Deloitte.
デロイト トーマツ

2023年 Global Future of Cyber Survey

サイバーをビジネスの中心に据え、
長期的な価値を構築する

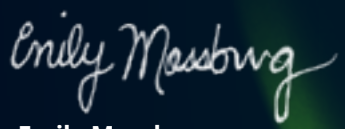
答えはサイバーにある

今日、私たちはサイバーに関して、強力で新しい考え方が生まれていることを目の当たりにしています。それは、サイバーを組み込むことによって得られる本来のビジネス価値を明らかにするものです。そしてリーダー達は鋭く新しい視点でサイバーに注目しています。サイバーは企業全体に関わるだけにとどまらず、強力な成長戦略の重要な一翼を担っているのです。

サイバーは、もはや単なる義務や技術に特化した予防習慣の集合体ではなく、企業が成果をあげるための重要な機能に成長しています。このことは 本レポートであるデロイトの「2023年Global Future of Cyber Survey」でも明確に示しています。本年度のグローバル調査は過去最大規模のサイバーに関する調査であり、様々な業界のリーダーを対象に、サイバーの現状と今後の展望をより明確に把握することを目的に実施されました。その結果、イネーブラーとしてサイバーの注目度が高まってきていることが分かりました。組織の規模に関わらず、サイバーは常に検討すべき課題として位置付けられ、ビジネスに不可欠な取り組みや投資の中心的な存在となっています。

私たちはサイバーの将来に胸を躍らせており、本レポートの重要な発見を、ぜひ皆さんと一緒に考えてみたいと思っています。本レポートでは、調査結果に基づくデータに加え、調査回答者から直接得た見解やインサイト、さらにビジネスの将来に可能性を与えるサイバー、クラウド、その他のテクノロジーに関するデロイトのインサイトを掲載しています。

皆さんのご健勝をお祈り申し上げます。



Emily Mossburg,
Deloitte Global Cyber Leader

目次

サイバーの先にあるもの

サイバーをビジネスの中心に据え、長期的な価値を構築する

世界中の組織が、技術中心の考え方、脅威に対する警戒を主眼にした考え方を超えて、サイバー思考とサイバー活動をビジネス全体に深く組み込むことで達成できる、潜在的なプラスの結果に目を向けはじめました。それにより、サイバーの将来像はより鮮明になりつつあります。

世界はますます相互に結びつき、それは新たな成長機会とともに新たなリスクをもたらしています。デジタル技術、データの急激な増加、ビジネスニーズの進化により、脅威のアタックサーフェスは拡大し、新たな課題が生まれたことで、サイバーは戦略的なビジネス課題として浮上しています。サイバー脅威を取り除き、ビジネス価値を守り、そして顧客の信頼を維持するためには、サイバー部門、リスク管理部門、事業部門などの部門を超えた連携が不可欠です。

近年、多くの企業経営者は、デジタルビジネスプロセスへの継続的な移行、テクノロジー環境、サイバー脅威をめぐる状況の急速な変化に注目してきました。実際、ハイブリッドITの管理とデジタルトランスフォーメーション（DX）は、企業が直面する二大課題として浮上し、複雑さは企業の新しい基準として定着しています[1]。

今日、新しい現実が形作られつつあります。デロイトの「2023年Global Future of Cyber Survey」では、サイバー脅威、企業活動、将来について、世界中の様々な業界のリーダー数百人に意見を求めました。この調査には、企業全体の経営幹部レベルのエグゼクティブのほか、IT、セキュリティ、リスクを担当するシニアリーダーが含まれています。この新しい現実は、次のような調査結果によって裏付けられています。

サイバーは、ビジネスにおける明確な機能領域として進化しており、従来のITの枠を超えて、ビジネスの成果を実現するための重要なフレームワークの一部となっています。

関係性のトランスフォーメーション

「サイバーセキュリティは、企業のビジネスリスクとしてとても大きく焦点が当てられはじめています。組織全体の連携において、添え物や後付けとしてではなく、サイバーセキュリティをトランスフォーメーションの中核的な構成要素として捉えるという大きな変化が生じています。私たちは、DevSecOpsにしろ製品開発にしろ、サイバーセキュリティを組み込むという点で多くの対応を行っており、安全に物事を構築するために（社内の）パートナーとともに共創を始めています。これは一種の文化的なトランスフォーメーションなようなものです。」

—Shell グループCIO兼CISO、Allan Cockriel

2023年以降を見据えると、サイバーは従来のテクノロジーの枠をはるかに超えて成長しています。今や多くの組織の事業運営・成果・機会にサイバーがより密接に織り込まれています。サイバーはテクノロジーのみに特化したものではありません。サイバーは基礎となるものです。組織全体のサイバーに関する意思決定者の間では、サイバーはビジネスの構造の一部となり、ビジネスの目標達成を支える要素として組み込まれています。

サイバー脅威がITの問題からビジネスの問題へと変化したように、サイバー戦略もITからビジネスへと変化し、最終的には戦略的なビジネス目標や成長を支えるようになっています。取締役会レベルでは、ビジネスの優先事項としてのサイバーがより明確になりつつあります。今回の調査では、回答者の70%が、サイバーが取締役会の議題として毎月または四半期ごとに定期的に取り上げられていると回答しています。

これは、ハイレベルで戦略的なビジネス上の意思決定において、サイバーが重要な位置を占めていることを明確に示しています。

企業は、幅広いビジネスの成功を可能にするためにサイバーが果たす役割をますます認識するようになっています。

調査回答者の圧倒的大多数は、サイバーとビジネスインパクトの間に強い関係があることを認識しており、86%の回答者がサイバー施策が少なくとも1つの主要なビジネス優先事項に対して重要かつポジティブな貢献をしたと回答しています。そして、ほとんどの組織がこの価値判断をもとにして今後も事業を進めていく方針であり、58%が来年のサイバー投資を拡大することを計画しています。

70%

サイバーが取締役会の議題として毎月または四半期ごとに定期的に取り上げられていると答えた回答者は70%でした。

経験豊富な取締役会

「取締役会は明らかにサイバーセキュリティを重視しており、素晴らしいレベルでリソースを配分する意思があります。取締役会は今や、有能なセキュリティリーダーがどこにいるのか、また問題を解決するための投資ができている人がどこにいるのかを見分けることができる知識を身に着けています。その違いが分かることで、上級管理職や取締役会の許容範囲も変わっていくでしょう」

—消費者団体 CISO

サイバーはビジネスイネーブラーとしてのポテンシャルがあるにもかかわらず、これを効果的に活用する能力は組織によってまちまちです。一方、明確なリーダーとして、他の組織が追随できるような価値への道筋を定義している組織も登場しています。

今年の調査の一環として、デロイトは、サイバー計画のレベル、取締役会レベルでのサイバーへの関与、サイバーに関する戦略的行動のレベルに基づいて、サイバー関連の取り組みで優れたパフォーマンスを発揮している、サイバー成熟度の高い組織を特定しました。これらの組織は、業務・戦略計画、組織の情報セキュリティを継続的に改善するための行動計画、パートナーやサプライヤーのセキュリティ体制を監視・追跡するためのサイバーリスクプログラムなど、サイバー衛生にとって重要な行動を十分に実施しています。

これらの組織は、特にサイバーに関する取り組みとビジネス価値を結びつけており、サイバーへの取り組みが以下の事柄に大幅なプラスの影響を与えたと回答する傾向があります。

- ブランドレピュテーション
- 顧客とデジタルへの信頼
- 経営の安定性（サプライチェーンやパートナーのエコシステムを含む）
- 収益

サイバー成熟度が高い組織は、サイバーが主要なビジネス戦略に価値をもたらし、新たな挑戦への自信を組織に与え、ビジネスのアジリティを高め、効率化を可能にすると回答する傾向があります。また、こうした組織は、自社が利用しているサードパーティのサイバーサービスから非常に高い価値を得ていると回答する傾向も見られます。

ビジネスを前進させる

「プロジェクト、イニシアチブ、ビジネス目標の達成には、情報セキュリティとプライバシーの影響を考慮し、適切なプロセスに組み込むことが不可欠です。私たちはビジネスの構成要素や状況に関するアイデア出しの段階から参加します。私たちの戦略は、ビジネスをサポートすることに100%特化したものであり、ビジネスなくしてサイバーとプライバシーは存在しないことを認識しています。コンプライアンスを遵守し安全性を確保しつつ、ビジネスを前進させて成長を促進するための価値ある貢献をしたいと考えています。」

—Marriott SVP兼CISO、Arno Van Der Walt

54%

売上高50億ドル以上の企業の54%は、サイバー対策に年間2億5,000万ドル以上のコストを費やしています。

71%

売上高5億ドル以上50億ドル未満の企業の71%は、サイバー対策に最大で年間2億5,000万ドルのコストを費やしています。

インサイトを得た経緯

メソドロジー

デロイトは、今日のビジネスとテクノロジーにおける状況の複雑さを踏まえ、サイバーの重要性を認識しつつもその価値の活用に苦慮している企業リーダーのニーズに焦点を当て、「2023年Global Future of Cyber Survey」を企画しました。そして従業員1,000人以上、年間売上高5億ドル以上の企業を対象に、世界20カ国のディレクターレベル以上のサイバーに関する意思決定者（経営幹部レベルのエグゼクティブおよびその直属の部下）1,000人以上に対して本調査を実施しました。

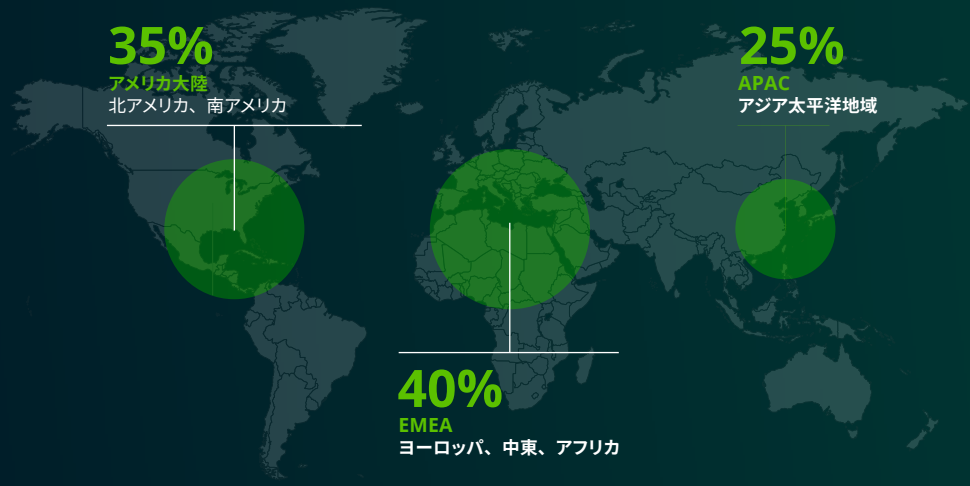
また、今日のサイバーが企業に与える影響の拡大を正確に把握するため、回答者のサンプル数を2021年の調査時の約600人から、約2倍となる1,110人に増やしています。加えて、より詳細なインサイトを得てデロイトの見解を検証するため、様々な業界や地域の上級サイバー意思決定者に詳細なインタビューも行いました。

今回のアプローチでは、戦略から戦術、文化、テクノロジーの導入まで、サイバーの将来に関連するあらゆる側面を網羅しています。

本調査の中核となるのは、以下の意図や取り組みです。

- デロイトの2021年版レポート以降、サイバーがどのように変化したかを探ること
- 未来志向の視点でサイバーの将来をより鮮明にすること
- サイバーがもたらすビジネス価値とインパクト、およびサイバーからより大きな価値を得るために先進的な組織が取り組んでいる注目すべきアクションを理解すること

調査対象組織の本社所在地



未来を左右するサイバー

この２年間でサイバーがどのように進化したかという本質的な背景を説明するだけでなく、主要な組織がより成熟したサイバー戦略を導入した場合に生じるビジネスへの影響を理解するために、デロイトではサイバー成熟度という視点を発展させました。

サイバー成熟度が高い組織と、中程度または低い組織を区別することで、サイバーリーダーと呼べる突出した層を特定し、サイバーがビジネスの成功と価値をどの程度支えているかをより深く理解することができます。

今日、「サイバー」とは「ビジネス」を意味し、基礎的かつ不可欠なビジネスの必須条件です。サイバーの重要性はどれだけ誇張してもしすぎることはないのです。どの企業にとってもサイバーの未来は、経営幹部レベルと取締役会のコミットメント、そしてサイバーによって組織全体が思い描けるようになるビジネス価値によって形作られるでしょう。今回の調査結果は、最高情報セキュリティ責任者（CISO）とその他の経営幹部レベル、そして取締役会が連携してビジネスをリードし、ともにイノベーションを実現するという、新しい原動力が生まれつつあることを示しています。

別の言い方をすれば、サイバーはより広範なビジネス戦略全体に組み込まれるべきものです。ITのリスクを軽減するのみならず、継続的なビジネス価値を推進する、成功に不可欠な構成要素として、サイバーは全ての機能領域に含まれるべきです。

インパクトを実証する

「リスクを最小化することで、どの部分にどのような影響を与え、どのように業務を円滑かつ効果的に継続できるようにしたかを明確にすることができます。事業運営や統合の課題を抱えていることが多いビジネスパートナーとの関係ではなおさらです。」

—消費者団体 CISO

状況の変遷を見る

2021年最終四半期に発行した前回レポート以降、世界の産業界は、優先事項、ビジネス施策、そして能力を調整をしながら、多方面にわたる絶え間ない混乱を乗り越えてきました。

2021年と今回のどちらの調査でも、私たちは回答者に対して組織のDXの優先事項をたずねました。これは、組織にとって現在どの技術が重要であり、また、それゆえに未来のサイバー戦略の一環として考慮する必要があるかを特定できるようにするためです。

企業の最優先課題の上位2つを2021年と比較すると、クラウドがデータアナリティクスに取って代わり2位から1位にランクアップしています。その他の運用技術・産業用制御システム、人工知能、コグニティブコンピューティングはわずかに上昇し、5位以内にとどまりました。そして新たに5位以内に5Gがランクインしたことで、組織内におけるビジネスの目標達成において5Gが果たす役割が大きくなっていることが反映されています。

クラウドの重要性が依然として高まる中で、サイバーに関する複雑な課題も考慮する必要が出てきました。こうした考慮は、データやアプリケーションをオフサイトで、かつ様々な環境下でホスティングする際に特有のものです。各組織のクラウドとサイバークラウドの成熟度にはかなりばらつきがありますが、デロイトが最近行った「Future of Cloud Survey Report」では、多くの組織がこのような懸念を克服し、リスク関連のクラウドのユースケースで非常に前向きな成果をあげていることが示されています。実際、83%の組織がクラウドへの投資がビジネスリスクや規制上のリスクの軽減という点で好ましい結果をもたらしていると回答しています[2]。これは、成熟したサイバークラウド機能、責任共有モデル、データプライバシープログラムの導入に関するポジティブなシグナルであるといえます。

DXの優先事項

当時と現在

サイバーが果たす役割

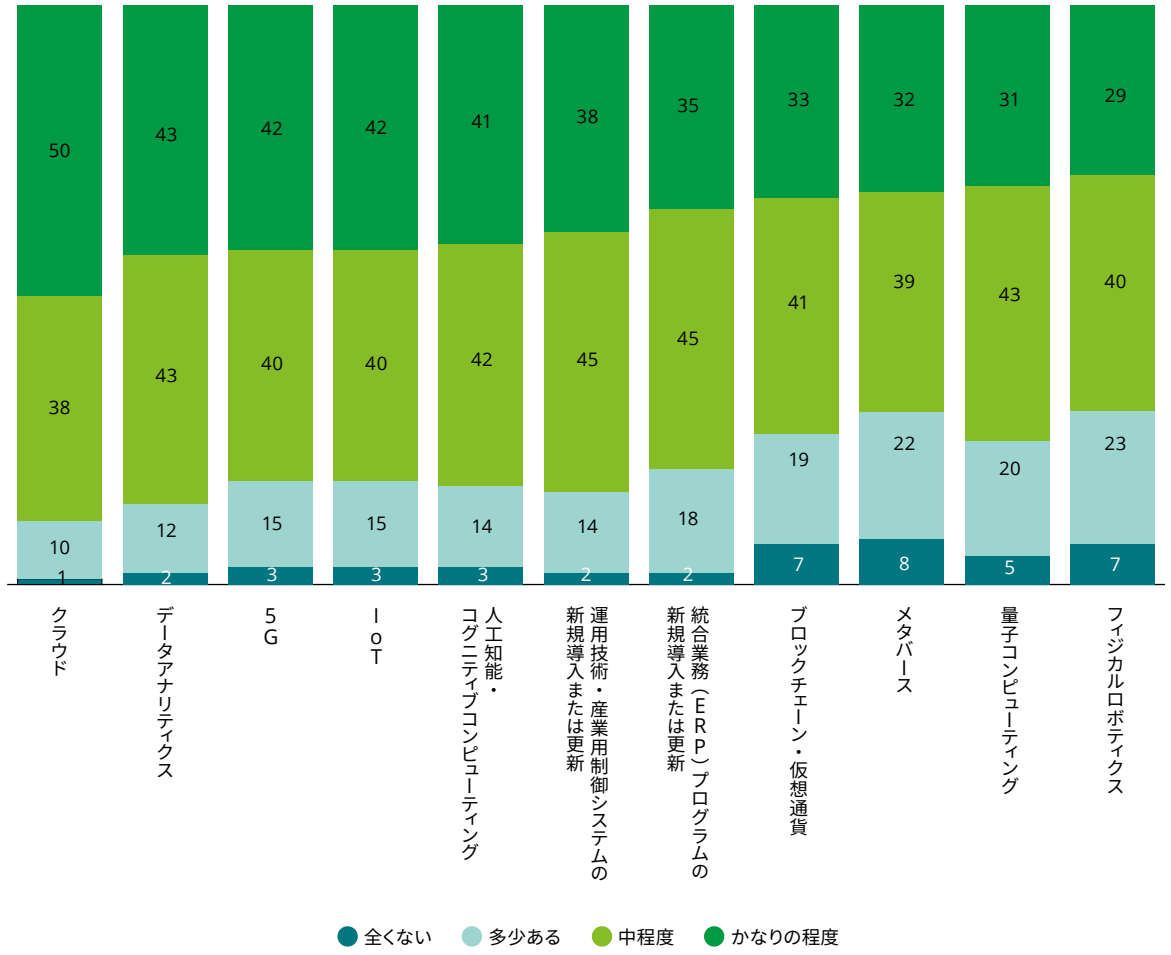
「Global Future of Cyber Survey」では、主要なDX構想のそれぞれにおいて、サイバーが果たす役割について質問しました。その結果、経営者はサイバーがDXの全ての優先事項であり、特にクラウド、データアナリティクス、5Gにおいてサイバーは重要な役割を果たすと考えていることが明らかになりました（図1）。

デジタルの優先事項や新たなテクノロジーが進化する一方で、私たちが分析した、組織に対するサイバーインシデントの影響も進化しています。組織のフォーカスポイントが、サイバーレディネスがもたらすプラスの影響と長期的なビジネス価値に移っても、サイバー脅威に対抗し、ビジネス上の悪影響とリスクを軽減するサイバーの中核的な能力を見失わないようにすることが重要です。

図1：注目されるサイバー

企業のDX施策において、サイバーが主要な役割を果たすことが期待されている

（四捨五入により比率の合計が100%にならない場合があります。）



最重要課題

「誰もがこの（サイバー）問題を検討すべき最重要課題としており、戦略設計、予算設計、ソリューション設計にこの問題を組み込んでいます。」

—金融サービス業 CISO

インシデントとその影響に関するインサイト

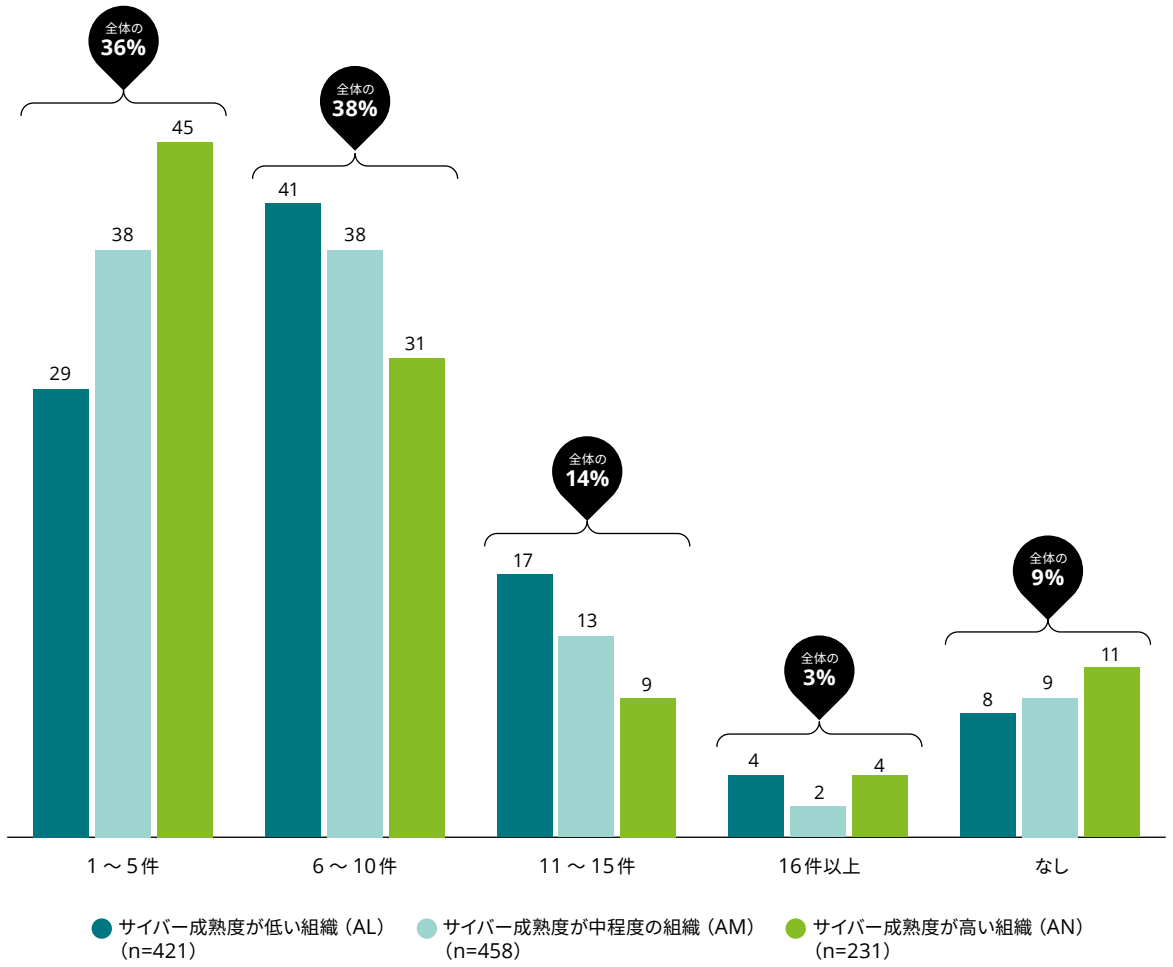
サイバーインシデントまたは侵害の発生頻度は引き続き変わらず、91%の組織が少なくとも1件以上被害を受けたと回答しています。尚、2021年の調査におけるこの割合は88%でした。組織におけるサイバーに関する懸念は、様々な脅威アクター、情報源、ツール、技術によってもたらされています。成熟度が高い組織は、サイバー犯罪者やテロリスト、そしてフィッシング、マルウェア、ランサムウェア攻撃についてより懸念しているようです。成熟度が低い組織、中程度の組織はサービス妨害攻撃（DoS攻撃）に対して大きな懸念を抱いています。また、成熟度が低い組織の方がより重大なサイバーセキュリティイベントを経験していると回答していることは注目に値します（図2）。

91%

組織の91%が少なくとも1件のサイバーインシデントまたは侵害が発生したと回答しています。

図2：重大なサイバーセキュリティイベントの件数

（単位：%）



一方、オペレーションの混乱は引き続きサイバーインシデントが引き起こす最も大きな影響ですが、収益の損失と顧客の信頼の喪失は2位と3位にランクアップし、回答者の56%が中程度または大規模な範囲でサイバーインシデントに起因する影響を受けたと回答しています。そして、ここで1つの仮説が成り立ちます。成熟度が高い組織は、ビジネスの中で現実に起きていることを深く理解していることから、その影響を違った形でとらえることができるが、成熟度が低い組織は理論的な影響を評価しているのかもしれないということです。とはいえ、成熟度が高い組織は、サイバー施策を実行することで、そこからブランドの評判や信頼の向上、業務上のメリット、財務上のメリットなど、より多くのプラスの影響を得ているようです。成熟度が低い組織や中程度の組織では、他の領域と比較して、ブランドの評判や信頼性の向上に関連するメリットを得る傾向があるようです。

このような大きな影響を受けて、組織のサイバー戦略・ソリューション・コントロールなど、組織のエコシステム全体にわたるリスクベースのサイバー戦略の必要性は、サイバーの将来にとってこれまで以上に重要となっています。ゼロトラストアーキテクチャは、セキュリティ体制の強化、セキュリティ管理の簡素化、エンドユーザーエクスペリエンスの向上により、企業の環境を最新のものにすることができます。ゼロトラストへの道のりには、ビジネス上の成果に沿った戦略に加えて、基礎的なサイバー問題の解決、手動プロセスの自動化、さらにセキュリティ組織やテクノロジー環境、企業自体の変革の計画など、多大なる努力と計画が必要です[3]。

図3：ネガティブな影響

サイバーインシデントや侵害は組織に以下のような悪影響を与えている

（2021年ではランキングの上位2つを選んでの回答、2023年では選択肢から上位2つを選んでの回答の結果）

サイバーインシデントや侵害がもたらすネガティブな影響	2021年（順位）	2023年（順位）	2023年（割合）
オペレーションの混乱（サプライチェーンやパートナーのエコシステムを含む）	1	1	58%
収益の損失	9	2	56%
顧客の信頼の喪失・ブランドへのネガティブな影響	4	3	56%
風評被害	5	4	55%
戦略的な施策への資金不足	該当なし	5	55%
技術的信頼性の喪失	該当なし	6	55%
人材確保・維持へのネガティブな影響	8	7	54%
知的財産の盗難	2	8	54%
株価下落	3	9	52%
規制当局による罰金	7	10	52%
経営陣の交代	5	該当なし	該当なし

ゼロを超えるもの

ゼロトラストの導入は、技術的な実装以上のものであり、文化、コミュニケーション、意識を左右するビジネス面および文化面でのトランスフォーメーションでもあります。

包括的なゼロトラストの導入は、ガバナンス（アーキテクチャおよび運用）、アナリティクスや自動化などのイネーブラー、アイデンティティ、データおよびデバイスなどのコアドメインなど、多くの要素に対処するものである必要があります。

56%

回答者の56%が中程度または大規模な範囲でサイバーインシデントに起因する影響を受けたと回答しています。

サイバー成熟度について理解する

サイバーの重要性が高まる今日の環境において、デロイトは世界中の何千もの組織と協力してきた経験から、回答者をサイバー成熟度によってセグメント化しました。

成熟度の定義

サイバー成熟度を定義し、サイバーの将来を形成するような優れたパフォーマンスを発揮している組織を特定するために、以下の通り、3つの先進的な慣行に基づいて組織を評価しました。

強固なサイバー計画
サイバー脅威に対する防衛・対応のための戦略的、運用的、戦術的な計画がある

重要なサイバー活動
定性的・定量的なリスク評価、業界ベンチマーク、インシデント対応シナリオの策定などの活動を実施している

取締役会の効果的な関与
取締役会が定期的にサイバー関連の問題に対処しているなどの取り組みをしている

成熟度グループの詳細
それぞれの先進的な慣行を点数化することで、調査対象の組織を以下の3つのグループにセグメント化しました。

規模や業界を問わない成熟度合
3つのグループを横断的に見ることで、より広い範囲で特徴を掘り下げ、成熟度の傾向や特徴を明らかにしました。3つのセグメント（低、中、高）には、業界や組織規模、収益規模を問わず企業が分布する結果となっており、属する業界や規模と成熟度との間に明確な関係があるわけではないことを示しています。

38%
サイバー成熟度が低い組織：
先進的な事例のいずれも実行していない

41%
サイバー成熟度が中程度の組織：
先進的な事例のうち1つを実行している

21%
サイバー成熟度が高い組織：
先進的な事例のうち2〜3つを実行している

成熟を価値につなげる、組織全体のために

私たちが明らかにした3つの主要な慣行、すなわちサイバー計画、活動、取締役会の関与が実現できるかどうかは、利害関係者が組織全体におけるサイバーの責任と関与の重要性を認識しているかどうかに左右されるということであり、これは極めて重要なことです。

CISOはサイバーの組織的な推進役として機能しますが、こうした先進的な慣行の多くは、全社的な取り組みによって初めて可能になるものです。

以下のような形での取り組みが考えられます。

- IT *部門*とシニアビジネスリーダーで構成される統括組織の設置とサイバープログラムの監視
- 組織や取締役会レベルでの、インシデント対応シナリオの策定とシミュレーションの実施
- 取締役会への定期的なサイバー関連最新情報の提供を通じた資金確保
- 全従業員を対象とした年1回のサイバー意識向上トレーニングの実施

私たちが特定した成熟度が高い組織は、サイバーに関する責任を組織全体に分散させることの有効性を認識しています。このような取り組みは、事業部門にサイバー専門家を組み込むか、少なくとも、サイバーチームとの調整を明確な責任として課せられている担当者を各事業部門に置くというデロイトの一般的なガイダンスと一致しています。また、サイバー管理における最大の課題として、組織全体のガバナンスが不十分であることを挙げる割合は31%少なくなっています（サイバー成熟度が低い組織は35%、中程度の組織は34%、高い組織は22%）。

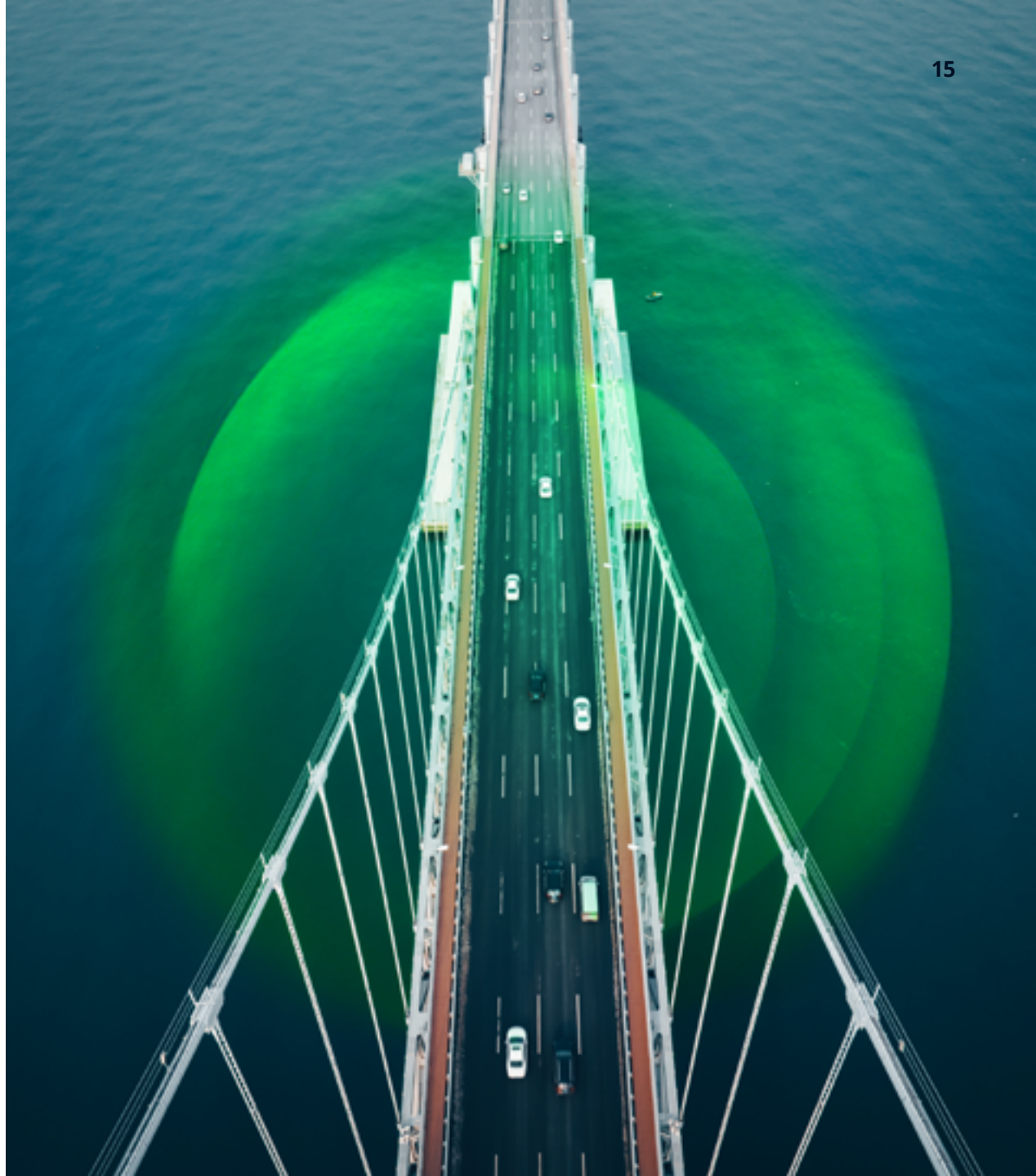
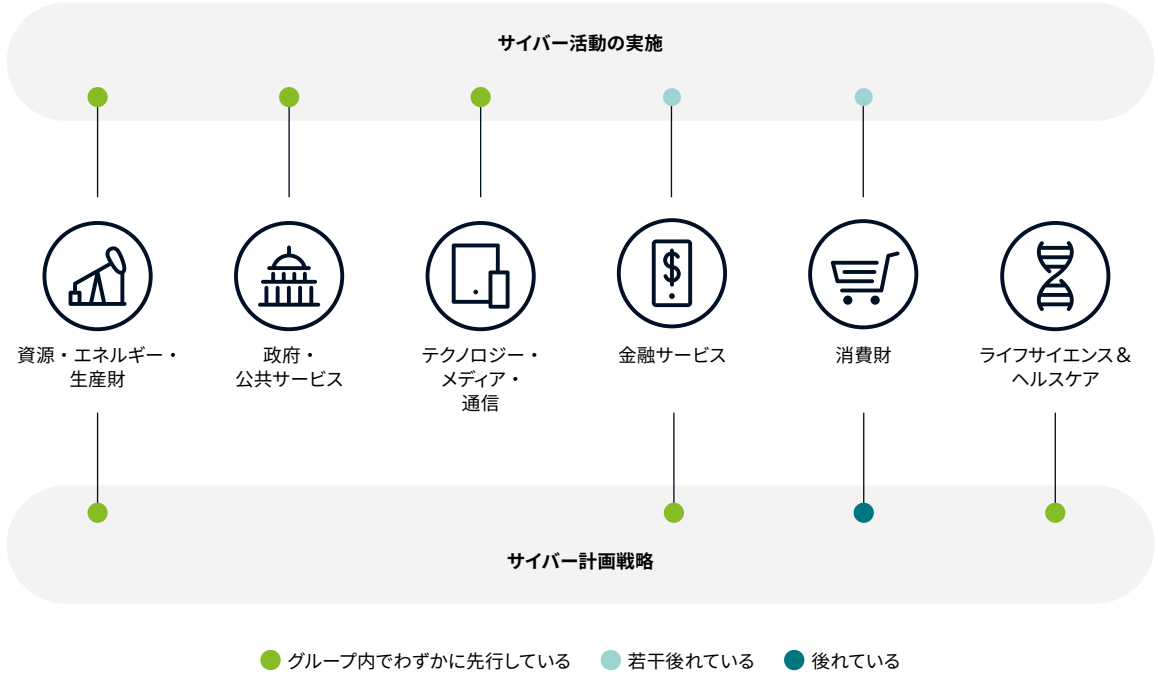


図4：各業界の位置付け



サイバー活動の例

- 毎年のサイバー計画の分析および更新
- ビジネスとITのシニアリーダーで構成された管理組織を設置し、サイバープログラムを監視
- リスク定量化ツールを使用し、サイバー投資に対するリターンを測定・保証
- 組織や取締役会レベルでのインシデント対応シナリオの策定
- 外部からの支援・アウトソーシングによるサイバー施策の管理

サイバー計画戦略の例

- 全従業員を対象とした年1回のサイバー意識向上トレーニング
- 毎年更新・テストされるサイバーセキュリティインシデント対応計画
- データの保管、処理、送信の全ての段階でデータ保護方法を評価する包括的な計画
- パートナーやサプライヤーのセキュリティ体制を監視・追跡するためのサイバーセキュリティリスクプログラム
- サイバーセキュリティとデータプライバシーに関するお客様の声の継続的な取り込み

業界

今回の調査対象となった6つの業界のうち、サイバー活動を5つ以上、全体平均よりもやや高いレベルで実施しているのは3業界でした。この3業界とは、政府・公共サービス、資源・エネルギー・生産財およびテクノロジー・メディア・通信業界です。

資源・エネルギー・生産財およびライフサイエンス＆ヘルスケア業界は5つ以上のサイバー計画戦略を全体平均よりもやや高いレベルで実施しています。

一方、金融サービス業界は、8つのサイバー計画戦略のうち4つを全体平均よりやや高いレベルで実施しています。しかしサイバー活動に関しては、全体平均に比べ後れを取っており、全体平均を上回る活動は1つだけです。

そして、消費財業界は、重要なサイバー活動10項目のうち7項目が全体平均より若干後れており、全てのサイバー計画戦略が全体平均を下回るレベルで実施されていることがデータから明らかになりました。

組織の規模

また、従業員数20,000人以上の企業では、以下のような傾向があるという調査結果が出ました。

- リスクマネジメント、DX、デジタルトラスト、テクノロジーの近代化に関するビジネス戦略の重要性を理解している。
- 上記のビジネス戦略におけるサイバーの重要性を認識している。
- サイバー計画と重要なサイバー活動の実施に関与している。

結論

業界や規模に関わらず、どんな組織でも高いサイバーパフォーマンスと成熟度を目指すことができます。
但し、成功を、サイバーへの投資拡大を通じて成熟度を「購入する」能力のみに依存してはいけません。むしろどのような行動をとるか、どのような文化を構築するかがパフォーマンスを向上させる主な要因になります。

本調査では、売上高が5億ドルから10億ドルの企業を小規模企業と定義しており、100億ドル以上の企業を大規模企業としています。

サイバーでビジネスを強化する

サイバーのためのより大きなビジネスケースを構築する

組織の成熟度に関わらず、絶対的なセキュリティとリスク軽減を保証するサイバーアーキテクチャやアプローチは存在しません。むしろサイバー成熟度が高い組織の最も顕著な特徴は、サイバーへの投資から価値を引き出す能力を持っていることです。

優れたパフォーマンスを発揮する組織は、リーダーシップの発揮、計画、行動の各段階でより多くのことを行っています。その結果、サイバーに関する取り組みからより多くのビジネス価値を生み出しているようです。効率性、レジリエンス、アジリティの向上などの効果を確認するという点で、成熟度が高い組織は群を抜いており、サイバーとは通常結びつかないようなメリットを認識しています。

自信の創出、その他

成熟度の高い組織のリーダーの半数以上（55%）が、サイバーは新しいことに挑戦する自信を与えてくれると回答しています。成熟度が中程度の組織では45%、成熟度が低い組織では40%でした。

また、成熟度が高い組織の約70%が、サイバーが信頼性の強化と効率化の実現の両方に影響を及ぼしていると回答しており、これは成熟度が低い組織や中程度の組織の数値を大きく上回っています。

同様に、成熟度が高い組織のリーダーの大多数（65%）が、レジリエンスとアジリティもサイバーによるメリットであると回答しており、ここでもまた成熟度が低い組織や中程度の組織を大きく上回っています（図5）。

55%

成熟度が高い組織の55%が、サイバーは新しいことに挑戦する自信を与えてくれると回答しています。

図5：より大きな可能性を見出す

サイバーがビジネス施策に具体的な影響を及ぼしている領域

（単位：%）

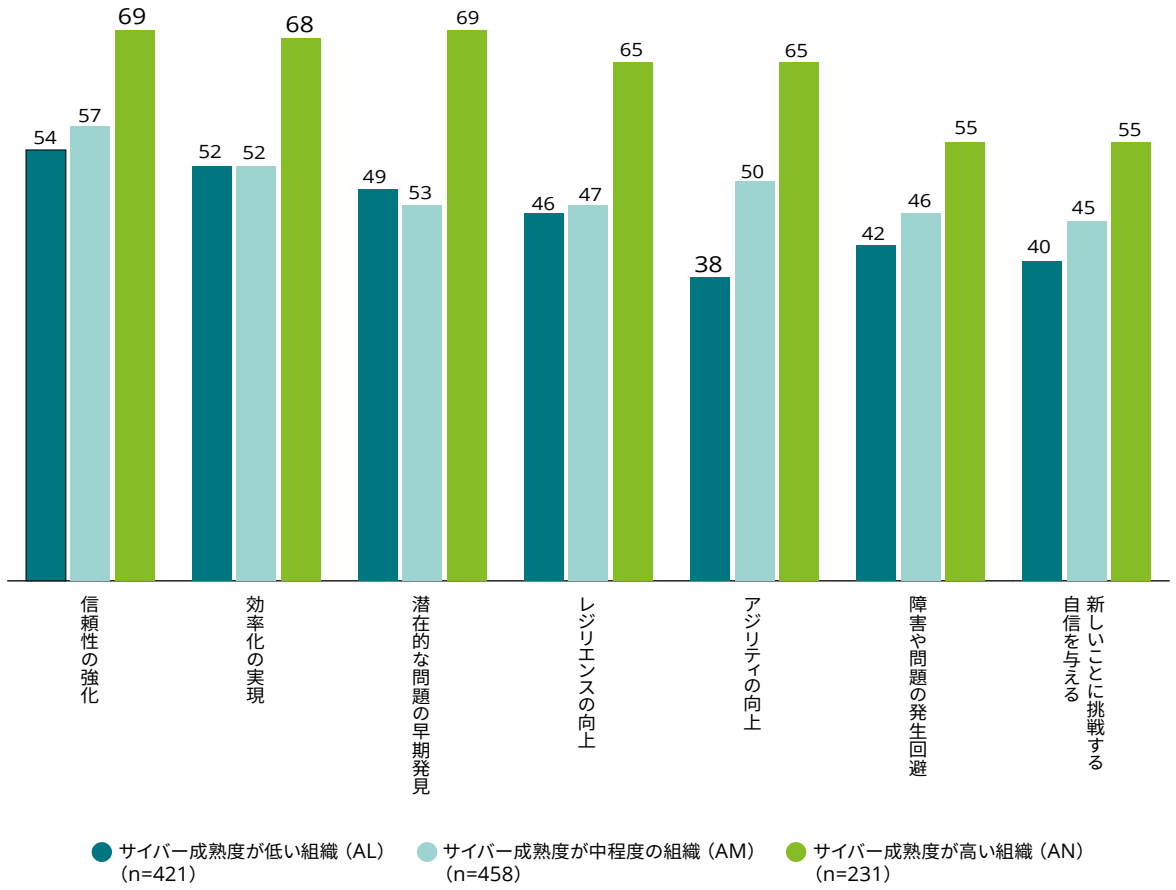
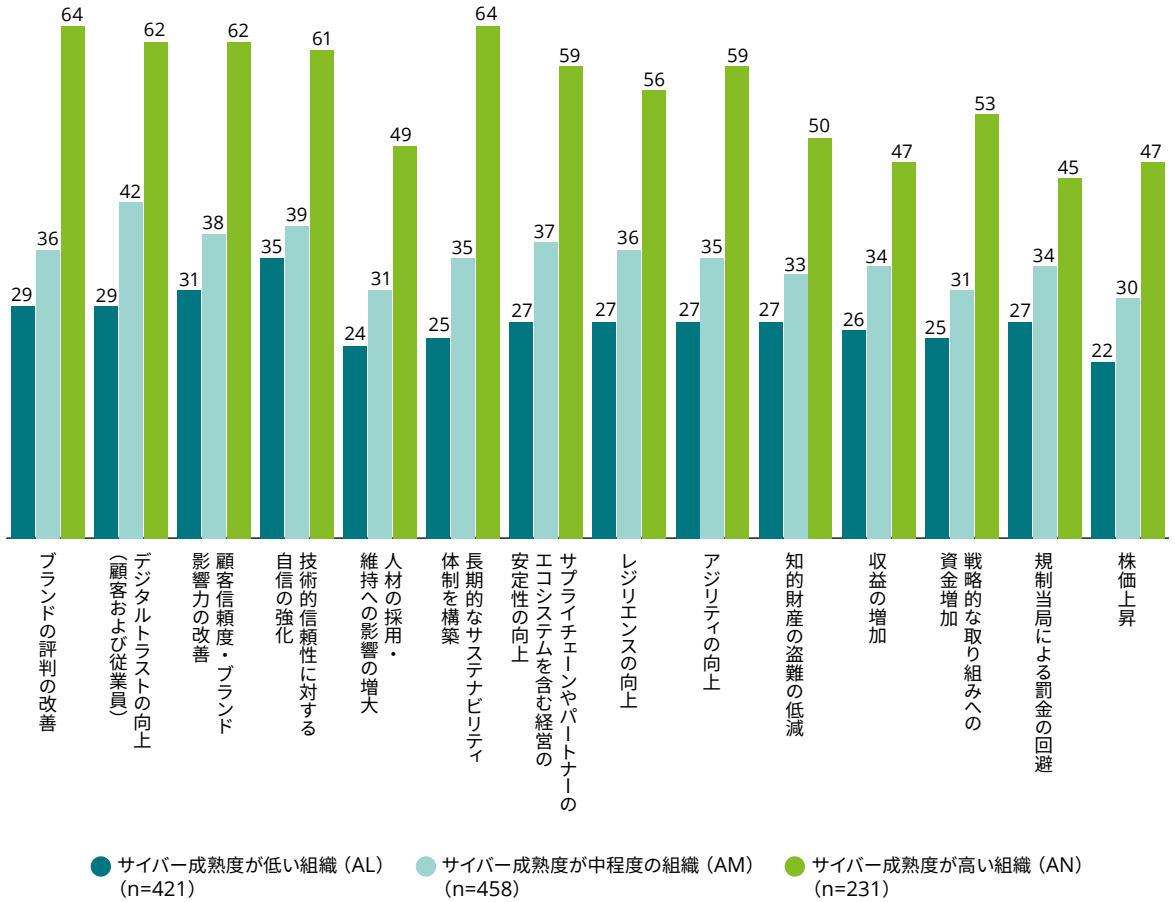


図6：実益の享受

サイバー施策は以下の分野でプラスの影響をもたらしている

（単位：%）



また、最も高いパフォーマンスを発揮している組織では、ブランドの評判の改善（64%）、収益の増加（47%）、サプライチェーンやパートナーのエコシステムを含む経営の安定性の向上（59%）、人材の採用・維持への影響の増大（49%）、長期的なサステナビリティ体制の構築（64%）、顧客信頼度・ブランド影響力の改善（62%）といった領域において、サイバー施策によるプラスの影響があったと回答する傾向が見られました。

サイバーにおいて、信頼は最も重要な問題です。成果をあげるための「エコシステム」として、全てのステークホルダーと信頼関係を構築する必要があります。例えば、信頼度の高い従業員は顧客満足度を2倍に高めることができ、また、顧客があるブランドを信頼している場合、そのブランドで再購入する可能性は88%高まるのです。顧客との信頼関係の構築は、パートナーにも影響を与え、時価総額を4倍まで向上させ、信頼度の高い企業の時価総額は最終的に同業他社を最大400%上回るといわれています。

また「2023年Global Future of Cyber Survey」のデータに基づき、グローバルな組織は、サイバーとそれがもたらす信頼を含むメリットとの関連性を明確に確認することができています。サイバーに投資している組織は、様々な価値指標で大きなメリットを得ていますが、最も高いパフォーマンスを発揮している組織は、全ての戦略的施策でその価値をより多く得ています（図6）。

顧客の期待

「私の個人的な推測では、顧客は我々の製品に対してサイバーセキュリティのために多くの追加料金を支払うことを望んでいないと思います。顧客が*期待*するのはサイバーセキュリティがすでに組み込まれていることでしょうし、そうすること自体が*差別化要因*となるのです。」

—自動車業界 CISO

400%

顧客との信頼関係の構築は、パートナーにも影響を与え、時価総額を向上させ、信頼度の高い企業の時価総額は最終的に同業他社を最大400%上回るといわれています。

成熟度が高いサイバー組織が、成熟度が低・中程度の組織を上回っているもう1つの領域は、サードパーティのサイバーサービスを利用することで得られる価値です。

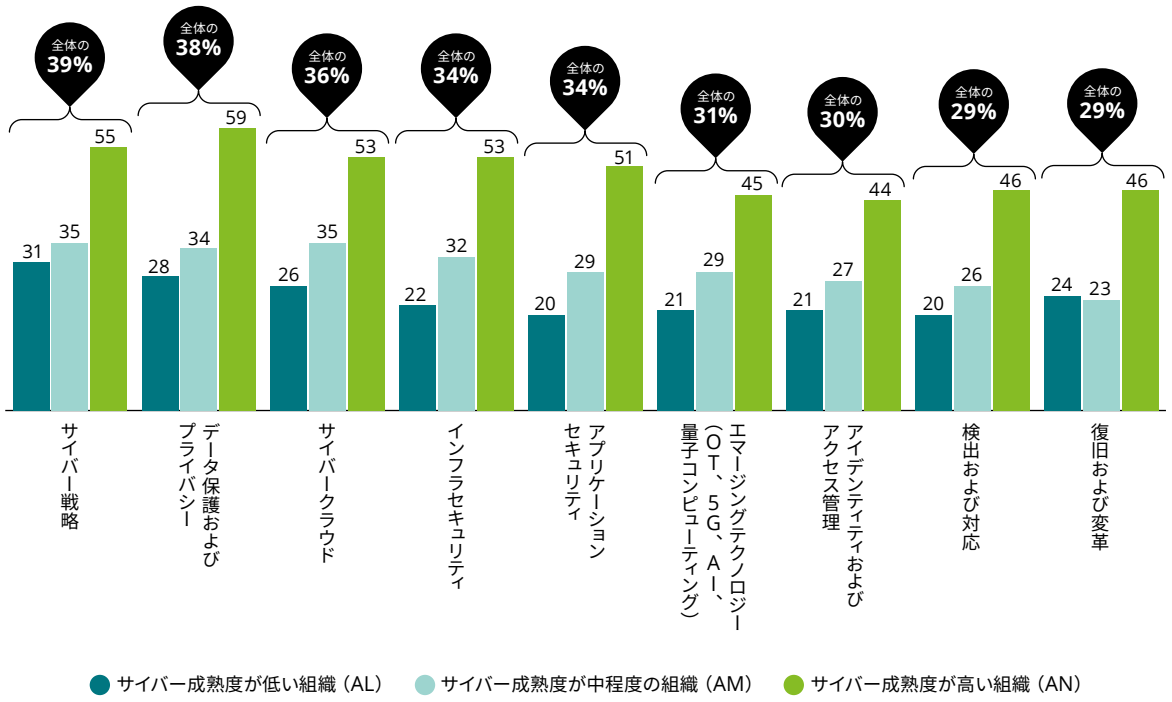
優れたパフォーマンスを発揮する組織の過半数が、サイバー戦略、データ保護およびプライバシー、サイバークラウド、インフラセキュリティ、アプリケーションセキュリティに関するサードパーティサービスに、測定可能な価値があると回答しています。一方、成熟度が低い組織、中程度の組織のうち、これらの領域で価値があると回答した企業は少数でした。

組織はサードパーティサイバーサービスがもたらす価値を活用するために、増大するサービスエコシステムとそこから生じる固有の複雑性を管理する方法を検討する必要があるということです（図7）。

図7：ベンダーから価値を得る

サードパーティサイバーサービスから価値を得ていると企業が回答した領域

（単位：%）



学ぶべき教訓：リーダーに倣う

優れたパフォーマンスを発揮しているこのような企業が、サイバーへの投資からビジネス全体に大きなメリットを引き出していることを考えると、他の組織もサイバー成熟度が高い企業の例を参考にし、自社内のより広い範囲でサイバーへのエンゲージメントを実現するための指針として活用することが推奨されます。

これらの成熟度が高い組織がサイバーから得た成功に基づき、自社のビジネスも以下のような質問を深く掘り下げる時期が来ているのかもしれません。

自社には適切なテクノロジーとパートナーのエコシステムが導入されているか、また拡大する複雑なサードパーティネットワークをどのように管理すればよいか？

自社は正しい方法で、正しい領域に投資ができているか、またサイバーが組織全体のどこにどのような価値をもたらしているかを理解するための適切なフレームワークがあるか？

自社は正しい方法で、正しい領域に投資ができているか、またサイバーが組織全体のどこにどのような価値をもたらしているかを理解するための適切な「価値フレーム」があるか？

サイバーの将来を形作る重要なインサイト―注目すべき5つの領域

1 多方面での関与

すでに述べたように、優れたパフォーマンスを発揮する組織は、組織全体がサイバー活動に関与しています。成熟度が高い組織が成熟度が中程度または低い組織に比べて、より多くのサイバー関連の先進的な事例を活用していることは当然なのですが、この組織の関与度合いの格差は最も顕著なものの1つです。

リーダーシップ
成熟度が高い組織のうち、ビジネスとITのシニアリーダーで構成された管理組織を設置してサイバープログラムを監視している組織の割合は、成熟度が低い組織の約3倍、中程度の組織の約2倍です（成熟度高の企業が60%、成熟度中の企業が36%、成熟度低の企業が22%）。

シナリオ策定
同様に、成熟度が高い組織は、成熟度が低い組織の約3倍、中程度の組織の約2倍、組織レベルや役員レベルでインシデント対応のシナリオ策定を行っています（成熟度高の企業が60%、成熟度中の企業が30%、成熟度低の企業が20%）。

.

2 DX施策の重要性

成熟度が高い組織は、DXの主要な優先事項の中心にサイバーを置く傾向が非常に強く見られます（図8）。

そのようなDXにおける優先事項の導入は、業務のアジリティとビジネスの成功を確保するために不可欠です。しかし、そのいずれもが重大なサイバーリスクを伴い、成熟度が高い組織はその現実に特に敏感にとらえているといえるかもしれません。

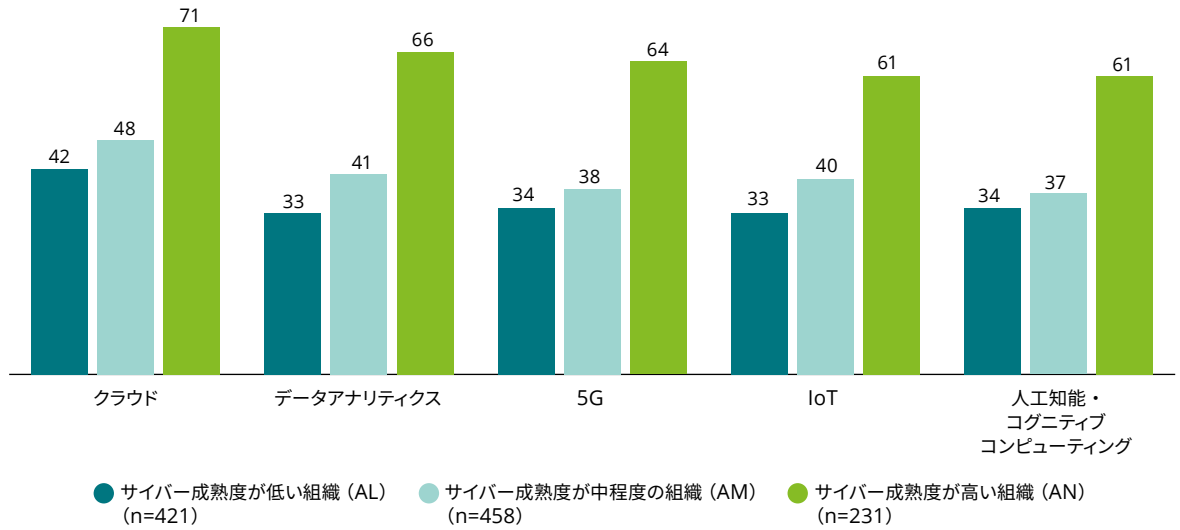
例えば、AIはサイバー戦略や企業のデジタルビジネスに関する目標達成のイネーブラーになりえますが、デジタル技術につきものであるサイバーリスクをもたらす可能性もあります。ここで紹介した先進的な事例以外にも、デロイトが最近発表した「State of AI in the Enterprise」レポートでは、リスク軽減のための具体的な取り組みがコスト削減や新規市場への参入などのより良い成果ももたらすことが強調されています。AI関連リスクは企業にとって非常に重要な問題です。また、AIの意思決定における説明可能性と透明性、データプライバシーや同意の不履行、AIシステムに関する安全性の懸念など、いずれも組織が懸念する倫理的リスクとして大きくクローズアップされていることが分かりました[5]。

これらのリスクを管理することは、組織のAIの取り組みに大きな影響を与えます。実際、AIに関する調査では、回答者の50%がAI関連リスクの管理をAIプロジェクト拡大の阻害要因の1つとして挙げています。こうした意見にもかかわらず、AIリスク管理を組織全体のリスク管理の取り組みに整合させて実施している回答者はわずか33%にすぎません。しかし、調査対象組織のうち、高い成果を上げた組織の33%、成果が低い組織の29%は、AIシステムの独立監査を外部ベンダーに依頼しています。

AIで結果を出すことを目指す
「しかし、一言でいえば、私たちはビジネスのイネーブラーとしてサイバーセキュリティに対応しながら、量子コンピューティングやメタバース、そしてAIも含めて、（サイバーに関しての）知識共有や理解促進のための取り組みも進めているのです。」

―NEOM CISO、Mesfer Almesfer

図8：サイバーとともに進化する
具体的なDX構想におけるサイバーの重要性についてどのように認識しているか（成熟度グループ別）
（単位：%）



3 強固な計画

リスクを効果的に軽減し、ビジネス価値を高めるサイバー戦略を策定するには計画が最も重要であることが分かっています。そして本レポートで特定された優れたパフォーマンスを発揮する組織は、計画の重要性を十分に認識しているようです（図9）。

サイバー成熟度が高い組織では、以下を含む強固な計画を策定しているという傾向が見られます。

- 毎年更新・テストされる**サイバーセキュリティインシデント対応計画**（成熟度が高い組織の87%）
- サイバー脅威に対処するための**事業・戦略計画**（91%）
- データの保管、処理、送信の全ての段階で**データ保護方法を評価する包括的な計画**（88%）

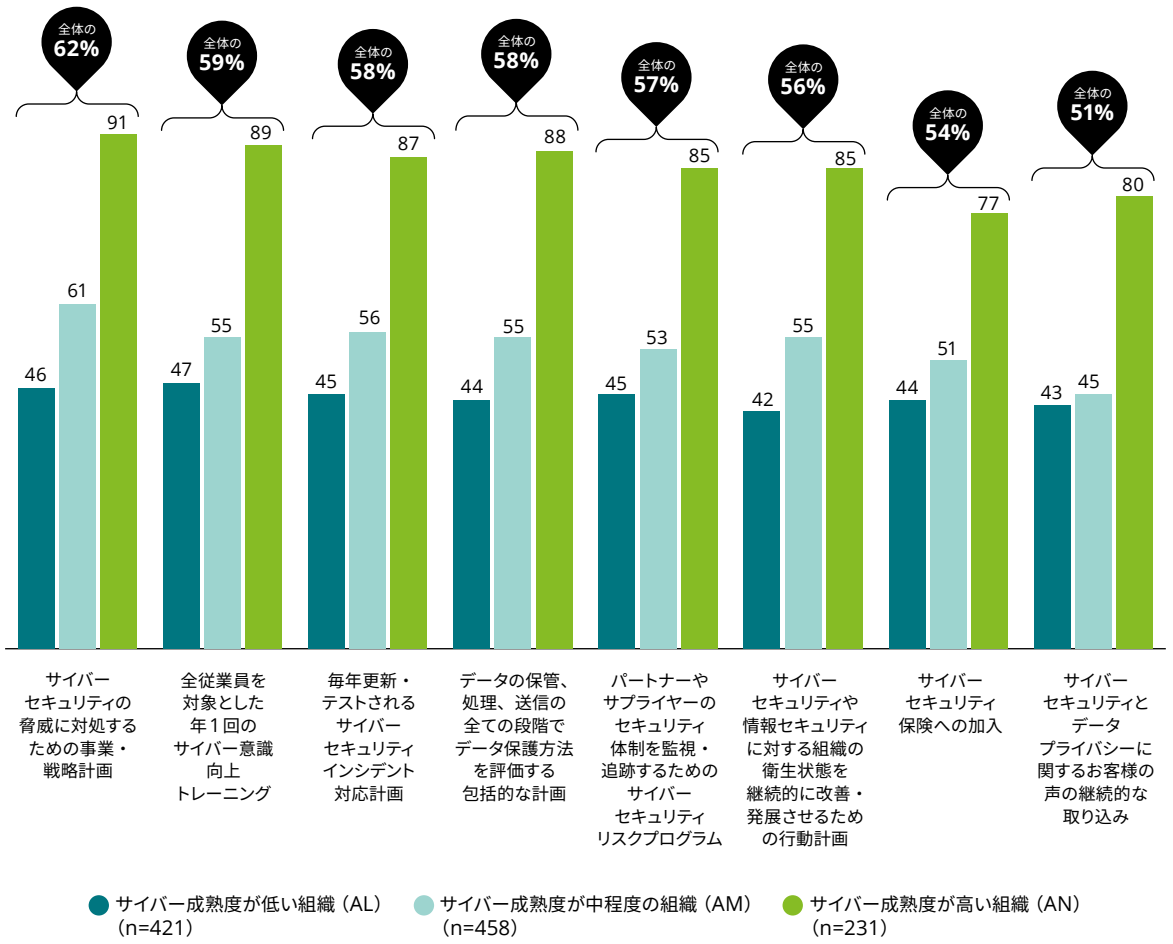
91%

成熟度が高い組織のうち91%は、サイバー脅威に対処するための事業・戦略計画を策定しています。

図9：計画の現状（成熟度グループ別）

各活動を十分に実施している組織

（単位：%）



4 人材への評価と投資

サイバーに関する問題や活動は、脆弱性をつく攻撃者であれ、サイバー戦略・戦術を担当する意思決定者であれ、デジタルビジネスプロセスやサイバープログラムを実行する最前線の従業員であれ、最終的には人に関するものです。優れたパフォーマンスを発揮するためには、スキル、経験、そしてサイバーに特化した強力な人材が必要不可欠です。サイバー施策を推進するために適切な人材を確保するには、従来の人材像にとらわれない視点が重要になってきます。例えば、カスタマーエクスペリエンスデザイナーは、取引プロセス、データ収集、プライバシーに関する潜在的な脆弱性を特定し、サイバー施策に必要なインサイトをもたらすかもしれません。

人材、特に真に適切な人材を集め、定着させることは難しいことです。サイバー関連の責任ある立場になれば、ストレスやその他のプレッシャーは当然発生します。そしてそれは激しいものです。実際、この調査の一環としてインタビューに応じていただいた英国の金融業界のリーダーである回答者は、「上級責任者」に任命されたことで、サイバーリスクは事実上CISOの管轄となり、特定の事象が発生すると「深刻で個人的な影響が及ぶ可能性がある」と指摘しています。サイバーは本質的にビジネスに深く関与するものであるため、企業内の単一の役割や部門が管轄すべきものではなく、どのようにサイバーリスクに対処していくべきかというのは盛んに議論されている点でもあります。

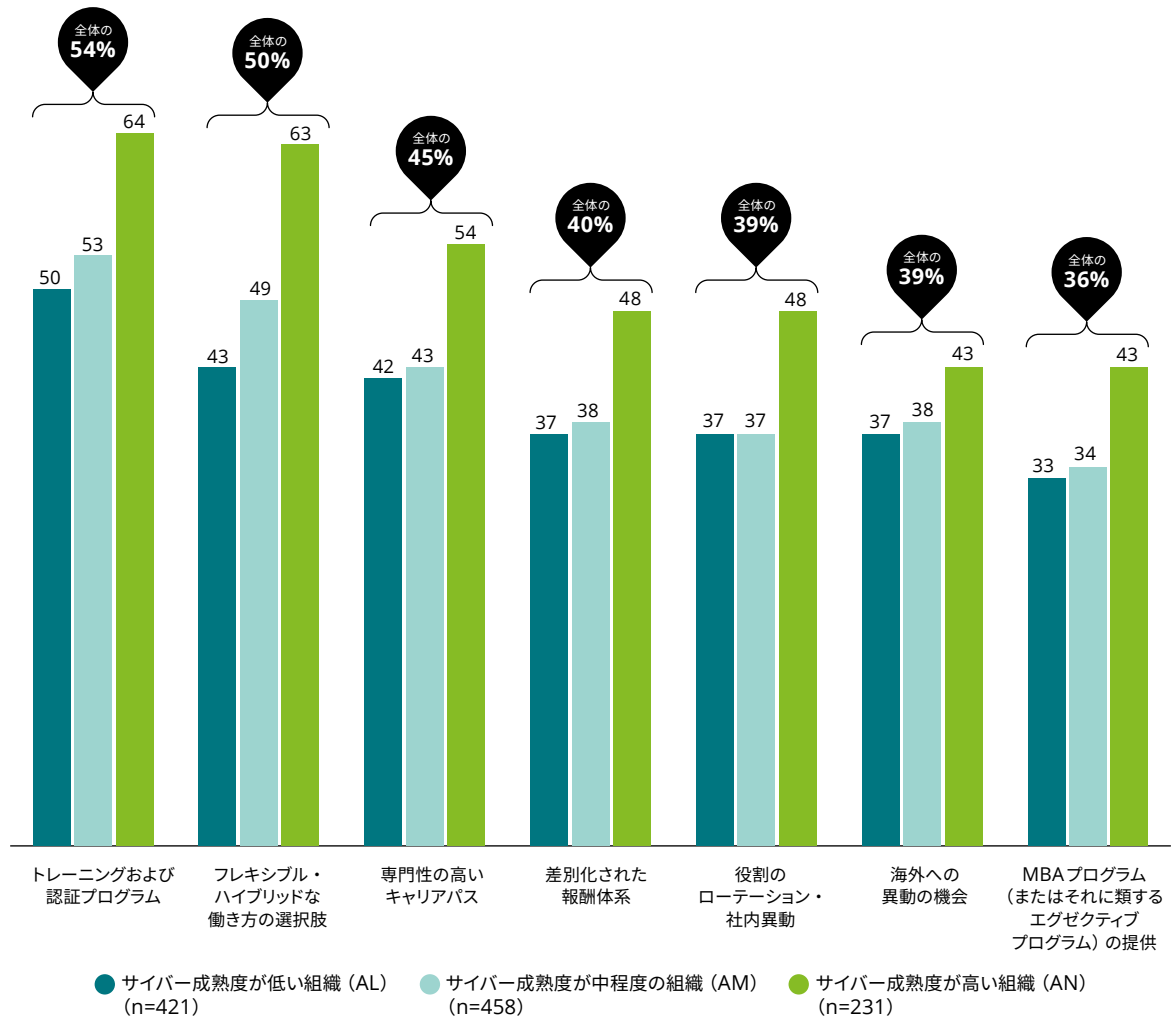
全体として、成熟度が高い組織は、経験豊富な人材がサイバー関連の取り組みに対してもたらす重要性を認識しており、貴重な人材を維持するために有意義な措置を講じています。成熟度が高い組織は、サイバー管理における最大の課題として、熟練したサイバー専門家の不足を挙げる傾向が見られます（成熟度高の企業が47%、成熟度中の企業が38%、成熟度低の企業が37%）。

より成熟した組織では、その強固なプログラムが人材課題の一端を担っている可能性があります。サイバー関連の活動をより広く深く実施するにつれ、チームや能力が限界に達していることに気づき、より成熟したプログラムをサポートするために、高度で多様なスキルを持つ人材をより多く導入する必要性を認識するかもしれません。

しかし、成熟度が低い組織は、はたして本当に同じレベルの人材の課題に直面していないのでしょうか。それとも適切なスキルを持った人材を配置することに十分に重点を置いていないだけなのでしょうか。後者であれば、人材獲得を重視することが優先されるべきです。人材こそは、最終的に成熟度が高い組織になるために役立つものです（図10）。

図10：人材の活用方法

既存の人材を活用、維持、育成するために組織がとっている戦略



5 ツールやサービスの多様なエコシステム

成熟度が高い組織は、自分たちだけではサイバーの将来をリードすることができないことを痛感しています。ビジネス価値をもサポートできる未来志向のサイバー能力を構築するためには、テクノロジー、能力、および外部から提供される広範なエコシステムに頼る必要があります。

優れたパフォーマンスを発揮する組織は、パフォーマンスが中程度および低い組織と比較して、以下に関連したサードパーティの製品やサービスを幅広く導入している傾向があります（図11）。

- アプリケーションセキュリティ
- サイバークラウド
- サイバー戦略
- データ保護およびプライバシー
- 検出および対応
- エマージングテクノロジー（OT、5G、AI、量子コンピューティング）
- アイデンティティ管理およびアクセス管理
- インフラストラクチャのセキュリティ
- 復旧および変革

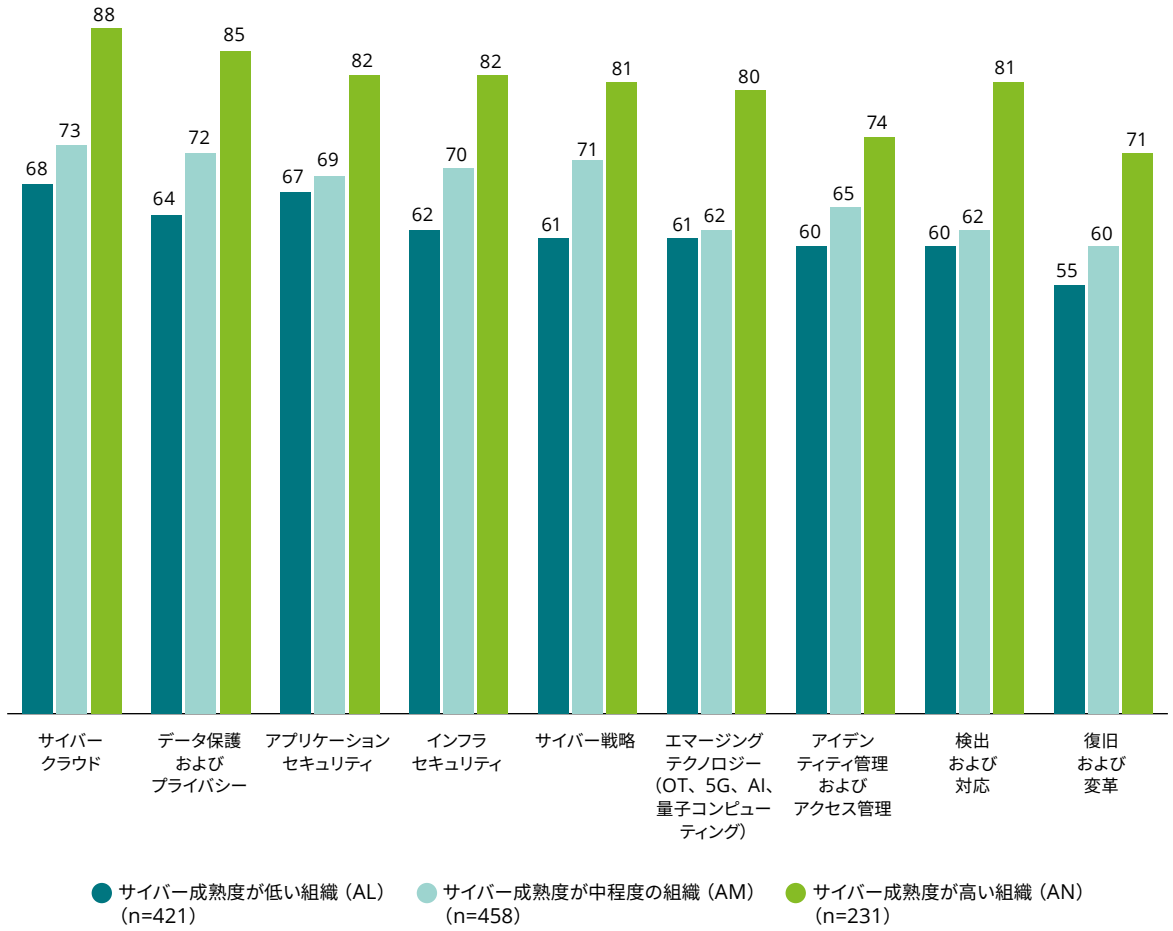
ツールやサービスの導入はサイバーレディネスを向上させますが、同時にエコシステムを確実に計画、管理、運用する必要性が生じます。複数のベンダーと協力して複雑に進化する問題を解決し、統合された環境の一部としてサイバー機能を実行、監視、更新することは、それ自体が複雑なニーズをもたらします。

皮肉なことに、複数のサイバーベンダーが存在することで、複雑さが増し、侵害などの新たなリスクへの入り口となる可能性があります。状況によっては、ベンダーの監視を統合することがこの課題をシンプルにする方法の1つとなります。

今後2年間で使用されるサイバーベンダーの平均数は増加すると予想されるため、監視を簡素化し、一元化するケースも同様に増加すると思われます。また、業界団体などの招集機関と連携し、エコシステムの管理方法に影響を与える可能性のある技術開発や新たな慣行をよりよく理解することも、検討すべきアプローチの1つです。

図11：外部を頼る

組織は以下の領域でサードパーティのサイバーサービスプロバイダーを利用している



行動の変化

従業員の潜在的なサイバーリスク指標を検出し軽減するための自動行動分析ツールの利用が大幅に増加しました。今回の調査では76%がそうしたツールを使用していると回答していますが、2021年の調査では使用していると回答したのは53%でした。

視野を広げる

「100%社内だけで対応する戦略ではうまくいきません。規模が拡大できないし、うまくいかず象牙の塔のようになる傾向があります。私たちは様々なパートナーと仕事をしていますが、これは主に新しいアイデアを得るためであり、戦略面で導いてもらうためでもあります。」

—自動車業界 CISO

さて、これから どうすればいいのか？

企業のリーダーがビジネスの拡大や成長を期待するのであれば、サイバーはその計画に不可欠な要素であると考えるべきです。また、サイバーは今後のビジネスの目標達成のために使用する全てのツールにおいて不可欠な要素であるべきです。

「サイバーは後回し」という時代は終わりました。どのようなビジネスにとっても、強力なサイバー戦略があれば新しい技術力はより効果的なものになります。新しいテクノロジーは、将来のビジネスモデルを支える革新的なソリューションをもたらすと同時に、サイバー面では予期せぬ課題をもたらします。サイバー戦略や投資が後れを取らないようにしながら、これらのテクノロジーをどのようにしてビジネス価値に活かしますか？

まず、ゼロトラストアプローチは、新しい技術に関わる取り組みの中心であるべきです。セキュリティアーキテクチャから信頼の前提を取り除き、全てのアクション、ユーザー、デバイスを認証することで、ゼロトラストはより強固でレジリエントなセキュリティ体制を実現します。組織的なメリットに加えて、エンドユーザーにとっても効率的な作業に必要なツールやデータへのシームレスなアクセスが可能になるという大きなメリットがあります。

「当社のように大規模なIT資産のある組織では、ゼロトラストトランスフォーメーションへの道のりは複雑になります。多様な業務に対応するために様々なデバイスとの接続を求めるパートナーで構成される、拡大し続けるエコシステムの複雑性を管理しながら、ビジネスのペースで変革を進める、しかも全てセキュアに進める必要があるのです。」

—Shell グループCIO兼CISO、Allan Cockriel

「AIやスーパーコンピューティングのようなデータインテンシブなものやビジネスに高度に特化したものなど、デジタルソリューションはより幅広く多様化していきます。当社のサイバー環境を効果的に保護し、規制基準を満たすようにするには、そのようなソリューションを常に更新していく必要があります」

—BASF Data Protection Officer、Charlie Huang

イノベーションの導入についていえば、まず戦略から始め、その戦略を支える利用可能なテクノロジーをサイバーの観点から理解し、そのうえでクリティカルな視点で見るようにしてください。例えば、あるデータサービスやプラットフォームを利用することはどのように組織の目的に合致し、それによってどのように信頼を生み出す能力が強化され、リスクや脅威からの解放が実現されるのでしょうか。そこから、適切なニーズに適切なソリューションを適用するようにします。

将来に備える

新しい技術に内在するリスクと機会を察知することは、進化を続ける脅威という状況に対応するための方法の1つです。急速に変化するテクノロジーのトレンドに追いつくべく、サイバー施策を進めるというものではないでしょう。テクノロジーの変化に対する備えが不十分であればあるほど、サイバーリスクの管理に対する備えも不十分となってしまうため、取り組みを進める必要があるのです。

一例として、5Gの重要性が高まっていることが挙げられます。5Gは今回の調査でDXの優先事項の上位項目リストに新たに加わりました。5Gは遠隔医療や製造業における資産追跡、高度なトレーニングのための拡張現実など、新しいユースケースを可能にする一方、大きなアタックサーフェスも存在します。5Gの導入には、当初からセキュリティを設計して組み込むことが重要ですが、それは同時にとてつもなく複雑な問題をもたらすことになります。

一方、AIは今回の調査でも優先事項の上位項目に入っており、サイバーを含む様々な面での複雑性に対処する際に役立ちます。セキュリティ侵害に悩まされる企業にとって、サイバーAIはセキュリティチームがサイバー攻撃者の動きを上回るスピードで対応できるだけでなく、その動きを予測して事前に行動することも可能にし、戦力増強につなげることが可能となります。また、AIと自動化により一部のアナリストの面倒な作業が排除できるため、そのアナリストをより戦略的で困難な役割を果たせるように育成することができます。

また、もっと先にあるテクノロジーについて考えはじめるのに早すぎるということはありません。量子コンピューティングもその1つです。今回の調査の回答者のうち、今後数年間のデジタル優先事項としてこれを挙げていたのはわずか4%でした。量子コンピューティングは、企業にとって非常に大きな潜在的コンピューティングパワーを発揮する一方で、サイバー攻撃者にとっての武器にもなりえるため、企業には「Quantum Readiness（量子コンピューティングへの準備）」という新たな足場が必要なのです。

セキュリティバイデザイン

「私たちは、セキュリティが私たちの価値提案の多くの要素の1つであることを確認するために、『セキュアバイデザイン』と呼んでいるものに実際に投資しています。ソフトウェアと製品のライフサイクル全体にわたってポリシー、ツール、コントロールに投資し、安全で優れた技術を確実に作り上げています。顧客はそれを期待しているのです」

—Shell グループCIO兼CISO、Allan Cockriel

前進する

サイバーの将来とビジネスの将来は密接に絡み合っています。サイバーに関する考え方、計画、活動をどのように全てのビジネス施策に組み込むかがその施策の成功に直接影響します。

言い換えれば、サイバーは基礎的なもので、ビジネスの将来を支えるデジタルトラストを実現し、維持するための基盤です。ビジネスがデジタル領域にますますシフトしていく中で、効果的なデジタルエコシステムを構築するには、ビジネスの成功を促進する効果的なサイバー戦略を策定する必要があります。

ブランドの評判、顧客の信頼とロイヤルティ、経営の安定性、収益の増加。これらは全てサイバー関連の施策をいかに計画し実行するか、つまりサイバーの基盤をいかに強固なものにするかとつながっています。新しいクラウド構想に着手するとき、新しい製品やサービスを開発するとき、サードパーティをエコシステムに追加するとき、そして従業員に新しいツールを提供するときに「cyber first」を考えることが不可欠です。サイバーの重要性はインサイト、プラットフォーム、接続性、効果的な体験、整合性の必要性など、他の全てのデジタル必須事項にも織り込まれているのです。

始めましょう

サイバーにどのようにアプローチするかは、ビジネスの将来にどのようにアプローチするか、そしてビジネスの目的をどの程度達成できるかに大きく影響します。現在どのような状況であろうと、またこれからどのような道を進みたいと考えていようと、なにが可能で今後なにが待ち受けているのかを明確に理解することから始めることが大切です。

謝辞

Ian Blatchford, Scott Buzik, Luca Covolo, Deborah Elder, Jaya Gopalan, Jeremy Guterl, Matthew Holt, Dan Konigsburg, Daphne Lucas, Diana Kearns-Manolatos, Emily Mossburg, Mike Nash, Kelly Nelson, Jud Payne, Sean Peasley, Ashley Reichheld, Heather Saxon, Daniel Soo, Scott Tillett, Niels van de Vorle, Marius von Spreti, Emily Werner

問い合わせ先

Emily Mossburg
Global Cyber Leader
emossburg@deloitte.com
+1 571 766 7048

Ian Blatchford
Asia Pacific Cyber Leader
iblatchford@deloitte.com
+61 474 288 278

Amir Belkhelladi
Canada Cyber Leader
abelkhelladi@deloitte.ca
+1 514 393 7035

Peter Wirnsperger
Central Europe
Cyber Leader
pwirnsperger@deloitte.de
+49 40 320804675

Niels van de Vorle
North and South
Europe Cyber Leader
nvandevorle@deloitte.nl
+31882882186

César Martín Lara
Spain Cyber Leader
cmartinlara@deloitte.es
+34 914381416

Deborah Golden
United States
Cyber Leader
debgolden@deloitte.com
+1 571 882 5106

桐原 祐一郎
Kirihara, Yuichiro
Japan & Asia Pacific
Cyber Leader
ykirihara@tohmatsu.co.jp

Endnotes

1. Deloitte 2021 Future of Cyber Survey.
2. Closing the cloud strategy, technology, and innovation gap. Deloitte US Future of Cloud Survey Report, 2022.
3. Future of Digital Trust: Driving forces, trends and their implications on our digital tomorrow. Deloitte. 2021.
4. The Four Factors of Trust: How Organization Can Earn Lifelong Loyalty.
5. Fueling the AI transformation: Four key actions powering widespread value from AI, right now. Deloitte's State of AI in the Enterprise, 5th Edition report, October 2022.
6. Take 5: 5G cybersecurity, Part of Deloitte's 'Take 5 on 5G' article series.
7. Cyber AI: Real Defense, Deloitte Tech Trends 2022.
8. Quantum Cyber Readiness Deloitte's perspective on transitioning to a quantum secure economy

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイトトーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイトトーマツ税理士法人、DT弁護士法人およびデロイト トーマツ コーポレート ソリューション合同会社を含む）の総称です。デロイトトーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約30都市に約1万7千名の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTLおよびDTTLの各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTLはクライアントへのサービス提供を行いません。詳細は www.deloitte.com/jp/about をご覧ください。
デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイトアジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務、法務などに関連する最先端のサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促し、より豊かな経済、公正な社会、持続可能な世界の実現に向けて自ら率先して取り組むことを通じて、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来175年余りの歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの約415,000名の人材の活動の詳細については、(www.deloitte.com）をご覧ください。

Member of
Deloitte Touche Tohmatsu Limited