uvance Wayfinders

Consulting by Fujitsu

サイバー攻撃のレジリエンス格差

富士通 サイバーセキュリティレポート

FUJITSU

AI時代に成功する企業は、いかにイノベーション・リスク・レジリエンスのバランスをとるか

サイバーセキュリティの深刻なインシデントが増え続けています。脆弱性を発見してから悪用されるまでの猶予は、これまでは数週間でしたが、いまではたったの数時間です。頻繁な攻撃は業務を混乱させて社会的信頼を失墜させるだけでなく、何十億という単位で市場価値を損ないます。

2025年8月、ジャガー・ランドローバー社が標的にされたサイバー攻撃では、19億ポンドの被害があったと報道されました。また、あるグローバル食品企業に対するランサムウェア攻撃では、生産・出荷ラインを停止せざるを得ず、顧客や従業員データが流出する騒ぎとなりました。

このような事件は氷山の一角に過ぎません。富士通が、グローバルな企業・組織の経営層をはじめとする意思決定に関わるビジネスリーダー400人を対象に行った調査では、サイバー攻撃による業務中断が、あらゆる業種や規模の企業の日常的なリスクになっていることが明らかになりました。組織がデジタルトランスフォーメーションを加速させる一方では、AI技術も発達することで犯罪者の攻撃範囲が広がっただけでなく、新しい攻撃手段として悪用されている現状があります。

2/3

…の企業が、過去12か月間に1件以上のサイバーセキュリティ案件が発生したと回答。

経営層はこうした変化をすでに把握しているようです。調査に協力した組織の約3分の2が、過去12カ月間に1件以上の重大なサイバーセキュリティインシデントがあったと回答しました。また、過去3年間でサイバー攻撃の頻度は増加していると述べています。

このため、脅威に対応し、ビジネスを混乱や被害の長期化から守る「サイバーレジリエンス」が、いま経営層の最大の課題となっています。サイバーレジリエンスについて「組織全体の戦略において極めて重要」と67%の経営層が回答したのに対して、「技術的な要件に過ぎない」と回答したのはわずか33%でした。

多くの組織がサイバー攻撃のリスクを認識していますが、対応レベルはさまざまです。当社の調査によると、リーダーシップや投資、イノベーションなどを通じてレジリエンスを強化できた組織と、脆弱な組織との間には、大きな差があることがわかります。

AIの効果の陰に新たなリスク

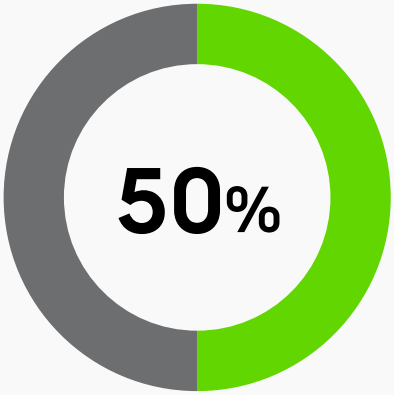
AIは組織運営を変革する一方で、サイバー脅威の様相も変えつつあります。

犯罪組織は、AIを悪用し、システムの脆弱性をものすごいスピードで発見したり、マルウェアを自動で開発したりできるようになりました。フィッシングの手口はより巧妙化しています。一度、攻撃者にシステムへのアクセス権を知られたら最後、攻撃者はAIを使いあっという間に情報を盗み、大きな混乱を引き起こします。

調査では、経営層は脅威の深刻さを認識していることがうかがえます。「AIを活用したサイバー攻撃は、自社のセキュリティとレジリエンスにとって最大のリスクだ」と回答したのは61%にのぼりました。

脅威は企業の外側からだけではなく、内側にも発生します。AIの導入が広がるのにあわせて、攻撃に悪用される領域も拡大しています。多くの企業ではAIのイノベーションのスピードが速すぎてガバナンスの対処能力が追い付いていません。調査では、経営層の50%が、自社のセキュリティやガバナンスの仕組みが追いつかないにも関わらず、AIによるイノベーションを優先させるプレッシャーを感じていると答えています。

ガバナンスによる対応は、往々にして事後的になりがちです。半数以上（56%）の組織では、最初から特定のセキュリティに予算をあてて対策を立てるのではなく、テクノロジー導入後に既存のセキュリティ対策をあてはめていると回答しました。このような目的に合わない仕組みには脆弱性が残り、悪用されやすいのが特徴です。



…の幹部社員は、サイバーセキュリティやガバナンスの整備より、AIによるイノベーション加速を優先しなければならないプレッシャーを感じているという。

透明性の確保も課題です。多くの経営層が、従業員がどのようにAIを利用しているのか把握していないと述べています。57%は、組織の管理下にない、いわゆる「シャドーAI」が大きなリスクだと指摘しています。AIの適切なガバナンスにはモニタリング体制が必要です。

一方で調査は、AIがもたらすポジティブな効果も示しています。組織が適切なガバナンスを確立できれば、セキュリティの領域を超えたメリットがあるというのです。回答者の約10人中7人（68%）が、強固なAIセキュリティは顧客やパートナー企業との信頼を強化し、長期的なビジネス価値につながると述べています。AIの推進とサイバー対策のバランスは難しい課題ですが、実現した際の成果は非常に大きいといえます。

「未然防止」から「発生後の対処」へ

従来のサイバーセキュリティ対策は、発生前に止める未然防止を軸に構築されてきました。しかし、攻撃が激増し手口も巧妙化したいま、サイバー犯罪を完全に防ごうとするのは現実的ではなくなっています。

この点について、多くの経営層も理解しているようです。現在のサイバーセキュリティは発生を前提としており、予防が主眼ではないと回答したのは67%です。サイバー攻撃に対するレジリエンスの真価とは、すべての攻撃を阻止できたかではなく、インシデント発生後も業務を継続できるかどうかにあります。組織は、最悪の事態に備えてセキュリティ対策を立てる必要があるのです。

調査結果を分析したところ、レジリエンスへの取り組み方には、組織によって明確な差があることがわかりました。一部の経営層は、重大なサイバーセキュリティ攻撃に適切に対処し、大きな損害を出さずに業務を復旧できると確信しています。このグループを、本調査では「先行グループ」と呼びます。一方で、サイバー攻撃が自社に与えるさまざまな影響がとにかく心配な経営層もいます。こちらは「その他の組織」と呼びます。

2つのグループの自信の差は、それぞれの戦略的な選択の違いからくるものです。次に、先行グループのサイバーレジリエンスが強い要因と、その他の組織が自信を持てない理由、そして両グループから何を学べるか考察してみましょう。

企業カルチャーとしてのサイバーセキュリティ

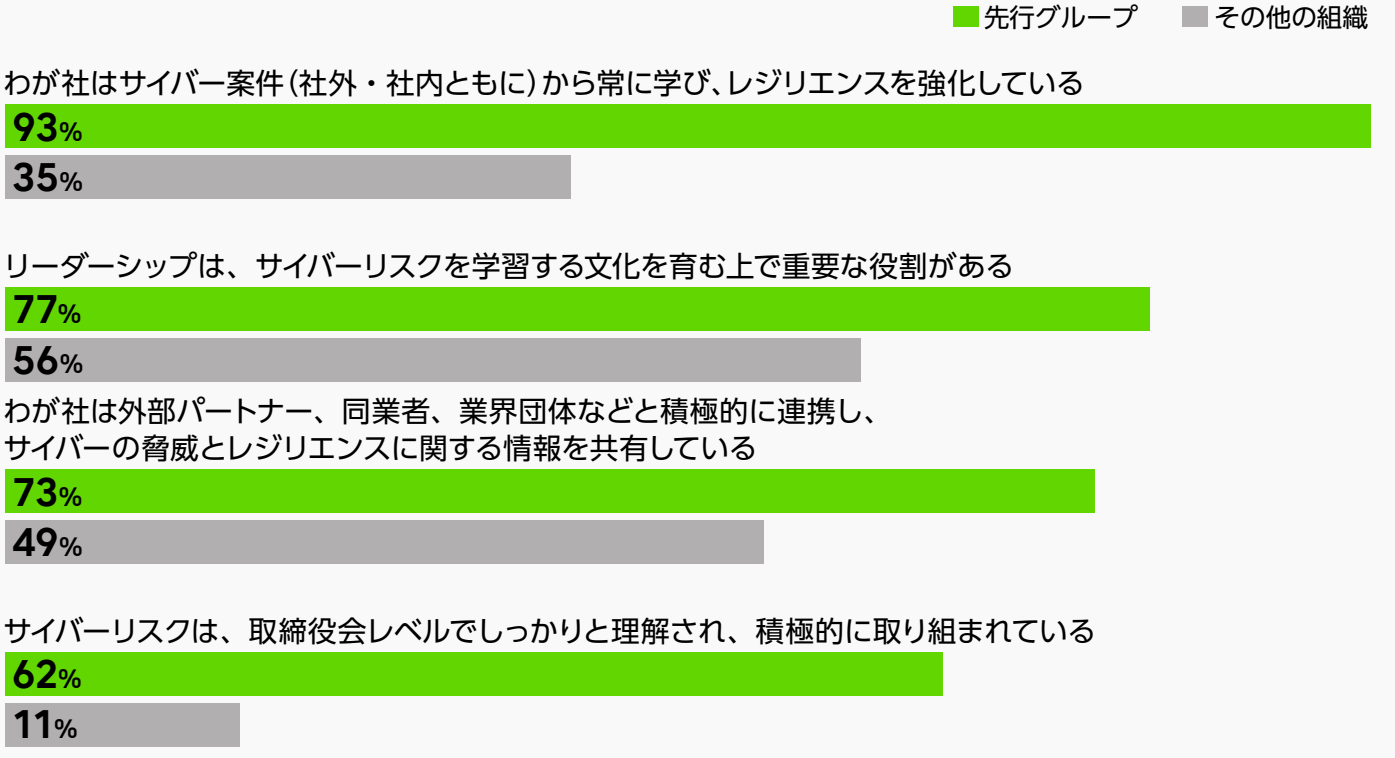
サイバーセキュリティの強度は、最も脆弱な部分への対策で決まります。一度の判断ミスや組織全体の意識の低さは、高度なセキュリティインフラでさえも危険にさらします。サイバーレジリエンスは全社的に取り組む優先課題である必要があります。

強固なレジリエンスがある組織は、サイバーセキュリティに関するカルチャーを変革したいと考えた場合、それがトップダウンで始まることを理解しています。先行グループの4分の3以上（77%）が、「自社の経営層はサイバーリスクを学習する文化を育む上で、重要な役割を果たしている」と回答しましたが、その他の組織では56%にとどまりました。

取締役レベルでは、この差はさらに顕著です。先行グループでは過半数（62%）が、「サイバーリスクは、取締役会レベルでしっかりと理解され、積極的に取り組まれている」と回答しましたが、その他の組織ではわずか11%にとどまりました。このようなリーダーシップの意識の差は、さまざまな現実的な影響となって現れます。サイバーレジリエンスを事業戦略全体に組み込むには、最高レベルからの指示が必須だからです。

先行グループではサイバーセキュリティが日々の最優先業務のひとつとして取り組まれている

Q：サイバーレジリエンスに関する以下の記述について、あなたの組織はどのくらい当てはまりますか？



先行グループは、レジリエンスには継続的な学習が不可欠だと理解しています。その大多数（93%）が、「社外・社内で発生するサイバーインシデントから常に学び、レジリエンスを強化している」と回答したのに対し、その他の組織では35%にとどまっています。また、73%は「外部パートナー、同業者、業界団体などと積極的に連携し、サイバーの脅威とレジリエンスに関する情報を共有している」と回答しましたが、その他の組織で同様の取り組みを行っているのは半数以下（49%）でした。

リードする企業では、サイバーレジリエンスはIT部門だけではなく、企業文化や意思決定のレベルで取り組まれていることが指摘できるでしょう。

先行する企業グループは責任あるイノベーションを重視

レジリエンスの高い組織ほど、イノベーションとガバナンスを両立できる傾向にあります。調査結果からは、先行する企業グループは、意識しながら両者のバランスを取っていることがうかがえます。72%は、「新興のテクノロジーはサイバーリスクを十分に理解し、安全策が整ってから慎重に導入する」としています。

その他の組織を見てみると、異なるアプローチです。過半数（59%）は、セキュリティ上の影響を完全に理解していない状態でも、スピード感を重視して導入しています。こちらのグループは導入競争では勝てるかもしれませんが、存在する認識の差は一度サイバー攻撃の標的となった場合、壊滅的な結果を招くおそれがあります。

格差は、AI戦略で特に顕著です。先行するグループは、そうではない組の4倍高い確率で、深刻なサイバーリスクにあわずAI主導のイノベーションを推進できる戦略を立てています。先行グループでは、従業員がどこでどのようなAIを使用しているかを把握しています。「シャドーAI」の使用状況については、56%が把握できているのに対し、その他の組織はわずか27%にとどまっています。

先行グループでは、次のフロンティアともいわれる「AIエージェント」についても一歩リードしています。10人中6人（61%）が、AIエージェントのシステムにも対応できるセキュリティ対策を組み込んでいます。これに対し、そのほかの企業では28%にとどまっています。

パターン認識や事前定義されたタスクに限定される従来のモデルとは異なり、AIエージェントは自律的に動き、少しの人間の介入や監督のもとで意思決定を行うことができます。この性質の違いは、実は脅威を増大させるものです。

内部的には、AIエージェントは複数のシステムと相互に作用することで脆弱性を生み出すおそれがあります。これは管理や監視が従来よりも難しいと考えられています。

AIエージェントに関する知識不足は、その他の組織で多かった課題です。社内のAIエージェントが、よくわからないサイバーリスクをもたらすのではと心配する割合は71%でした。先行グループの中で同じ懸念を抱いているのは37%と少なくなっています。

加えて、その他の組織の中では、サイバー犯罪にテクノロジーが悪用されることへの懸念も高い状態です。AIエージェントによるサイバー攻撃が発生した場合、新たなレジリエンス対応が必要になると、10人中8人（81%）が回答しました。これは先行グループの38%と比較して高い数値です。

AIの導入が加速する中では、組織はこのような知識の格差をできるだけはやく埋めていくことが求められています。アップスキリング、人材採用、外部とのパートナーシップなどがその手段となるでしょう。

「対処」から「レジリエンス」への転換

先行する企業グループとそれ以外のもうひとつの明確な違いは、サイバーレジリエンスの長期的な優先順位です。

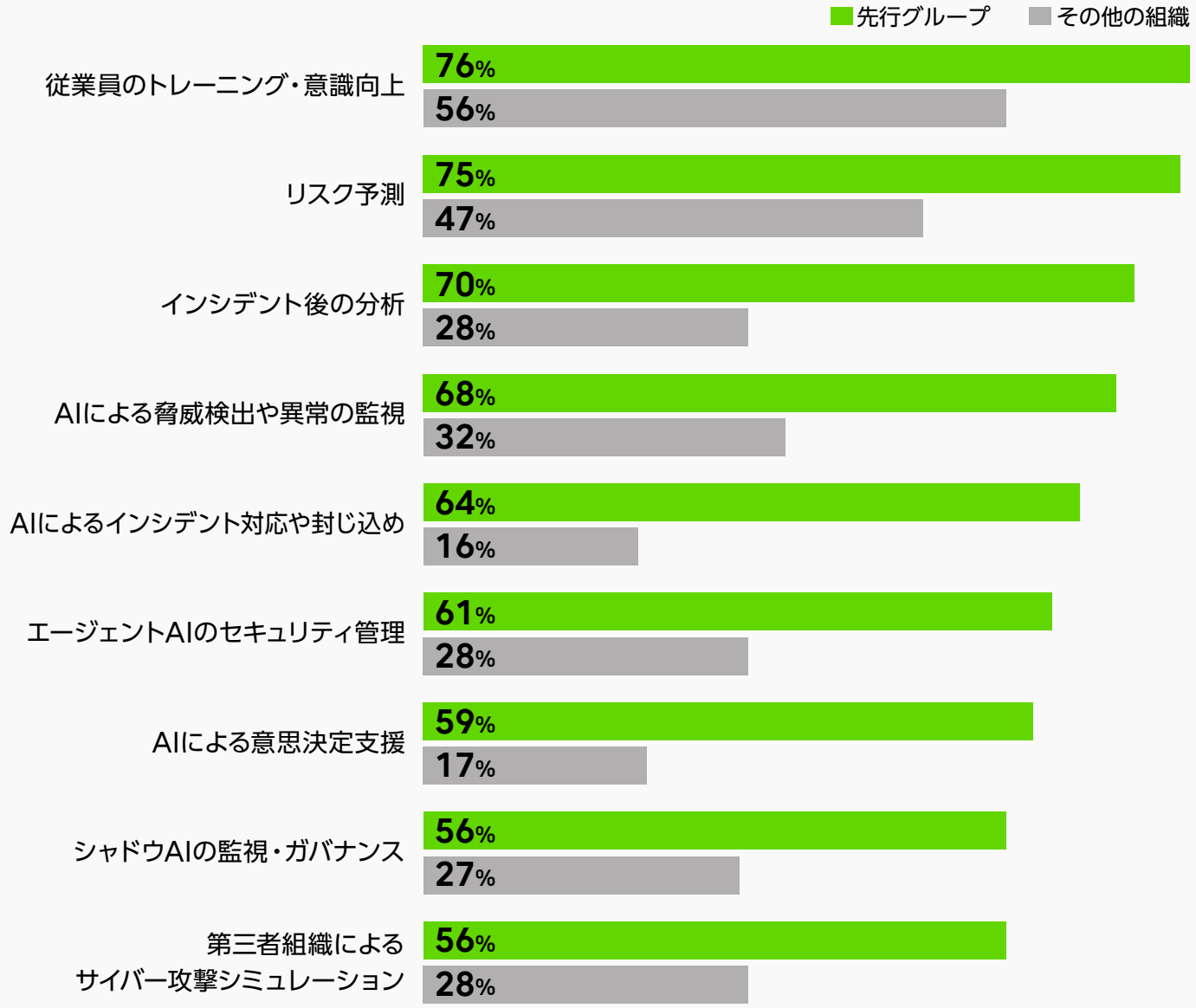
先行グループの多く（65%）は長期的な見通しで、レジリエンスの構築に注力しています。これに対し、そのほかの組織の68%が、差し迫った脅威や短期的なリスクの低減を優先すると答えています。どちらも重要ですが、場当たり的な対応に追われる組織は、対応が後手にまわってしまい、将来の大きな脅威に備え手を打つことが難しくなりがちです。

なぜ短期的な視点に偏ってしまうのでしょうか？ 調査を分析すると、より大きな成熟度の格差ともいえる違いが明らかになっています。

その他の組織の企業では、リスク予測や従業員研修といった理論上の計画や座学に大きく依存しています。このような取り組みは重要ですが、サイバー脅威が急速に変化している状況では実は不十分です。

先行グループはサイバーセキュリティの次の段階に進んでいる

Q：サイバーレジリエンスを強化するために、あなたの会社では以下のようなソリューションや取り組みをどのくらい活用していますか？
（頻繁に活用する・完全に組み込んでいる）



先行グループはこの点を認識しており、ベーシックな対応はもちろんのこと、検証と改善に注力しています。実環境でサイバー攻撃シミュレーションを実施し、頻繁にプロセスのストレステストを行っているのは半数以上（56%）です。

その一例が「ホワイトハット・ハッカー」演習です。これは、セキュリティの専門家がハッキングと同じ手法で（倫理的な問題はなく）システムの弱点を特定する訓練です。このシミュレーションは、経営層が攻撃者よりも先に脆弱性を特定し、レジリエンス戦略を検証するのに役立ちます。

AIの脅威はAIをもって制す

AIは間違いなくサイバーリスクを増幅させています。ただ、多くの経営層が見過ごしているのは、AIはまたサイバー犯罪から身を守る最も有用なツールでもあるということです。

この点についても、先行グループが優位に立っています。巧妙化するサイバー攻撃から守るためにAIは不可欠と答えたのは約10社中8社（79%）でした。その他の組織の企業では、わずか44%でした。

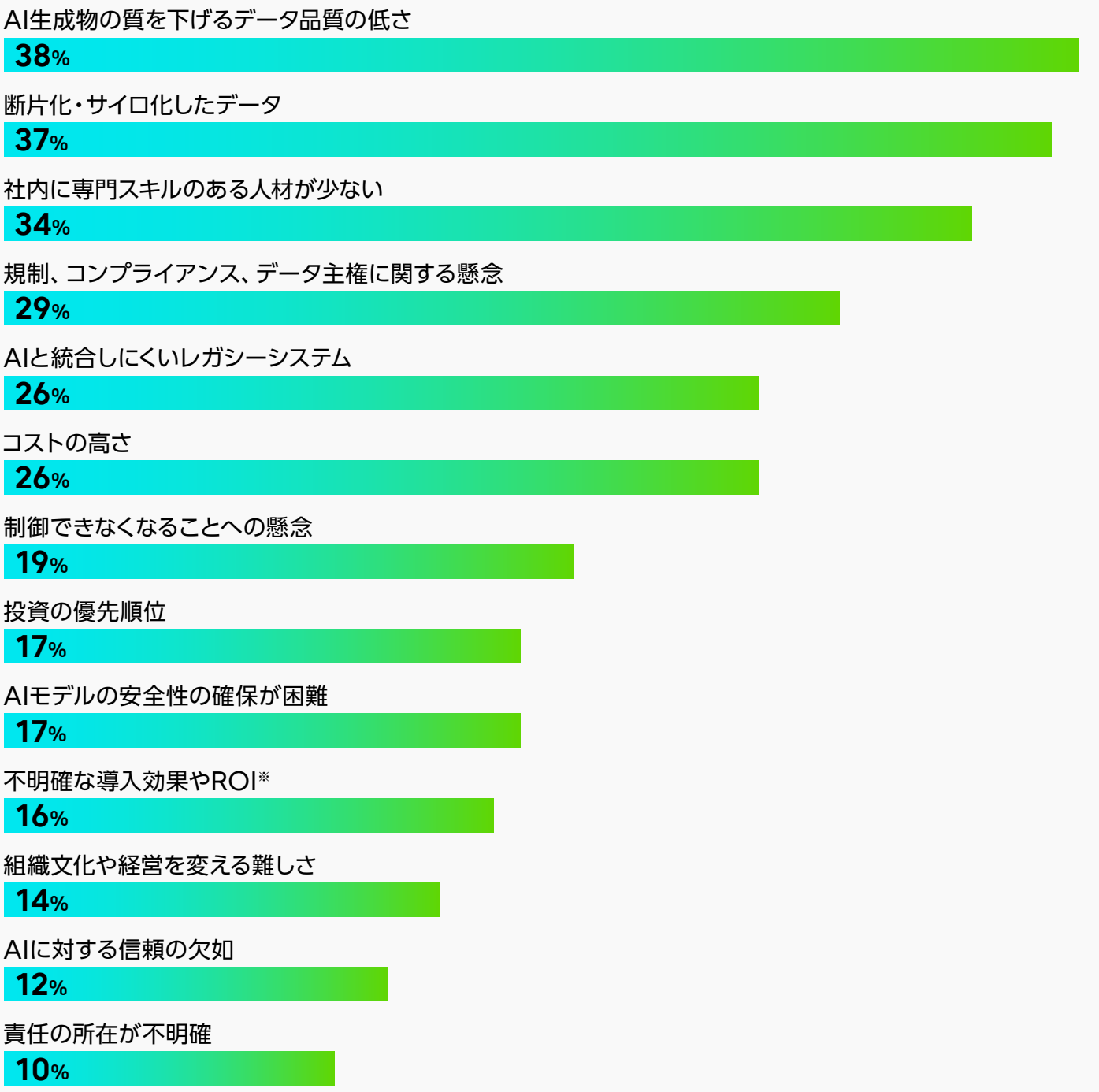
この認識は、それぞれの組織の戦略にも反映されています。先行するグループにおいては、AIで脅威や異常を検知する割合は、そのほかのグループと比べて2倍以上多くなっています。また、意思決定の支援にAIを利用する割合は3倍以上、インシデント対応や封じ込めにAIを利用する割合は、4倍以上多い割合となりました。つまり、AIツールによって、脅威をより早く特定し、迅速に対応し、常に備える体制ができているのです。

しかし、AIのポテンシャルをわかっている組織でも、壁に直面しています。調査では、AI導入におけるサイバーレジリエンスの最大の課題として、データ基盤と人材不足が浮かび上がりました。特に、品質の低いデータと断片化されたデータが問題です。続いて、社内の専門知識を持った人材の不足が挙げられています。

組織の準備が整っていなければ、たとえAIへ投資しても投資対効果（ROI）は期待できません。AIの潜在能力を引き出し、サイバーレジリエンスを向上させるためには、データのモダナイゼーションと人材研修が不可欠だといえるでしょう。

データ課題・人材不足がAI導入の障壁に

Q：あなたの組織のサイバーレジリエンス戦略において、AIを扱う上での最大の障壁は？



※ ROI：Return on Investment ＝投資した費用に対してどのくらい利益が出ているかを示す指標

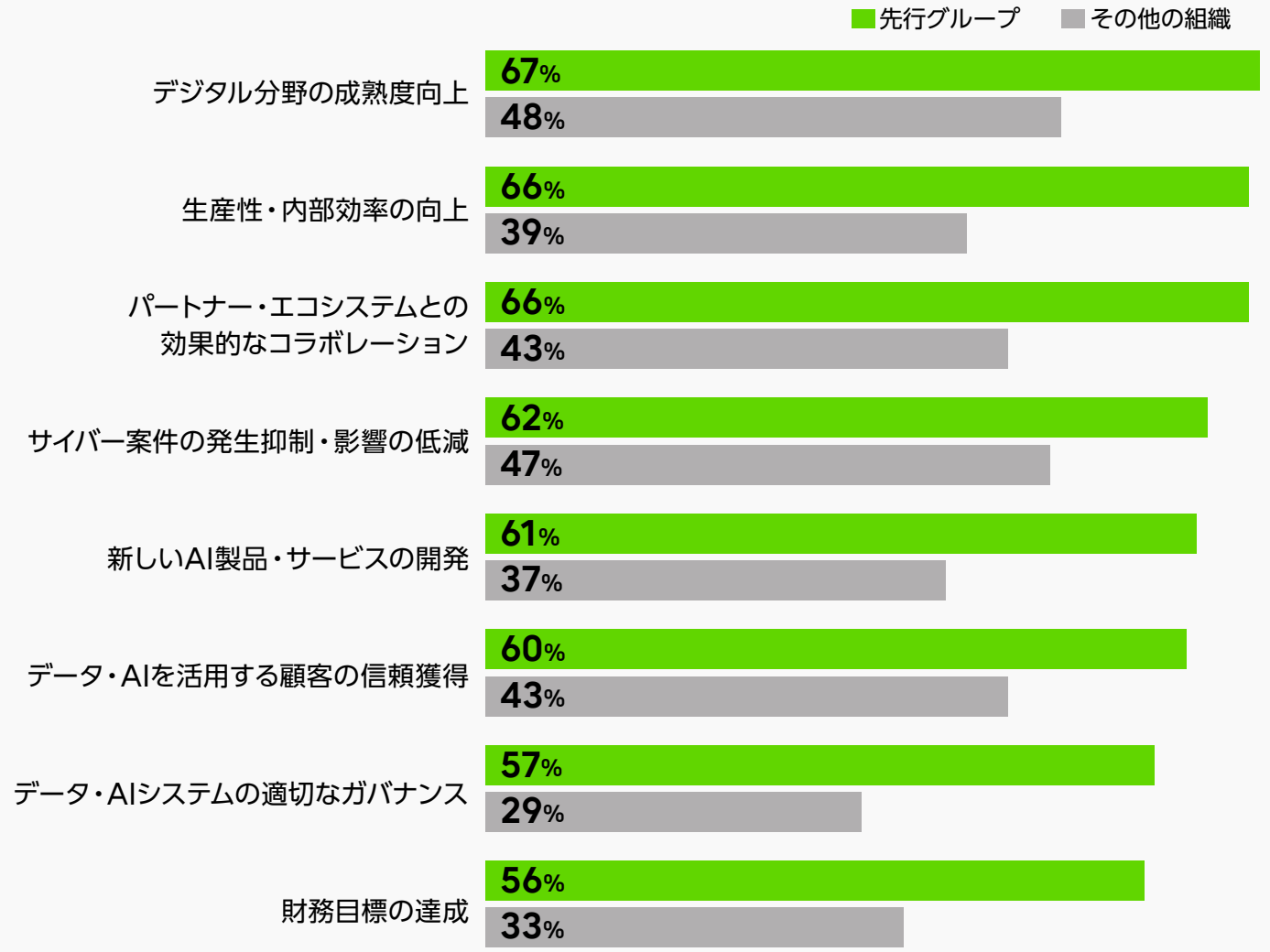
サイバーレジリエンスとビジネス成果との関係

実は、強固なサイバーレジリエンスを持つ組織では、すでに目に見える成果が表れています。セキュリティインシデントの発生頻度と影響を軽減できているのは、先行グループでは約10人中6人（62%）ですが、その他の組織では47%にとどまっています。

サイバーレジリエンスを強化するメリットは、セキュリティにとどまりません。

強固なサイバー耐性（レジリエンス）と業績は相関関係にある

Q：あなたの組織は以下の項目について、どのくらいの成果を上げていますか？（よい成果を上げている）



調査では、適切な対策、ガバナンス、管理体制を整備することで、組織がより迅速に、かつ自信を持ってイノベーションを推進できるようになっていることがうかがえます。

AIを活用した新製品・サービスの開発に成功した先行グループの割合は、10人中6人（61%）だったのに対し、その他の組織では37%にとどまっています。また、組織全体のデジタル成熟度を向上させたのは、先行グループでは67%だったのに対し、その他の組織では48%にとどまっています。

また、先行グループは、データやAIを活用しながら、顧客の信頼を得る力に優れています。これは顧客の獲得とビジネスの長期的な成功を支えています。また、財務目標の達成、生産性の向上、パートナーとの効果的な連携を示す値も、はるかに高くなっています。

この調査結果は、サイバーレジリエンスが、単なるリスク回避のためのツールではないことを示しています。つまり、ビジネスのパフォーマンスを向上させる手段でもあるといえるでしょう。

ビジネスのレジリエンスを強化する方法

今回の調査で特定された「先行する企業グループ」の存在は、AIによるイノベーションとサイバーレジリエンスの両立が可能であるだけでなく、互いに不可欠であることを示しています。

サイバーレジリエンスの確立に苦戦する組織でも、「先行する企業グループ」のリーダーになることは可能です。先行するグループとその他の組織との差は、事業の規模や業種ではなく、戦略で決まります。つまり、サイバーセキュリティへの取り組み方を変え、優先順位を見直すことで、組織が進む方向を変えることができるのです。

今回の調査の分析結果と、当社のサイバー戦略支援の経験から導き出した先進的な組織への道筋は以下の通りです：

1. 侵入を前提とした設計にし、防御だけを考えないこと

レジリエンスの高い組織は、サイバー攻撃による侵入は避けられないものだと考えています。こうした組織はシステムを「要塞」にする考え方を捨て、侵入を前提にして、システム、プロセス、ガバナンスなどの仕組みを設計しています。攻撃の検知、対応、そして迅速な復旧を重点に考えることで、経営層は防御が突破されても、業務の継続をはかることが可能になります。

2. レジリエンスをリーダーシップと企業カルチャーに浸透させること

サイバーレジリエンスは経営会議から始まります。IT部門だけが担当する技術の問題ではないと認識する必要があります。組織は、セキュリティ侵害は起きるものだという前提において、サイバーレジリエンスを企業文化に浸透させる必要があります。そうすることではじめて、経営層や一人ひとりの従業員が、いざというときに業務の継続と信頼の維持のために果たすべき役割を理解できるようになるでしょう。

3. 真に重要な資産を守り、実環境でシミュレーションすること

すべてを守ろうとする姿勢からは脱却すべきです。ミッションクリティカルな資産に絞り、リアルな攻撃シナリオを想定して対策を検証することです。そうすることで、業務への影響が最も大きい領域にリソースを集中できるようになります。これこそ、レジリエンス戦略を机上の計画ではなく、実際に機能させるために有効な方法です。

調査概要

本調査は、富士通がFT Longitude社に委託し、2026年2月に実施しました。

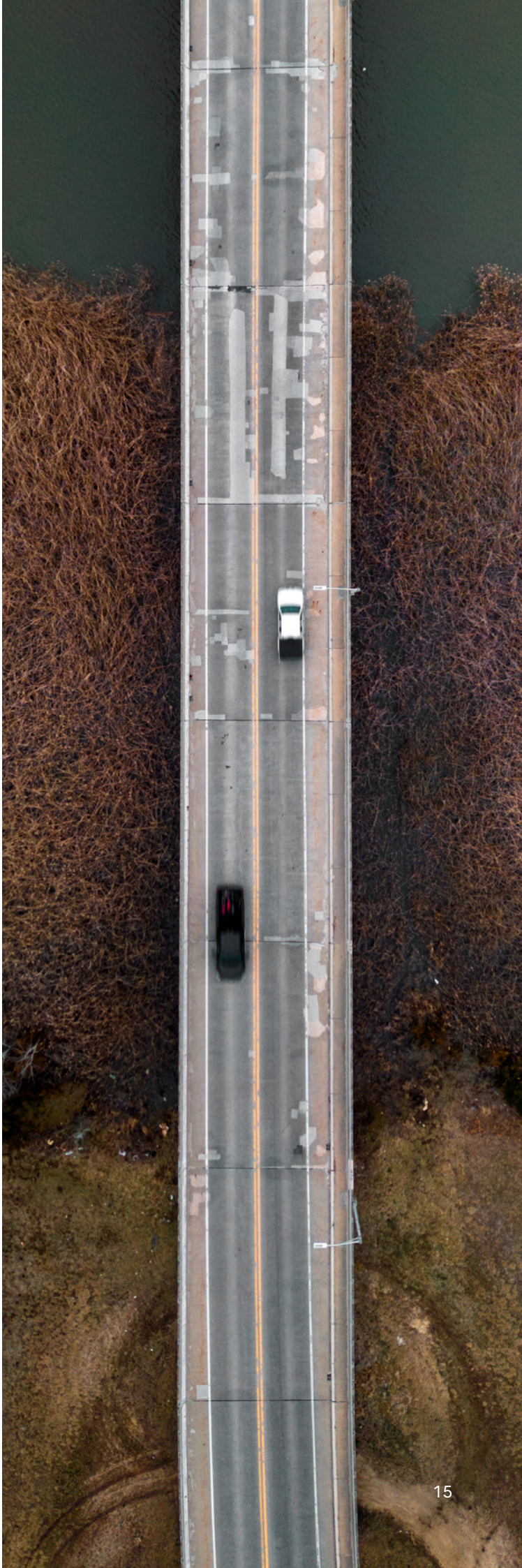
実施対象：オーストラリア、日本、英国、米国を拠点に活動する経営層をはじめ意思決定に関わるビジネスリーダー400人

職種：テクノロジー・IT、財務、企画戦略、
実行部門から同数

業種：金融サービス、製造、
エネルギー・資源・ユーティリティ、
物流・サプライチェーン、
ヘルスケア・ライフサイエンス、
小売・消費財、公共・政府・防衛セクター、
IT通信、プロフェッショナルサービス

経営規模：従業員1,000～4,999人（53%）、
5,000～49,999人（38%）、
50,000人以上（10%）

※本レポートの各種数値は整数にまるめた関係上、合計が100%にならない場合があります。



uvance
Wayfinders

Consulting by Fujitsu

FUJITSU