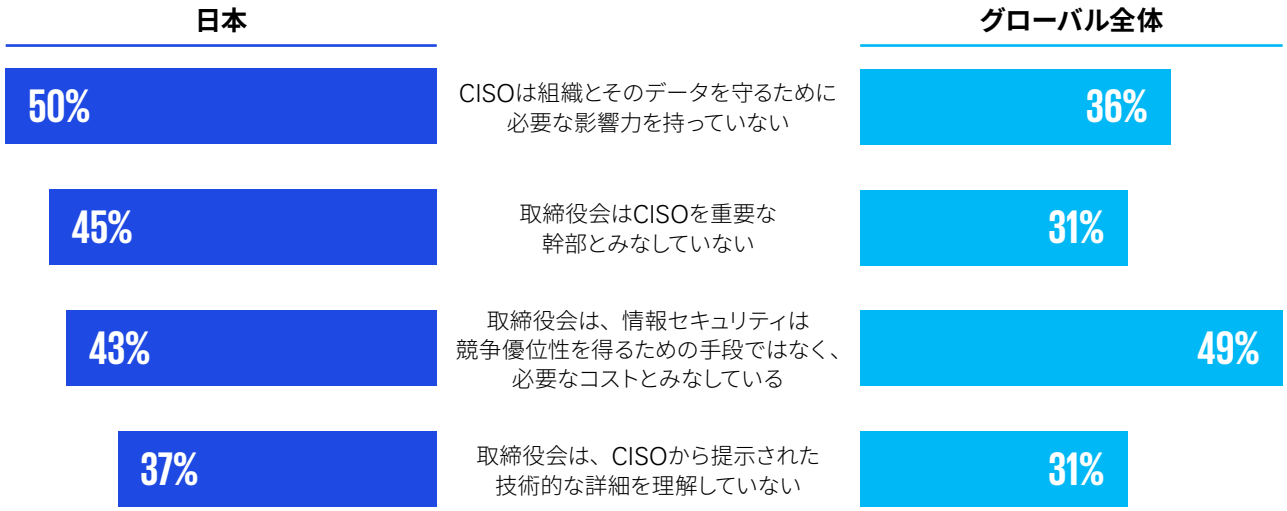
本調査においても、日本では「取締役会はCISOを重要な幹部とみなしていない」「CISOは十分な影響力を持っていない」との回答率が高く、組織におけるCISOの影響力が限定的であることが読み取れます。

デジタル技術を活用してステークホルダーの利益を守り、社会の要請に応え、企業価値を維持していくためにも、CISOへの期待はますます高まっています。

CISOが取り組むべき課題については、2022年7月に公表した調査レポート『強制者からインフルエンサーへ』にまとめていますので、今後の対応の一助としてご活用ください。

図表2：取締役会とCISOに関連する日本とグローバル全体の比較

各選択肢において「当てはまる」と回答した人の割合



＊ https://kpmg.com/jp/ja/home/insights/2022/01/cyber-security-survey2022.html

CISO／セキュリティチームの社内外との連携強化

本調査によると、他国と比較して日本のCISO／セキュリティチームが力を発揮できていない、社内外との連携に関する領域としては「サイバーセキュリティに関する教育・啓発の推進」「サイバーインシデント発生時のステークホルダー・広報対応」「規制当局との相互信頼関係の構築」が挙げられ、さらなる推進が必要な状況が明らかになりました。

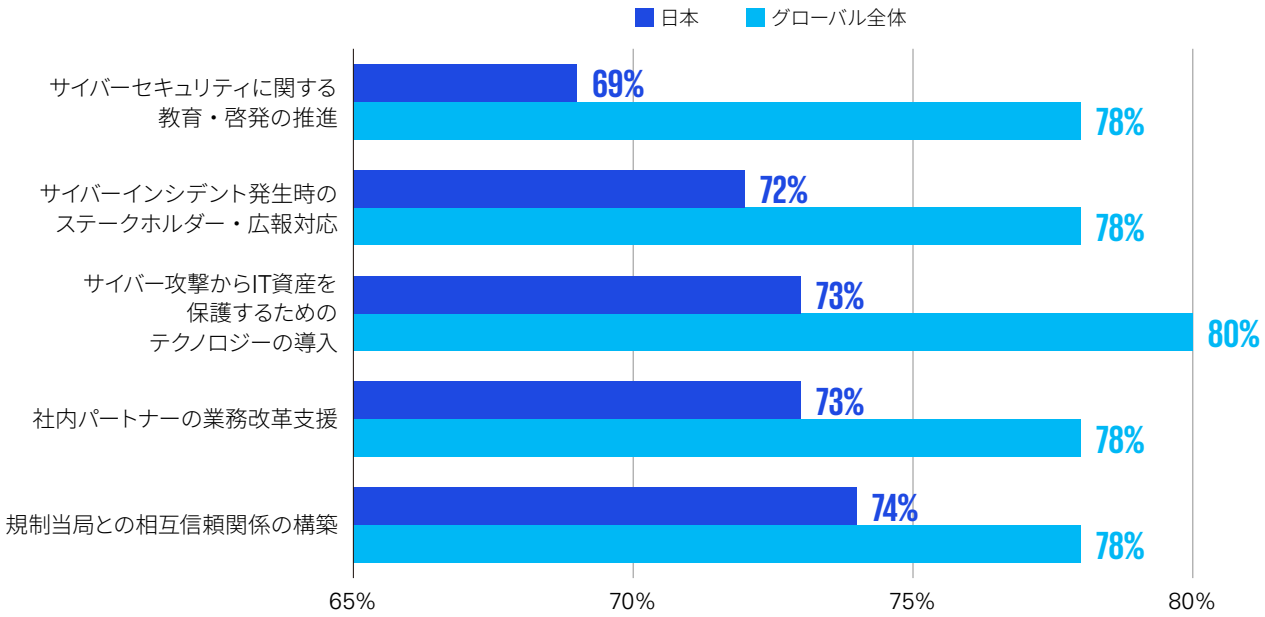
特に、報告されているセキュリティ侵害の大部分には、何らかの人的エラーの要素が含まれており、企業にとっては、人的要因に対応した包括的なサイバーセキュリティ戦略の策定・維持が重要となっています。

CISO／セキュリティチームは、セキュリティソリューションの導入推進にとどまらず、役員／部門長／一般社員／システム開発・運用要員／セキュリティオペレーターなどの役割に合わせたセキュリティ教育プログラムを策定し、セキュリティに関する教育・啓発を継続的に推進することが求められています。

ヒューマンリスク低減のための施策については、KPMGのウェブページ『人的ファイアウォール』にまとめていますので、ご参照ください。

図表3：自組織のCISO／セキュリティチームは以下の領域で力を発揮することができていますか

各項目において、自組織のCISOや情報セキュリティチームが「効果的な役割を果たしている」と評価した回答者の割合



デジタルトラスト獲得のための社内支援

「サイバー攻撃からIT資産を保護するためのテクノロジーの導入」において、グローバル全体で80%、日本が73%となっており、日本では、システムの完全性を確保する取組みについて優先順位が比較的低い可能性があります。

製品のIoT化やスマートファクトリーへの投資が進み、高度に接続された社会では、機密性の確保だけでなく、使いたい時に使えること（可用性）、データや処理が正確であること（完全性）もステークホルダーからのデジタルトラスト獲得に重要な要素となり得ます。

また、「社内パートナーの業務改革支援」についても日本とグローバル全体とで乖離がみられました。近年の業務改革は、デジタル技術の活用がカギとなっており、業務プロセスのDX化の進展によってサイバーアタックサーフェス（サイバー攻撃を受ける可能性のある領域）が拡大する恐れがあります。

CISO／セキュリティチームは、DXにおいても強固なセキュリティが確保できるよう、「セキュリティ・バイ・デザイン」の考え方に沿って、ルール・ガイドラインの整備や体制の確立に取り組み、内部関係者を支援する必要があります。

セキュリティ・バイ・デザインについては、KPMGのウェブページ『ニューノーマルでの新たなセキュリティの現実』でも触れていますので、ご参照ください。

サプライチェーン攻撃への対応強化

ランサムウェア攻撃は、企業単体のみにとどまらず、グループ会社や取引先に多大な影響をもたらすインシデントにつながる恐れがあるため、もはやサイバー攻撃への対策範囲は自社だけでなく、サプライチェーン全体で捉えなくてはなりません。本調査においても、「サイバーセキュリティ強化のためにパートナー企業との協力／情報交換を行っている」という回答がグローバル全体で42%でした。ただ、日本企業においては30%程度と、グローバル全体を10ポイント以上下回りました。

日本では、大企業を中心に、サプライヤーのセキュリティ対策状況を確認する際、年1回のセキュリティ調査票の回収や、数年に1度のセキュリティ監査の実施で済ませるケースも少なくないようです。一方、グローバルでは調査票・監査に加え「セキュリティリスクレーティング」を活用することで、日次でサプライヤーのセキュリティリスクをモニタリングし、改善を促すケースが増えてきています。

パートナー企業のセキュリティチーム間で最新のサイバー攻撃の事例共有を行う勉強会の開催や、CSIRT間で脅威情報・脆弱性情報を共有する仕組み作りなど、今後はサプライチェーン全体でのセキュリティ強化が一段と必要になります。

サプライチェーンセキュリティの強化のための施策をKPMGのウェブページ『増大するサプライチェーンセキュリティのリスク』にまとめていますので、ぜひご活用ください。

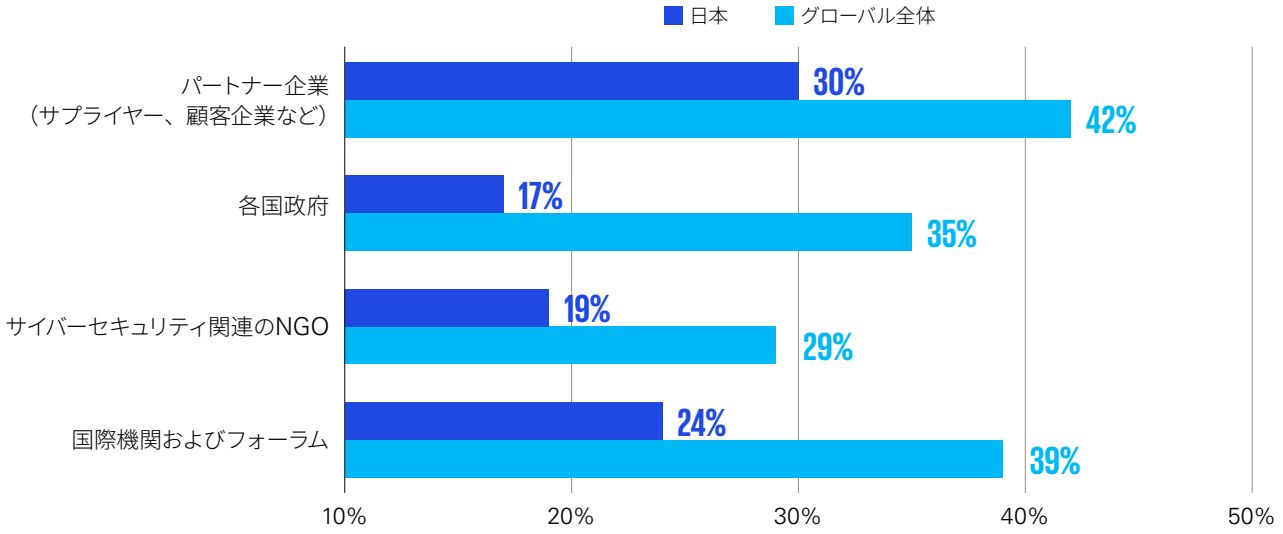
サイバーセキュリティコミュニティの構築

攻撃グループは、単一のターゲットだけを攻撃するのではなく、セクターや組織、サプライチェーン全体を標的にしています。本調査において、日本企業では「各国政府」「サイバーセキュリティ関連のNGO」「国際機関およびフォーラム」のいずれにおいても、サイバーセキュリティ強化のための協力／情報交換が十分ではない結果となりました。エコシステム全体のセキュリティ水準を向上させるには、これらの組織との協力が重要です。

特にサイバー攻撃にはトレンドがあり、それを理解するためには、自組織への攻撃だけでなく、コミュニティを通じてどのような攻撃が増加しているか、サイバー攻撃の動向をタイムリーに収集することがカギとなります。

セキュリティ強化のためのコミュニティ形成について、KPMGのウェブページ『デジタル社会で良き「サイバー市民」であるために』で解説していますので、今後の対応の一助となれば幸いです。

図表4：サイバーセキュリティ強化のために、次のうちどの組織と協力／情報交換をしていますか



調査方法および謝辞

KPMGサイバートラストインサイト2022について

KPMGインターナショナルは2022年5月から6月にかけて、世界各国の上級管理職1,881名を対象に調査を実施し、さらに企業経営者5名を対象に、サイバーセキュリティとプライバシー保護が信頼の構築と維持に果たす役割についてインタビューを行いました。

調査対象サンプルのうち、42%がCxOを含む経営層で構成されています。回答者には、31の市場（アジア太平洋地域24%、欧州・中東・アフリカ地域50%、北米16%、南米10%）および次の主要産業分野（エネルギー・天然資源、金融サービス、ライフサイエンス・製薬、メディア、娯楽、技術、公共部門、通信）のリーダーが含まれています。

全回答者は、1億米ドル以上の年間売上高があり、うち45%は5億米ドル以上、23%は10億米ドル以上、7%は50億米ドル以上です。

KPMGは、以下の方々のご協力に感謝いたします。

- Bashar Abouseido氏, SVP and CISO, Charles Schwab
- Ulrich Baisch氏, CIO, Bechtle
- Allan Cockriel氏, CISO, Shell
- Ann Johnson氏, Corporate Vice President, Microsoft Security Business Development
- Mark Thompson氏, Chief Strategy Officer, International Association of Privacy Professionals (IAPP)

KPMGについて

KPMGは進化する脅威に直面しても、レジリエントで信頼できるデジタルな世界の構築を支援します。KPMGのサイバーセキュリティの専門家は、リスクを多角的に捉え、組織全体にセキュリティを浸透させることで、以下のことを後押しします。

企業が、安全で信頼できるテクノロジーを用いて将来を予測し、より迅速に行動することで、優位性を確立できるようにすること。

KPMGの各ファームは、役員室からデータセンターまで、サイバーセキュリティに関するあらゆる領域で専門知識を有しています。顧客企業のサイバーセキュリティを評価し、ビジネスプロフェッショナルと連携させるだけでなく、高度なソリューションの開発、導入支援、継続的なリスクの監視に関するアドバイス、サイバーインシデントへの効果的な対応を支援します。

KPMGは、常に進化し続けるテクノロジーを活用し、過去と未来のギャップを埋めながら、信頼を築き、価値を創造し、保護しながら、ビジネスの前進をサポートします。

信頼できるデジタルの世界をともに創りましょう。

お問合せ先

KPMGコンサルティング株式会社

T : 03-3548-5111
E : kc@jp.kpmg.com

kpmg.com/jp/kc

本レポートで紹介するサービスは、公認会計士法、独立性規則および利益相反等の観点から、
提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。
詳しくはKPMGコンサルティング株式会社までお問い合わせください。

kpmg.com/jp/socialmedia

本冊子は、KPMGインターナショナルが2022年10月に発行した「KPMG Cyber trust insights 2022」を、KPMGインターナショナルの許可を得て翻訳したものです。翻訳と英語原文間に齟齬がある場合は、当該英語原文が優先するものとします。

Designed by Evalueserve.
Publication name: KPMG cyber trust insights 2022 | Publication number: 138298-G | Publication date: October 2022