サイバーレジリエントCEO

サイバーセキュリティに自信のある CEO は サイバーセキュリティをいかに考えているか

Voices of Change

洞察から行動へ、特別な価値への道はここから始まる。

accenture

最高経営責任者（CEO）はサイバー攻撃がビジネスにもたらす脅威を十分に認識しています。

一方で、ほとんどの CEO がサイバー攻撃を回避したり、
被害を最小限に抑えたりする自社組織の能力が不十分だと感じています。

彼らは自社組織がサイバー攻撃に遭って初めて、サイバー攻撃への耐性を高める方法を学ぶのです。

こうしたサイバーセキュリティに対する保守的な考え方は、
サイバー攻撃のリスクと復旧コストを増大させる結果につながりかねません。

本調査によって、より良いサイバーセキュリティ対策の存在が明らかになりました。

サイバー攻撃のリスクを最小限に抑え、サイバーレジリエンスを
ビジネス変革の中心に据えるために CEO がとるべき5 つの行動を明らかにします。

執筆者

Paolo Dal Cin
シニア・マネジング・ディレクター
グローバル・リード
アクセンチュア セキュリティ

主に経営幹部と連携し、セキュリティ戦略、ビジネスレジリエンス、サイバーディフェンス、スレットインテリジェンス、マネージド・サービスに関するソリューションやサービスを推進。

Valerie Abend
シニア・マネジング・ディレクター
グローバル・サイバー・ストラテジー・リード
アクセンチュア セキュリティ

企業全体のセキュリティ、およびレジリエンス・プログラムをリード。サイバーリスクの管理について経営幹部、取締役会、規制当局、政策立案者に助言している。

Rachel Barton
シニア・マネジング・ディレクター
ヨーロッパ・ストラテジー・リード
アクセンチュア・ストラテジー

成長戦略を専門とし、C-suites や取締役会と協力して、大規模な変革を通じて持続的な成長を支援。

Yusof Seedat
ソートリーダーシップ・ディレクター
グローバル・リサーチ・リード
アクセンチュア セキュリティ

サイバーセキュリティの研究をリード。データ主導のソート・リーダーシップの作成に注力し、グローバル企業の戦略的意思決定と市場でのポジショニングを支援。

謝辞

サラ・バード、ガルギ・チャクラバーティ、アーリーン・リーマン、アイリーン・モイニハン、マナヴ・サクセナ、アン・ヴァンダー・ヒデ、アリッサ・ワーリー、クリスティン・ヤンナキスの各氏の本報告書への貢献を称えたい。

内容

エグゼクティブ・サマリー

サイバーセキュリティはビジネスの優先事項のひとつです。サイバーセキュリティによって円滑なビジネスの維持、組織のパフォーマンスを最適化し、顧客やサプライヤーとの関係性の担保が可能です。一方で、サイバーセキュリティを軽視した場合、組織は多くのリスクにさらされる可能性があります。

様々な技術の顕著な進化により、デジタルの脆弱性が浮き彫りになっています。生成AI（生成AI）や量子コンピューティングなどの先進技術、環境問題、消費者の嗜好の変化、サプライチェーンの混乱、地政学リスクなどが様々な要素が絡みあい、サイバーセキュリティにおけるレジリエンスは経営の最優先課題となっています。

一握りの組織のみが、新たな企業価値創出の道筋である Total Enterprise Reinvention によってディスラプションに対応しています。自社ビジネスの核となるデジタル基盤（デジタルコア）と継続的な変革のための企業文化・能力の醸成を行い、企業のあらゆる部分を変革しています。

こうした中、アクセンチュアは今日のサイバーセキュリティに強いリーダー像を深く理解するため、日本を含む世界の有力企業の CEO 1,000人を対象に調査をしました。調査の結果、CEO はサイバーセキュリティを十分に認識しており、96%がサイバーセキュリティ対策は組織の成長と安定に不可欠であると回答しています。一方、サイバー攻撃によるビジネスへの損害を回避または最小限に抑える十分な能力を有しているか、という点については74%が懸念を示しています。CEO の大多数が、自社の組織が真にサイバーレジリエントであるという自信が持てておらず、その自信のなさがサイバーセキュリティ投資の優先順位に表れています。

アクセンチュアは、サイバーセキュリティに関する知見に基づき、CEO が現在直面している3つの課題を特定しました：

サイバーセキュリティとビジネスの関係についての理解が不十分

サイバーセキュリティの恩恵を定量化することは困難です。CEO の半数以上が、サイバーセキュリティの導入コストはサイバー攻撃を受けた場合のコストよりもはるかに高いと回答していますが、実際には異なります。当然のことながら、理解が不十分であるがゆえに、十分な戦略策定ができていません。サイバーセキュリティの問題を議論するための取締役会を実施していると答えた CEO は、わずか15%に過ぎないという結果にも表れています。

サイバーセキュリティ・リスクとコンプライアンスの問題は異なる

サイバーセキュリティリスクは、バックオフィスの管理部門が対処すべきコンプライアンス上の問題とみなされています。CEO の約半数（44%）が、サイバーセキュリティをビジネスにおける戦略的課題として捉えておらず、継続的な監視ではなく単発的な介入で対処ができると回答しています。一方 CEO の60%が、「セキュリティ・バイ・デザイン」（サイバーセキュリティをビジネス戦略や特定のサービス、製品に最初から組み込む）を導入していないと回答しています。

日々急速に変化するビジネスに影響を及ぼすリスクに対応できていないリーダーたち

進化するサイバーの脅威や新たなセキュリティリスクを認知できておらず、サイバー攻撃に対処できなかった際の復旧コストをきちんと理解していると確信している CEO はわずか33%です。様々な変化をもたらしている生成AIを例に挙げてみましょう。もし安全性が担保されていなければ、組織はセキュリティ侵害のリスク増大、規制の不遵守、風評被害、競争優位性の持続困難といった数々の問題に直面するでしょう。ビジネスにおけるサイバーセキュリティが及ぼす影響範囲とその重要性を制限すると、CEO は新たなビジネス機会を逃しかねません。CEO がサイバーセキュリティの重要性を理解し、時間と労力を割いて取り組み始めるのは、サイバー攻撃を受けてからであることが多いです。サイバー犯罪が急激に増加している状況や、企業のレピュテーションやブランドへの潜在的な影響を考えると、このようなアプローチは危険です。

本調査と分析で、CEO が積極的かつ自信を持ってサイバーレジリエントになる方法を検証しています。

アクセンチュアは「サイバーレジリエントCEO 行動指標」（25個の先進的な実践活動をベンチマーク）を定めました。これにより企業のサイバーセキュリティレジリエンスを測定することが可能です。この指標を使用したところ、サイバーセキュリティのレジリエンスを主導している CEO は少数派（5%）であることがわかりました。

このグループ（アクセンチュアはサイバーレジリエントCEOと呼びます）は、人材、イノベーション、持続可能性、顧客など組織のあらゆる面でサイバーセキュリティを評価する広い視野を有しています。

サイバーレジリエントCEO は、セキュリティ侵害やコンプライアンス要件に頼ることなく、サイバーセキュリティのアプローチに積極的に取り組んでいます：

1. 変革の初期段階からサイバーレジリエンスをビジネス戦略に組み込む
2. サイバーセキュリティに関する説明責任を組織全体で共有
3. 組織の中核となるデジタルコアを保護
4. 組織の境界を超えてサイバーレジリエンスを拡大
5. 継続的にサイバーレジリエンスの向上を図り、時代の最先端を行く

このようなリーダーの企業は、他の企業よりも迅速にサイバー脅威を検知し、対応することができます。その結果、サイバー攻撃を受けた際の復旧コストは大幅に軽減され、財務実績も他の企業を大きく上回っています。本調査では CEO がとるべき、自組織のサイバーレジリエンスを評価し、強化するための実践的な行動について詳述します。

サイバー脅威の複雑さ

今日、デジタルは、継続的な人材プールへのアクセスや政策・経済における安定性と収益性に至るまで、あらゆるものの中核となっています。

しかし、急速に高まるサイバー脅威や、セキュリティが組織のデジタルコアに組み込まれていない場合にもたらされるリスクは、国家や企業の競争力を阻害する可能性があります。例えば、

- ウクライナ侵攻と地政学的な多極化は、多くの変化をもたらしています。特に、世界のサイバー犯罪に関するコストは年間10兆5000億ドルに達すると予想されています。2025年には、2015年の3兆ドル[1] から上昇し続けており、世界のサイバーセキュリティに関する支出は2026年に3000億ドルに達すると予測されています。[2]

- デジタルインフラとオペレーションのレジリエンスを確立するには、多くの業界で基本信念を再検討する必要があります。また、IoT やクラウドベースの人工知能（AI）サービスなどレジリエンスを確立するために重要な技術的要素も必要です。

- オペレーショナル・テクノロジー（運用・制御技術）や製品はサイバー攻撃に対してますます脆弱になっています。これらのサイバーフィジカルシステムの安全性を確保するには、より多くの時間とコスト、そしてより複雑なシステムの構築が必要となることが課題として認識されています。

- 生成AIのようなデジタル革新は、新たな複雑性をもたらす可能性が高いです。CEO の64％が、悪質なサイバー攻撃者は生成AIを利用して、高度で検知が困難な新たなサイバー攻撃を仕掛ける可能性があると回答しています。

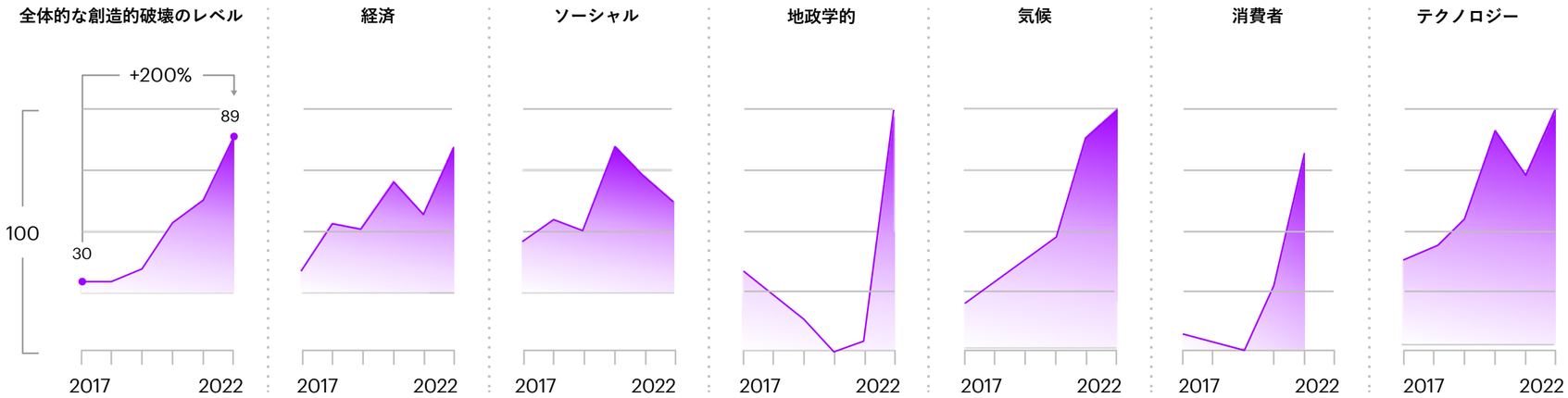
10年前、アクセンチュアはあらゆるビジネスがデジタル・ビジネスになることを予見しました。今日ではあらゆる組織がテクノロジー組織になっています。これらの企業は、クラウド、エッジコンピューティング、5G、そして現在では生成AIなど、デジタルテクノロジーを幅広く活用し、伝統的な価値観や生活習慣の劇的な変化がますます広がる中で変革に取り組んでいます。アクセンチュアの調査では、96%のCEOが、現在および将来の変革イニシアチブにおいてテクノロジーが重要な役割を果たすと回答しています。

しかし、このようなデジタルトランスフォーメーション（DX）と企業の再創造の取り組みによってもたらされる劇的な変化は、サイバー攻撃の新たな手段ももたらすことになり、サイバー攻撃が急増するだけでなく、ビジネス計画も根底から覆されつつあります。アクセンチュア・グローバル・ディスラプション・インデックス（図1）は、経済、社会、地政学、気候、消費者、テクノロジーの変化を網羅した複合指標です。創造的破壊のレベルは2017年から2022年にかけて200%増加したことが示されています。[3]

図1. アクセンチュア・グローバル・ディスラプション指数

創造的破壊のレベルは2017年から2022年にかけて200%増加

6つのサブコンポーネントの平均に基づく総合的な混乱度。



出典：アクセンチュア、2023年のトータル・エンタープライズ・リインベンション（企業全体の再創造）

組織のサイバー攻撃に対する脆弱性になりかねない Disruptive Force（破壊的要因）について CEO に尋ねたところ、次のような回答が得られました：

52%

テクノロジー・イノベーション

半数以上（52%）の CEO が、テクノロジー・イノベーションの加速がサイバー攻撃におけるトップリスクだと回答しました。生成AI や量子コンピューティングのような先進技術導入にあたっては、サイバーセキュリティの観点で信頼性とレジリエンスが関係してくると回答した割合は86%に及びます。

51%

サプライチェーンの混乱

CEO の約半数（51%）が、サプライチェーンを2番目に高い外部リスクだと捉えています。様々な場所に広がるグローバル企業のバリューチェーン上の脆弱性が浮き彫りになっています。

90%

環境の脆弱性

環境問題について、CEO の大多数（90%）が環境の変化や自社の取り組みが脆弱性と関連しうると認識しており、高い懸念が示された外部リスクのひとつです 。

CEO はまた、消費者嗜好の変化と地政学的な緊張を、サイバー脅威に影響を及ぼしうる外部要因のトップ10に挙げており、90%の CEO は2年以内に壊滅的なサイバー脅威が発生するとも予測しています。[4]

こうした要因がサイバー脅威の状況を一変させると同時に、サイバーセキュリティが、信頼と信用、そしてレジリエンスをもってビジネス価値を創出するためにいかに重要な手段であるかを示しています。

サイズと規模

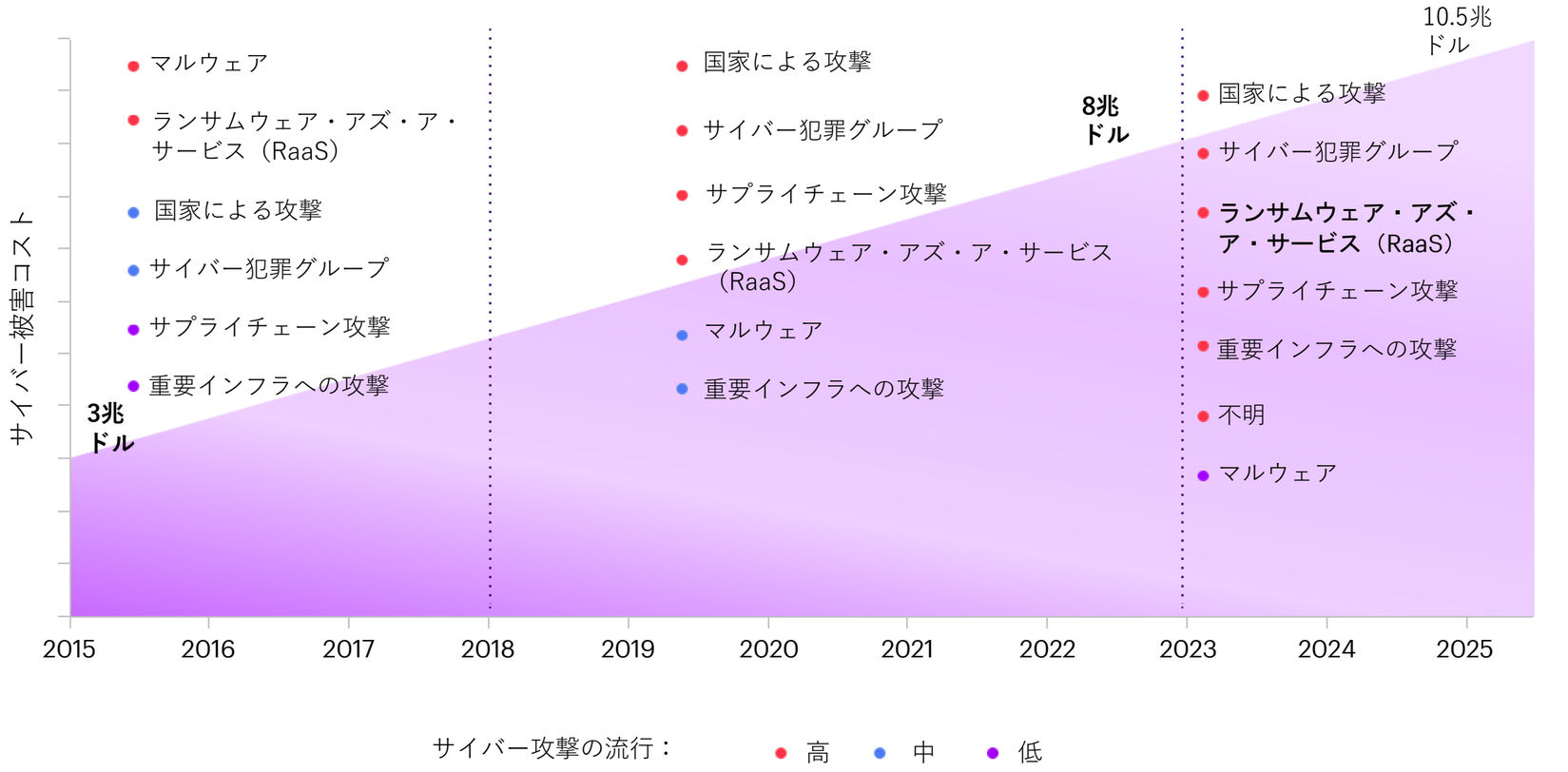
サイバー犯罪の被害額は、2015年の3兆ドルから2023年には8兆ドルに増加し、さらに今後も拡大すると予測されています。セキュリティー・ベンチャーズが発表した調査によれば、2025年には10兆5000億ドルにまで達すると予想されており、アメリカ、中国に次ぐ世界第3位の経済規模です。[5]

サイバー攻撃はますます複雑化し、頻発しています。世界規模で洗練されたオペレーションを実行している大企業でさえ一瞬で麻痺させることが可能です（図2）。

デンマークの海運・ロジスティクス企業マースクの例を見てみましょう。この「NotPetya」を使用した新種のランサムウェア攻撃は、サイバーセキュリティへの備えを強化するための警鐘となりました。この攻撃による同社のITシステムへの影響は即座に現れ、130カ国の600拠点で約5万台のコンピューターが被害を受けました。

ビジネスへの影響はその後も続きました。システムが使えず、港で船舶や重要な貨物が立ち往生したのです。損失額は3億ドルに上り、港湾インフラ、企業、消費者はもちろん世界的な出荷の中断によって9万人近い労働者に影響を及ぼしました。このランサムウェアの攻撃により、事業は20％縮小しました。[6]

図2. サイバー犯罪の被害コストと複雑性



出典：アクセンチュアリサーチ分析、セキュリティベンチャーズ

リスクと報酬

今、サイバーセキュリティ・リスクに対する CEO の注目が高まっています。サイバー攻撃で発生しうる金銭的損失、風評被害、業務上の混乱が認識されるようになり、危機感が高まり、考え方を変化させる原動力となっています。

CEO の96%がサイバーセキュリティの重要性を理解しており、サイバーセキュリティが組織の成長、安定性、競争力向上において重要な要素だと考えています。

大企業の決算説明会の記録を分析したところ、2017年から2022年にかけて、CEO がサイバーリスク、サイバーセキュリティ、サイバー攻撃という言葉について言及する回数が6倍に増加していることがわかりました。[7] さらに、CEO の90%が、サイバーセキュリティを自社の製品やサービスの差別化要因として考え、顧客の信頼構築に役立てていると回答しています。

96%

の CEO は、サイバーセキュリティの重要性を理解しており、サイバーセキュリティが組織の成長、安定、競争力向上において重要な要素だと考えています。

リスクに備える

サイバー脅威の状況が急速に変化する中、知識は力です。しかし、ビジネスにおけるサイバーセキュリティの価値に対する CEO の意識の高まりと新たに出現するサイバー犯罪者についての理解との間のギャップは広がっています。結果的に、サイバー攻撃を回避または軽減することに対してCEOの自信が低下しています。

端的に言えば、企業はまだサイバーセキュリティに強くはないし、サイバーに強いとは言うことはできません。最高経営責任者（CEO）は、サイバーレジリエンスをどのように測定し、自社のビジネスが正しい軌道にあることを確認すればよいのか分かっていません。しかし、デジタル世界ではあらゆるものがつながっているため、特にデジタルの露出と脆弱性が拡大するにつれて、その安全確保は不可欠です。

進化するサイバー脅威の状況について深く理解していると確信している CEO はわずか33%に過ぎず、多くの CEO はリスクにどのように対処すべきかわからずにいることが明らかになりました。またこれに伴って、74%の CEO は、サイバー攻撃によるビジネスへの損害を回避または最小限に抑える組織の能力に懸念を抱いています。本調査に回答した CEO の約60%は、一般的なサイバーレジリエンスを実践していると回答しましたが、それだけでは十分でないとも認識しています。さらに約半数が、サイバーセキュリティを継続的に注視すべき重要なビジネスイネーブラーとして考えるのではなく、サイバーセキュリティには単発的な介入が必要だと考えています。

このような消極的な考え方は、CEO がサイバーセキュリティに取り組むために投資する時間が限られていることにも表れています。また、サイバーセキュリティは定量化しにくいため、見過ごされがちです。CEO の54%は、サイバーセキュリティの導入コストはサイバー攻撃を受けた際に発生する復旧コストよりもはるかに高いと感じています。しかし、本調査によると、サイバーセキュリティへ投資を優先している企業は、サイバーセキュリティ被害時のコストを、そうでない企業に比べて最大3倍低く抑えています。

33%
進化するサイバー脅威の状況について深く理解していると確信しているCEOの割合

74%
サイバー攻撃によるビジネス損失を回避または最小化するための組織の能力に懸念を抱いている CEO の割合

60%
一般的なサイバーレジリエンスを実践しているが、それだけでは十分でないと認識している CEO の割合

15%
サイバーセキュリティ問題を議論するための取締役会を設けている CEO の割合

54%
サイバーセキュリティの導入コストは、サイバー攻撃からの復旧コストよりもはるかに高いと感じている CEO の割合

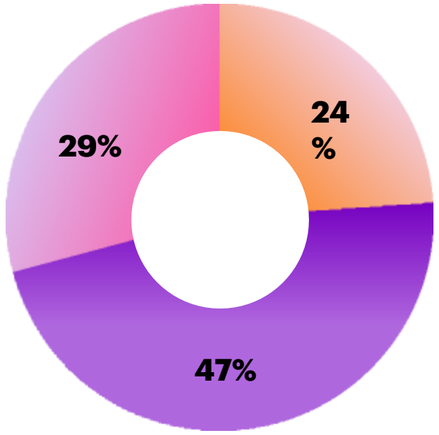
結果、多くのCEOはサイバーセキュリティをインシデントやコンプライアンスに左右される技術的な要素として扱う傾向があります

CEO の76%は、重要な機能に対してのみセキュリティ対策を実施するか、変革が完了した後、または脆弱性が検出された場合にのみセキュリティ対策を実施すると回答しています。大多数（91%）の CEO は、サイバーセキュリティは CIO または CISO の責任である技術的要素であると回答し、95%はコンプライアンスがサイバーセキュリティ戦略の主要な推進要因の1つであると回答しました。(図3)

図 3. CEO は、サイバーセキュリティを、インシデントとコンプライアンスに左右されるサイロ化された技術要素として扱っている。

10人に7人

CEO が、重要な機能に対してセキュリ ティ管理を実施するか、あるいは、変革が完了し、脆弱性が検出された後にセキュリティ対策を実施する



すべての変革イニシアチブにセキュリティ管理策を変革の初期段階から組み込む

スピードとリスク管理のバランスを取りながら、重要な機能のみにセキュリティ対策を実施する

変革のスピードを優先し、脆弱性が検出された場合にのみ、変革が完了した後にセキュリティを導入する

~50%

サイバーセキュリティには継続的な注意ではなく、単発的な介入が必要であると回答している CEO の割合

91%

サイバーセキュリティは**技術的な要素**であり、効率的に推進するために CIO や CISO が持つ専門知識に依存していると回答している CEO の割合

95%

コンプライアンスによって戦略的なサイバーセキュリティが推進され、組織が業界基準や各種規制要件を遵守していると回答している CEO の割合

出典：2023年アクセンチュアサイバーレジリエントCEO調査（n=1,000）

残念なことに、CEOが積極的に時間とリソースを投資し、CISOやテクノロジー部門を超えて期待を拡大するのは、重大なサイバーインシデントを経験した後であることが多いです。

2021年5月に発生したコロニアル・パイプラインへのサイバー攻撃は、多くの CEO が変化に対応する能力に不安を抱えたまま、サイバーセキュリティにおける脆弱性に対する考えの大転換を求められていることを物語っています。この攻撃は、同社の経営を混乱させただけでなく、米国南東部への燃料供給にも支障をきたし、パニック買いやガソリン価格の高騰を招きました。攻撃者は2時間のうちに100ギガバイトのデータを盗みました。彼らは請求や会計システムを含む同社のITにランサムウェアを感染させました。

これを受けてコロニアル・パイプライン社は、ランサムウェアによる被害拡大を防ぐためにパイプラインを停止した結果、市場での供給不足を招きました。同 CEO は上院公聴会で、同社はランサムウェア攻撃を防止するための対策を講じていなかったことを認めました。攻撃後、同社はセキュリティチームを刷新し、初の最高情報セキュリティ責任者（CISO）を採用し、サイバーセキュリティ・プログラムの再構築に着手しました。[8]

サイバーレジリエントCEO
に必要な5つの行動

CEO にとって、サイバーレジリエンスにおけるギャップを埋めることはビジネスの優先事項です。

サイバーレジリエンスを測定可能な 25個の実践活動をもとに構成されるアクセンチュアの「サイバーレジリエントCEO 行動指標」（「調査について」を参照）では、サイバーセキュリティを優先する CEOが、自信、信頼、レジリエンスをもってビジネス価値を高めるために実施している実践活動を特定しました。

私たちは、これらの実践活動を5つの行動に分類しました：

01 ビジネス変革の初期段階からサイバーレジリエンスをその中心に据える。

02 組織全体でサイバーセキュリティに関する説明責任を共有する。

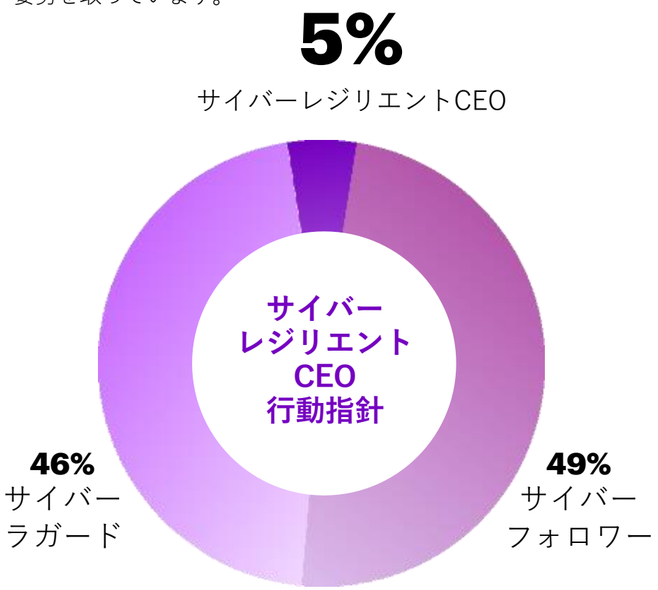
03 組織の中核となるデジタルコアを保護する。

04 組織の境界を越えてサイバーレジリエンスを拡大する。

05 サイバー脅威における時代の最先端を行くため、継続的にサイバーレジリエンスの向上を図る。

この指標を用いたところ、サイバーレジリエントなリーダーである CEO はわずか5%であることがわかりました。このような「サイバーレジリエントCEO」は、セキュリティ侵害やコンプライアンス期限を待たずに、常に3つ以上の行動を取っています。

サイバーレジリエントCEO に次ぐのが「サイバーフォロワー」です。全体の49%を占めるこの種の CEO は、5つの行動のうち少なくとも2つを確実に実行し、残りの行動からいくつか実践活動を採用しています。残りの46%を占める「サイバーラガード」は、一貫していずれの行動もとらず、基本的に、保守的な姿勢を取っています。



サイバーレジリエントCEOとは？

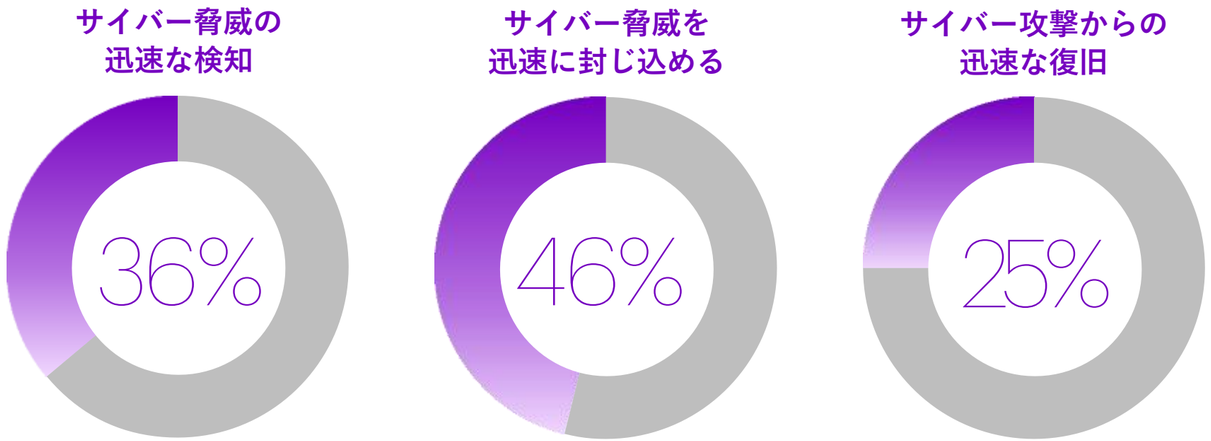
本調査によると、サイバーレジリエントCEOは次のように定義されます：

自信を持って行動する

サイバーフォロワーとサイバーラガードのCEOが24%だったのに比べて、サイバーレジリエントCEOのうち60%が自社の組織がサイバーレジリエントであると回答しています。これは、サイバー脅威をより迅速に検知し、封じ込め、復旧する能力（図4）や、サイバー攻撃を受けた際の復旧コストはサイバーフォロワーに比べてほぼ2倍、サイバーラガードに比べて3倍低いという事実によって裏付けられています。

2022年は、2021年よりもサイバー攻撃未遂件数が25%増加しているにもかかわらず、サイバーレジリエントCEOが率いる企業へのサイバー攻撃成功率（攻撃未遂件数に占める攻撃成功件数の割合）は、サイバーラガードCEOが率いる企業（14%低い）やサイバーフォロワーCEOが率いる企業（6%低い）に比べて低いこともわかっています。

図4. サイバーレジリエントCEOは行動を起こしています



出典：2023年アクセンチュアサイバーレジリエントCEO調査（n=1,000）
パーセントは、サイバーレジリエントCEOとサイバーラガードCEOの割合を示す。

変化を受け入れる

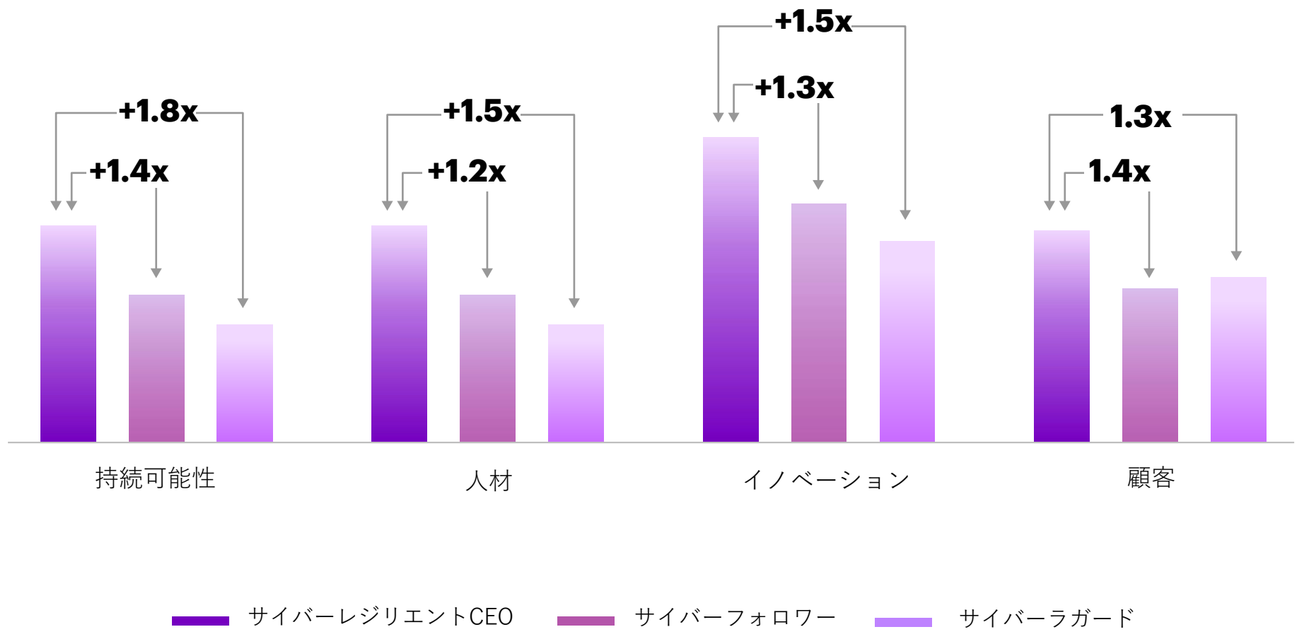
本調査により明らかになったサイバーレジリエントCEO はすべからく、全社的な変革を実現するための戦略を採用し、企業機能や事業部門を変革することで、機能や部門の枠を超えた能力を構築し、新たなパフォーマンスにおけるフロンティアを開拓しています。また、サイバーセキュリティを俯瞰して捉え、変革の初期段階からサイバーセキュリティを戦略に組み込んでいます。

総合的に評価する

サイバーレジリエントCEO は、自社のサイバーセキュリティ態勢を検討する際に、持続可能性、人材、イノベーション、顧客など、非財務的な指標を通じ、他の企業に比べて最大1.8倍も幅広く、組織のあらゆる側面でサイバーセキュリティを評価する視野を有しています（図5）。

図 5. サイバーレジリエントCEO は、サイバーセキュリティに対して組織のあらゆる側面からアプローチします

360˚サイバーアウェアネススコアは、CEOが非財務指標にわたってサイバーセキュリティをどの程度認識し、関連付けているかを評価するものです。



出典：2023年アクセンチュア サイバーレジリエントCEO 調査（n=1,000）

こうしたアプローチの結果、サイバーレジリエントCEOは、平均して他の企業よりも高いビジネス価値の創出を実現しています。

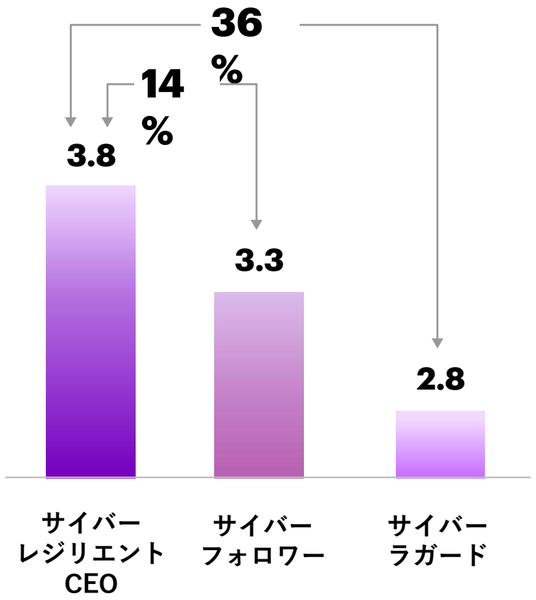
図6. サイバーレジリエントCEO は他社を財務面で上回ります

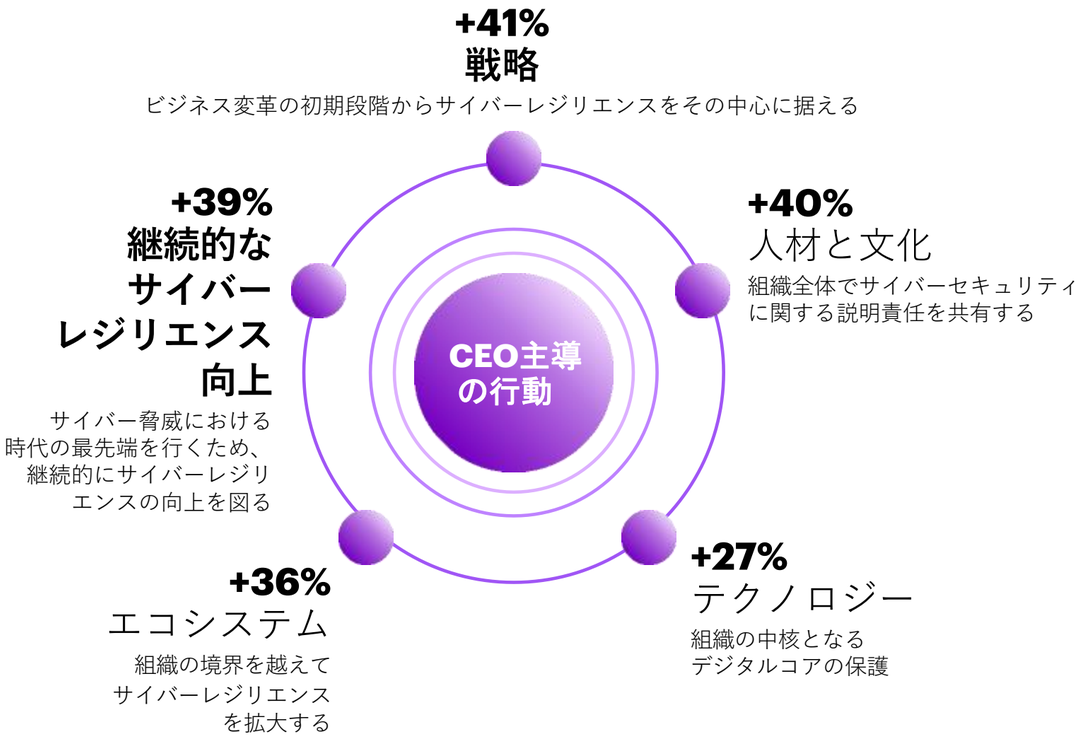
+16%	増収率の向上
+21%	さらなるコスト削減の改善
+19%	バランスシートの健全化

出典：2023年アクセンチュア サイバーレジリエントCEO 調査（n=1,000）

全体として、サイバーレジリエントCEOは、「サイバーレジリエントCEO行動指標」における5つの行動（戦略、人材と文化、テクノロジー、エコシステム、継続的なサイバーレジリエンス向上）のそれぞれにおいて、サイバーフォロワーを14％ポイント、サイバーラガードを36％ポイント上回っています（図7）。

図 7. サイバーレジリエントCEOは、「サイバーレジリエントCEO 行動指標」で他社を上回る。





サイバーレジリエントCEO vs サイバーラガードCEO

出典：2023年アクセンチュア サイバーレジリエントCEO調査（n=1,000）

サイバーレジリエントCEOハンドブック

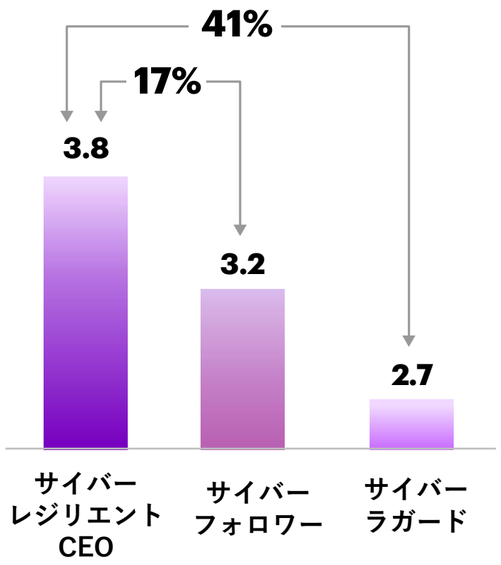
5つの行動をすべて実践することで、CEO はサイバーセキュリティをIT部門だけが担当する単なる技術的機能としてではなく、経営層から取締役会にまでの報告と説明責任を果たすプロセスを確立し、組織全体の優先事項へと昇格させることができます。

ビジネス変革の初期段階からサイバーレジリエンスをその中心に据える

サイバーレジリエントな組織にとって、ビジネス戦略に組み込まれたサイバーセキュリティに対する大胆なビジョンは、競争上の差別化要因として重要です。

「サイバーレジリエントCEO 行動指標」の「戦略」の側面では、サイバーレジリエントCEO は他の CEO を圧倒します。彼らは、サイバーレジリエンスをビジネス変革の初期段階からその中心に据えており、3.8 ポイントの優位性を獲得しています。これは、サイバーラガード企業に対して 41%、サイバーフォロワー企業に対しては 17%の優位性を示すという特筆すべきものです。サイバーレジリエンスを戦略的アプローチに組み込むことで、サイバーレジリエント CEO は、進化するサイバー脅威から組織を守り、強固なセキュリティ体制を維持するというコミットメントを示しています（図 8）。

図 8. サイバーレジリエントCEO は、サイバーレジリエンスをビジネス変革に組み込んでいる



出典：2023年アクセンチュア サイバーレジリエントCEO 調査（n=1,000）

実践的なステップ：戦略

1. サイバーセキュリティを新たな価値を見出すための戦略的なビジネスイネーブラーとして考える。

サイバーレジリエンスを変革の初期段階から戦略的なイネーブラーとして扱うことで、サイバーレジリエンスをビジネスの基盤に組み込むことができます。これには、CEO がサイバーリスクを評価するためのフレームワークを承認・ 支持し、戦略的なビジネス上の意思決定や投資に活用することを義務付けることが必要です。ビジネスリーダーが強力なビジネスケースを持ち、サイバーリスクマネジメントが理想とするビジネスを実現する理由と方法を理解すれば、最初から強力な実践活動を取れる可能性が高くなります。サイバーレジリエントCEO（約70%、サイバーラガードCEO の38%）は、この先進的な実践活動を推進する上で際立った存在です。その潜在的価値には説得力があります。アクセンチュアの調査によると、サイバーセキュリティとビジネス目標の相関性が高い企業は、収益、市場シェア、顧客満足度、信頼性、および従業員の生産性向上を実現する可能性が そうでない企業と比較して18% 高いことが明らかになっています。

2. サイバーパフォーマンスを財務パフォーマンスと同等に考え、エグゼクティブの個人的な業績成果と連動させる。

戦略立案から予算編成に至る意思決定プロセスの不可欠な要素としてサイバーセキュリティを導入することで、効果的なリスクマネジメントとリスク軽減戦略を実現できます。これにより、機密データの保護、業務の継続性の維持、顧客の信頼の保護に対する組織のコミットメントを示すことができます。その結果、進化するサイバー脅威に直面した際のレジリエンスを高めることができます。サイバーラガードCEO が20%であるのに対し、サイバーラガードCEO の60%は、サイバーパフォーマンスを財務パフォーマンスと同じ方法で管理しています。経営幹部がビジネス戦略や意思決定にサイバーセキュリティをどのように組み込み、関与させるかを検討してください。ただし、会社のリスク選好度に沿った方針と基準を満たしていない場合、リスクの受容度と深刻さについて責任を負う必要があります。

3. 重要なあらゆるイニシアチブの寿命を見極め、サイバーリスク評価を見直す。

新製品の発売、サービスの拡大、企業買収、新拠点での事業展開など、サイバーリスクマネジメントを継続的に統合することができれば、企業はビジネス戦略におけるサイバーセキュリティの潜在的な複雑性を定量化することができ、対処することができます。CEO は明確な目標を設定した上で、戦略立案から実施、またそのイニシアチブが存在する期間において、いつ、どこで、どのようにセキュリティに関する相談があり、リスクが特定され、解決策が提供されたかについて報告を求めるべきです。サイバーレジリエントCEO の70%近くがこうした行動を取っているのに対して、サイバーラガードCEO ではわずか41%です。

実践的なステップ：戦略

4. 組織的・技術的な複雑さを軽減する

組織や技術の複雑さがサイバーリスクを引き起こすこともあります。複雑な組織階層、意思決定プロセス、業務ワークフローを簡素化することで、CEO はリスクのみならず潜在的なサイバー攻撃に対する対応を改善することができ、サイバーセキュリティ対策の可視性と制御性を向上させることができます。これによりCISOはサイバー脅威をより迅速かつ高い信頼度で検知し、対応することができ、またリスクを緩和することができます。このような構造的な簡素化により、各種調整の改善、意思決定の迅速化、セキュリティ対策の効果的な実施が可能になり、最終的にはサイバーレジデンス全体が強化されます。

5. すべてのステークホルダーに対して透明性をもって接する。

サイバーレジリエントCEO の3分の2以上が、未遂も含めたサイバー攻撃とそれに対応する行動をステークホルダーにすべて開示するほど、透明性を重要視しています。これには、顧客、サプライヤー、規制当局など、企業のサイバーセキュリティ施策や対策、セキュリティ態勢に関心を持つ人々など、サイバー攻撃によって影響を受ける可能性のある社内外のステークホルダーも含まれます。サイバーインシデントに関する情報をオープンにし共有することで、企業は透明性へのコミットメントと、ステークホルダーとの強固な信頼関係を維持しながらサイバー脅威に取り組む積極的な取り組みを社内外に示すことができます。

さらに、企業はステークホルダーとの相互依存関係を強化しているため、透明性をもって彼らを主導し、また、エコシステムパートナーにも同様に期待値設定することで、サイバーレジリエンスを向上させることができるでしょう。米国証券取引委員会（SEC）がサイバーリスク管理の透明性を向上させるために策定した最新の規制は、コンプライアンスに基づく期待に応えるためだけでなく、エコシステム全体におけるステークホルダーのエンゲージメントとサイバーレジリエンスを向上させるためにも、情報共有の拡大を支援するための行動を呼びかけるものです。

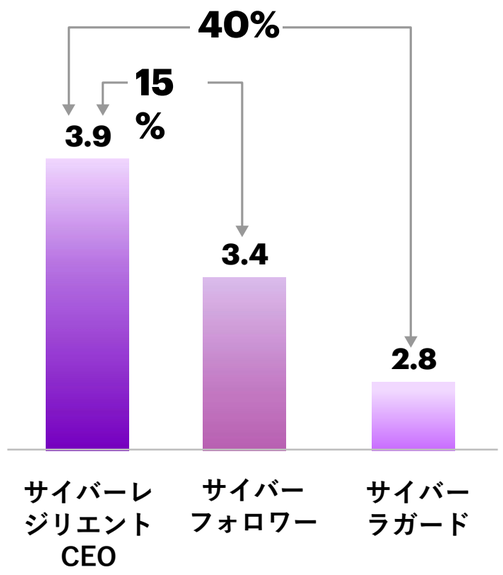
組織全体でサイバーセキュリティに関する説明責任を共有する

サイバーレジリエントCEO は、セキュリティ重視の企業文化の醸成には、セキュリティに対する非常に高い意識が必要であり、組織内のあらゆる人を巻き込む必要があることを認識しています。

「サイバーレジリエントCEO 行動指標」の「**人材と文化**」の側面では、CEO のパフォーマンスは、組織全体でサイバーセキュリティの説明責任を共有するための行動を促進するというセキュリティ慣行を採用しているか否かに基づいて評価されます。

サイバーレジリエントCEOのスコアは3.9 ポイントで、サイバーラガード 40%、サイバーフォロワー企業を15% 上回っています。サイバーレジリエントCEOは、企業のあらゆる部署、役職の従業員を巻き込んだサイバーセキュリティ文化の確立に積極的であることがわかっています。（図 9）

図 9. サイバーレジリエントCEO は、サイバーセキュリティ文化の確立により積極的である



出典：2023年アクセンチュア サイバーレジリエントCEO 調査（n=1,000）

実践的なステップ：人材と文化

1. 経営層全体に説明責任を共有する文化を浸透させる。

サイバーセキュリティを、安全性を担保しながらイノベーションを実現する競争上の差別化要因として捉えるようビジネスリーダーを鼓舞するため、説明責任を共有する文化を醸成しましょう。サイバーレジリエント CEO の3分の2が、CISO とより強固な関係を築き、他のリーダーを励まし、模範を示していると回答しています。説明責任を果たすには、CEO が経営層とそのリーダーシップ・チームのインセンティブを調整する必要があります。例えば、テクノロジー・リーダーシップに対する現在のインセンティブは、ほとんどの場合、アップグレードのスピードや新しいテクノロジーの導入、情報漏洩につながりかねない脆弱性を排除するためのセキュリティインセンティブに重きが置かれています。しかし、ビジネス上のインセンティブを共有することで、リーダーシップチームは説明責任を共有し、強化されたリスク管理を実践しながら、ペースを合わせて行動することができます。

サイバーレジリエントCEO のほぼ70%が説明責任の共有を採用しているのに対し、サイバーラガードCEO は37%にとどまります。CEO は、インセンティブと説明責任の両方を用いて、リーダーシップチーム内にサイバーセキュリティに関する説明責任を共有する文化を浸透させる必要があります。

これには、具体的な役割に基づく 経営層やリーダーシップの説明責任の測定、およびこれらの説明責任をサポートするための組織の権限付与が含まれます。例えば、CFO/COO について考えてみましょう。CFO/COO は、サイバーセキュリティインシデントの財務上の重要性を判断し、報告するためのプレイブックとプロセスを管理する必要があります。そのためには、取引量やビジネス機会損失への影響を熟知しているビジネス責任者や、アプリケーション、インフラ、プロセスの具体的な相互依存関係を把握している IT部門のリーダーシップなど、組織内の他リーダーからの洞察が必要です。同様にCHRO は、競争の激しい市場においてサイバー人材の採用とスキルアップを主導し、サイバーセキュリティの人的リスク要因に対処するセキュリティと意識向上のアプローチを組織が継続的に実施できるようにするためのパートナーとしての役割を担う必要があります。経営層とCISO の関係を強化することは不可欠であるが、CEO は、共通のアカウンタビリティによってサイバーレジリエントな成果をもたらすことを確認する必要があります。

2. 企業全体でサイバーセキュリティを最優先する文化を築く

CEO は、企業内のあらゆる階層でサイバーセキュリティに精通した行動の重要性を強調することで、サイバーセキュリティ・ファーストの文化を構築する上で重要な役割を果たすことができます。このようにCEO は、サイバーセキュリティの重要性について発言し、個人的な知識を深めるために努めていることを示すことで、模範となる必要があります。

また、CEO は、従業員に対して規範を示すだけでなく、経営層の各メンバーにまで十分に浸透させるためにサイバーリスク管理における透明性を確保し、サイバーリスク管理に対する説明責任を明確にする必要があります。注目すべきは、サイバーレジリエント CEO は、サイバーラガード CEO に比べて、このようなサイバーセキュリティ・ファーストの文化を積極的に醸成する傾向が62%も高いということです。こうした傾向が、従業員の給与算出からサプライチェーン構築、顧客との信頼関係構築に至るまで、企業機能や業務全体に安全なデジタル習慣の浸透につながっています。

実践的なステップ：人材と文化

3. イノベーションとレジリエンス推進のための行動喚起を先導する。

イノベーションはかつてないほど私たちの身近な存在になりました。AI、特に生成AIの普及は、サイバーセキュリティ上の課題だけでなく、組織がセキュリティ・プロセスを最適化・自動化する大きな機会をもたらします。CISO と協力して、生成AIのリスクとユースケースの両方を積極的に検討しましょう。生成AIの力を活用することで、全社的に仕事量を効果的に管理し、人件費比率が高くなる労働集約型のタスクを排除することができ、サイバー攻撃対策を強化することができます。サイバーレジリエントCEOは、サイバー攻撃対策のための生成AIの主な用途として、サイバー脅威の自動検知、サイバー攻撃時のシミュレーション・シナリオ、手作業によるセキュリティ・タスクの増強を挙げています。サイバーレジリエントCEOの半数以上が、CISOと緊密に連携して生成AI のリスクを評価・管理し、テクノロジーの安全かつ効果的な利用を確保しています。

例えば、アクセンチュアはインテリジェント・アプリケーション・セキュリティ・プラットフォームを通じて AI による自動化を導入しています。主要な商用スキャニング・ツールと AI の両方を大規模な脆弱性の特定と検査、そしてその減少のために活用し、アプリケーション・チームは数千時間の短縮に成功し、リスク削減も改善することができました。

4. セキュリティ人材のギャップ是正に向けた取り組みを支援する。

採用活動と並行して人材育成に投資することで、増大するセキュリティ人材のギャップを埋めることができます。そして、自動化、または生成AI によって拡張できる職務を特定しましょう。好奇心、クリティカルシンキング、問題解決能力などの特性を備えた人材採用するとともに、既存のスキルギャップを是正するためのトレーニングを提供することで、”人材の消費者” から “人材の創造者”になることができます。サイバーレジリエントCEO の約64%が、今後3年間にサイバーセキュリティ人材のスキルアップとリスキリングへの投資を増やす予定であると回答しているのに対し、サイバーラガードCEO ではわずか38%にとどまっています。

5. 重要度の高いセキュリティ分野にはCaaS（Cybersecurity-as-a-Service）を採用する。

サイバーレジリエントCEO の60%近くが、この戦略を優先的に実行しています。CaaS は、コスト削減、ベンダーの統合、人材格差への対応といったメリットをもたらすというのが大方の意見でした。

例えば、ある北米の小売チェーンが独立系上場企業になった際、IT業務の見直しが必要になりました。アクセンチュアは、CaaS を導入して小売業者の情報セキュリティ・チームをサポートするよう依頼され、当初はサイバー脅威インテリジェンスやセキュリティ・オペレーション・センター（SOC）など、同社のセキュリティ業務運営を支援していました。現在、アクセンチュアは、データ保護、アイデンティティ管理、ネットワーク・セキュリティ、脆弱性管理、セキュリティ意識向上およびリスク管理をサービスとして提供し、変革の初期段階から安全性を確保することで、同小売企業のサイバーレジリエンスとビジネス成果の向上を実現しています。

組織の中核となるデジタルコアを保護する

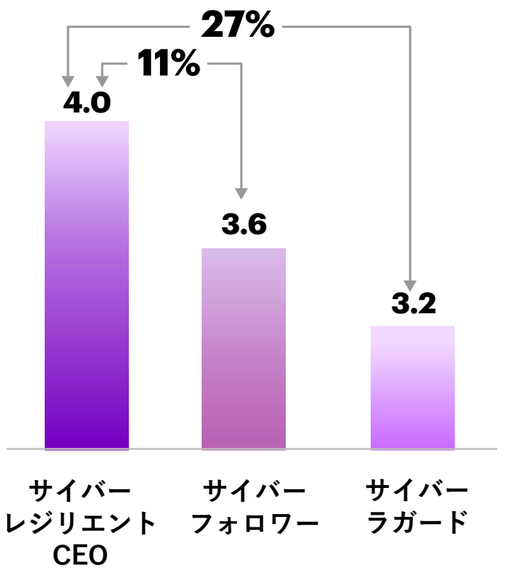
量子コンピューティングのような新たなテクノロジーを駆使して、（公開鍵暗号方式の）暗号化アルゴリズムがハッキングされ、個人情報やビジネス上の機密情報が流出するといったような、データの機密性とプライバシーをめぐる大きなリスクが発生する未来に、CEO は今から備える必要があります。

アクセンチュアの調査によると、サイバーレジリエントCEO は、インフラとセキュリティ層、データとAI層、アプリケーションとプラットフォーム層の3層から成るデジタル・コアの安全を確保できるよう徹底しています。このデジタル・コアによって、顧客、従業員、サプライチェーンパートナーにとって信頼できる環境を構築し、それを維持することで、改革に備えることができます。

「サイバーレジリエントCEO 行動指標」の「**テクノロジー**」の側面では、デジタル・コアを保護するために必要なテクノロジー関連のセキュリティ慣行を採用しているか否かに基づいて、CEO のパフォーマンスは評価されます。サイバーレジリエントCEOは4.0ポイントを獲得し、サイバーラガードを27%上回り、サイバーフォロワーを11%上回っています。

サイバーレジリエントCEO は、デジタルインフラのセキュリティを強化するセキュリティ対策を積極的に採用していることがわかっています。（図10）

図 10. サイバーレジリエントCEO はデジタル・コアの安全を確保する



出典：2023年アクセンチュア サイバーレジリエントCEO 調査（n=1,000）

実践的なステップ：テクノロジー

1. デザインされたセキュリティを優先し、推進する。

サイバー攻撃の影響を最小限に抑えるためには、迅速に対応できる俊敏なセキュリティ戦略を構築し、実行するためのリーダーシップの取り組みを支持することが必要です。そうすることで、組織は、万が一、サイバー攻撃に直面したとしてもシームレスな業務を維持できます。企業が安心して成長するためには、ビジネスにおける競争力を向上するため、デジタル化とサイバーレジリエンスの強化が必要です。その結果、ハイテクのける負債がセキュリティ領域への投資の減少に影響を及ぼしてはならないことを認識することが極めて重要です。サイバーセキュリティが後回しにされなければ、デジタル化の進展はレジリエンスの向上をもたらします。注目すべきは、サイバーレジリエントCEO の 2 人に 1 人が、変革の初期段階からサイバーセキュリティをその中心に据えています。その一例として、ある大手小売・商業銀行は、リスクと脆弱性を減少させ、データ保護を改善し、全体的なセキュリティ対策を強化するために、デジタル変革の初期段階でアジャイル・サイバーセキュリティに関す意思決定の導入を決定しました。さらに、同行はコンプライアンスを改善しながらコストとダウンタイムの削減を実現し、安全かつ信頼できる企業としての評判を高めています。一方、最近の調査によると、アプリケーション・セキュリティの不備によるエラーの発見が、計画の初期段階ではなく、アプリケーションのコーディング段階で発生した場合、修正にかかるコストは5倍になり、リリース後のコストは30倍にまで跳ね上がるということが明らかになっています。

2. ゼロトラスト・アプローチの推進

今日の CEO の最新の責務は、将来を見据えた戦略、特にゼロトラスト・フレームワークの積極的な採用という極めて重要なものです。この戦略的アプローチは、従来のセキュリティパラダイムを再定義するだけでなく、デジタル・コアの変革を先導しながら、レジリエンスを育成する触媒としても機能します。ゼロ・トラスト・マインドセットを採用するには、組織内でのセキュリティの捉え方とこれまでのやり方を根本的に転換する必要があります。これは、ユーザーの出自やネットワークの場所に関係なく、すべてのアクセス試行を不正アクセスの可能性があるものとして扱うことを意味します。ユーザ・アイデンティティ、デバイス属性、ネットワーク・コンポーネントの継続的な検証を提唱することで、CEO はセキュリティ意識を高める文化への道を開くことができます。

このアプローチの意義は、セキュリティ対策の強化にとどまりません。ゼロ・トラストの原則を受け入れ、支持することで、CEOは組織のデジタル・アーキテクチャを包括的に変革するきっかけを得ることができます。それは、データアクセス制御の再調整、強固な暗号化メカニズムの導入、最先端のリアルタイムモニタリングと異常検知システムの導入などを含みます。

このような全社的、かつ積極的なアプローチにより、CEO は自社組織の安全なデジタル・トランスフォーメーションを先導・推進するだけでなく、進化するサイバー脅威の状況を自信と俊敏性をもって把握し、乗り切ることができるようにチームを強化することで、レジリエンスを育成することができます。サイバーレジリエントCEOの70%がすでにゼロトラスト・アプローチを採用しているのに対し、その他の CEO は41%にとどまっています。

実践的なステップ：テクノロジー

3. デジタルの信頼構築を優先する

最高データ責任者（CDO）や CISO と協力し、顧客データやその他の機密性の高い情報に対する強固なデータガバナンスと保護対策を確実に実施する必要があります。サイバーレジリエントCEO の半数以上がこのアプローチを採用しています。消費者は、信頼を重視していることが明確になっており、再構築した価値観を支持しないブランドは容易に見捨てる傾向があります。新しいテクノロジーが台頭するにつれて、常に変化することに備えなければなりません。例えば、量子コンピューティングの進歩に歩に直面している今日、長期的にセキュリティを確保し続けるには、クリプト・アジャイル暗号化システムを採用する必要があります。将来に向けてシステムを保護し、顧客データを守るためには、潜在的なリスクを認識し、耐量子アルゴリズムを今すぐ導入することが極めて重要です。

4. 安全な先進技術

先進技術の開発とその活用のために、チーム全体に責任感を醸成しましょう。先進技術の採用・導入が進むにつれて、サイバーセキュリティ予算により多くのリソースを割り当てる必要があります。驚くべきことに、サイバーレジリエントCEO の76%（サイバーラガードCEO では41%）が、先進技術の採用が進むにつれてサイバーセキュリティ予算を増やす意向を示しています。

サイバーレジリエントCEO の半数は、生成AIをサイバーレジリエンスを向上させるために利用できる中核的なサイバーディフェンス・テクノロジーとして捉えています。生成AI に関連するリスクを評価・管理し、CISO と緊密に連携しながら、その安全かつ効果的な活用について組織内のあらゆるメンバーに責任を持たせます。そして、ガイドライン、プロトコル、コンプライアンス・ベンチマークを含むセキュリティ・フレームワークを開発し、生成AI と量子コンピューティングシステムに組み込みましょう。

生成AI と機械学習（ML）は、マルウェア、フィッシング、分散型サービス妨害（DDoS）などのセキュリティ脅威をリアルタイムで検出し対応し、セキュリティの自動化を強化し、膨大なデータセットを分析して、セキュリティ侵害を示すパターン、異常、傾向を特定する可能性を秘めています。しかし、生成AIの導入は、明確に定義されたガバナンス、基準、監視を伴って、慎重にアプローチされる必要があります。

組織の境界を越えてサイバーレジリエンスを拡大する

サイバーレジリエンスにおける目標は、情報セキュリティ機能の成熟度向上よりも広範です。情報セキュリティチームは、変化するサイバー脅威の状況を打破するために、継続的に能力を向上させる必要があります。CEO が CISO に責任を負わせることだけに焦点を当てては、サイバーレジリエンスは企業のビジネスリスクに沿わずサイロ化してしまいます。

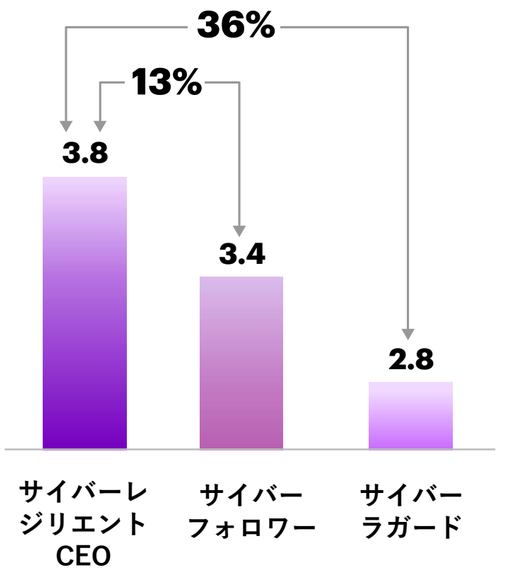
サイバーリスクがビジネスにおける最重要リスクと位置付けられているため、CEO は、企業全体のエンタープライズ・リスク・マネジメント（ERM）の一環として、経営幹部がリスクを評価し、対処していることを確認する必要があります。SEC が最近採択した規制によって義務化され、上場企業は取締役会メンバーのサイバーセキュリティに関する専門知識を報告することを課せられ、これによってサイバーセキュリティが正式に取締役会の場でも取り上げられるようになりました。

サイバーリスクは、製造現場や流通現場のようなサイバーフィジカル環境のみならず、オフショアプラットフォームのようなデジタルインフラ、医療機器のようなスマートデジタル製品、そしてサプライチェーンやサードパーティなど、企業のあらゆる側面にまで拡大しています。

最近のサイバー攻撃は、相互接続の拡大や、ネットワークへのアクセス、サプライチェーンやエコシステムの脆弱性が、最も安全なビジネスにさえ影響を及ぼす可能性があることを露呈しています。サイバーレジリエントCEOは、信頼できる環境を積極的に構築し、将来のサイバー脅威に備える必要があります。

「サイバーレジリエントCEO 行動指標」の社内および社外における「**エコシステム**」の側面では、サイバーレジリエントCEO は、エコシステムを脆弱性から守ることに積極的です。サイバーレジリエントCEO のスコアは3.8ポイントで、サイバーラガード企業と比較して36%、サイバーフォロワー企業と比較して13%高いパフォーマンスを示しています。（図11）

図 11.サイバーレジリエントCEO はエコシステムの保護に積極的



出典：2023年アクセンチュア サイバーレジリエントCEO 調査（n=1,000）

実践的なステップ：エコシステム

1. 戦略的パートナーシップにより、サプライチェーンがサイバーレジリエントとなることを期待する

あらゆるビジネスにおけるサプライチェーンの重要性を認識し、サイバーレジリエント企業とのパートナーシップを優先することが重要です。サードパーティのためにカスタマイズされたポリシーと管理策を導入し、サイバー危機の評価、準備、シミュレーションを共有しましょう。サイバーレジリエントCEOは、サードパーティに対する具体的なポリシーや管理策を実施する可能性において、サイバーラガード企業を40％上回っています。

2. 想定外のサイバー攻撃を封じるためのオープンな協力関係を構築する

サイバー攻撃による不測の事態を防ぎ、その影響を最小限に抑えるために、透明性が高く協力的な環境を醸成することが必要です。サプライチェーン全体で共有されるべき価値として、サイバーセキュリティの優先度が高く、かつ高い透明性が求められる調達領域から始めましょう。サイバーセキュリティの専門知識を有する社内のステークホルダーと強固な関係を構築することも重要です。また、社外においては同業他社や異業種パートナーとの知識共有イニシアチブに参加することも有益です。こうした業界を超えたパートナーとの取り組みにより、新たなサイバー脅威の一歩先を行くために必要なサイバー攻撃に関する指標や悪意あるハッカーを特定するためのリーディングプラクティスなど、タイムリーで実用的なインテリジェンスの交換が促進されます。サイバーレジリエントCEO の約86%は、部門全体のサイバーセキュリティ・リスクに関する知見を得るために、サイバーセキュリティ・サービス・プロバイダーと連携することの価値を認識しています。

3. サイバーレジリエンスを強化のため、規制当局と官民連携を積極的に活用する。

真にサイバーリスクに向き合い、デジタル経済を守るためには、行政と民間の協力が必要不可欠です。規制当局は、消費者や重要インフラに影響を及ぼすサイバー攻撃が増え続ける中、サイバーレジリエンスに対するアプローチを拡大、かつ深化させ続けています。CEO は、リスクベースのレジリエンス・アプローチを奨励し、ハイブリッド・クラウドやソブリン・クラウドなど、信頼やデータに基づくクラウドの採用を促進するために、規制当局に積極的に働きかけるべきです。さらに、官民連携に関与している CEO は、サイバー脅威に対抗するための情報共有、技術開発、共同の取り組みを促進しています。そのためには：

- コラボレーションを促進する：企業内および官民連携を通じて、サイバーディフェンスとレジリエンスの強化に取り組みましょう。行政および民間と協力して、部門特有のサイバーセキュリティのフレームワークおよび規制を確立しましょう。

実践的なステップ：エコシステム

- **グローバル規模のアライアンスに参加する：**国境を越えたサイバー攻撃に効果的に対処するため、米国と欧州連合（EU）のような国境を越えた国際的な連携に参加しましょう。国際的なフォーラム、イニシアチブ、協定へ参加することで、協力関係が強化されるほか、先進事例の共有やサイバーセキュリティ基準の調和、サイバー空間における責任ある行動規範の確立も促進されます。また、集団的なサイバーディフェンス能力を強化するために各国内および各国間の協力と情報共有も促進する必要があります。

- **業界特有の2国間協力**：継続的なモニタリングや脅威インテリジェンスなど、既知の悪質な行為者を特定するためのサイバー攻撃指標、戦術、テクニック、リーディング・プラクティスなど、タイムリーで実用的なインテリジェンスを外部に共有しましょう。

4.サイバー・フィジカル ワールドの保護にリーダーを参加させる。

企業は、新しい支社、製造拠点、配送センターを海外に建設し、拠点を拡大しています。物理世界とサイバー世界の接点が増え、オペレーショナル・テクノロジー（OT）の利用が拡大する中、直接的に、あるいは地域固有の新たなサプライチェーンを通じて業務妨害を狙ったサイバー攻撃から、拠点拡大に伴い発生した新たな業務を保護する必要があります。

5. 環境対策とサイバーセキュリティのレジリエンスとの関連性と脆弱性に向き合う。

重要性が高まっている環境問題への取り組みとサイバーレジリエンスの相互関連性を認識したうえで行動を起こす必要があります。例えば、風力発電所や屋上太陽光発電・蓄電プロジェクトなど、制御シス テムが各々接続され、より複雑なプロトコルを備えた分散型送電網への移行など、企業が化石燃料への依存度を下げるにつれて、サイバーセキュリティに関する新たな課題が顕在化する可能性があります。こうしたアセットの多くは、サイバーセキュリティを念頭に置いて設計されたものではありません。天候の影響を受けるため、気候変動に対するレジリエンスと持続可能性をサイバーセキュリティのレジリエンスと関連付けることが不可欠です。これを怠ると、脆弱性が増大する可能性があります。サイバーレジリエントCEO は、サイバーラガードCEO に比べて、環境に関する取り組みに存在するサイバーセキュリティの脆弱性を認識している可能性が 61% 高いです。

実践的なステップ：エコシステム

6. 情報セキュリティの成熟度を超えたサイバーレジリエンスの評価

企業のサイバー成熟度を評価することは重要ですが、単純に情報セキュリティ部門の能力を見直すだけでは、真のサイバーレジリエンスを体現するには不十分です。むしろ、CEO は、情報セキュリティ部門がビジネス全体のレジリエンスと密接につながっていることを理解し、確実なものにする必要があります。これは、ビジネスバリューチェーンの重要な機能全体にわたる統制の広範性と有効性を評価・測定し、ビジネス変革を支援し、ディスラプションを回避するためのスケールとスピード感をもってビジネスが運用できるようにするためのフレームワークを持つことを意味します。多くの企業は未だ、何が自社にとって最も重要であり、どこが最もリスクにさらされていかを把握しきれていません。レジリエンスを機能させるためには、ビジネス、テクノロジー、情報セキュリティ、およびサードパーティの間で、戦略、リスク、およびリソースの配分を明確に調整する必要があります。

7. 優れたサイバーセキュリティとリスクマネジメントの統合

サイバーリスクに基づくフレームワークと企業のリスク管理プログラムを統合しましょう。そして、経営層にサイバーセキュリティに関する業務の連携を指示し、保護すべきアセットと業務の優先順位を明確にしましょう。企業全体のリスクを評価する際に、サイバーセキュリティにおけるリスクも大いに考慮する必要があります。サイバーレジリエントCEOは、事業部門や機能を横断した全社的なリスク評価のアプローチをとっています（サイバーレジリエントCEO の64%に対し、サイバーラガード CEO は41%）。このような包括的な視点を持つことで、脆弱性をより全体的に理解することができ、サイバー脅威から企業をプロアクティブに防御する能力を強化することができます。

例えば、ある世界的な旅行会社は、サイバーセキュリティリスクをより広範な企業リスク管理の枠組みに統合することを選択することで、より優れたリスク管理、規制要件へのコンプライアンス改善、ビジネスと顧客の保護強化を実現しました。さらに、サイバーレジリエントCEOは、組織全体のサイバーオペレーションテストを重要視しています。想定外に発生するサイバー攻撃による被害を最小限に抑えるべく、脆弱性を検出するために定期的な評価を実施しています。こうしたプロアクティブなアプローチにより、潜在的な弱点を特定して対応できるようになり、サイバーインシデントの影響を軽減することができます。サイバーレジリエントCEOの70%がこの方法を採用しているのに対し、サイバーラガードCEO はわずか36%しか採用していません。

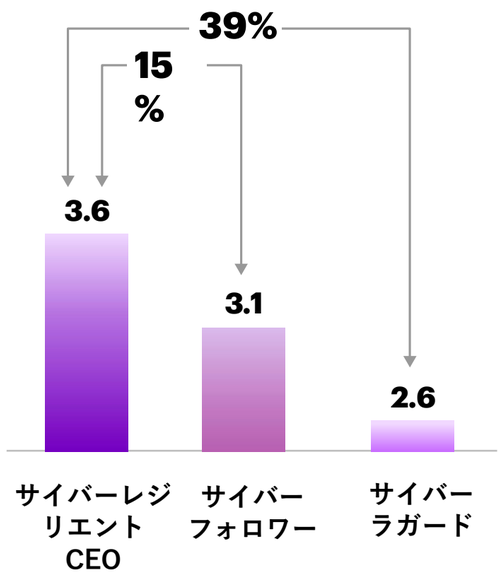
サイバー脅威における時代の最先端を行くため、継続的にサイバーレジリエンスの向上を図る

サイバーレジリエントCEOは、組織やエコシステムの中に安全な環境を醸成するための取り組みを実践しています。

サイバーレジリエントCEO は、サイバーセキュリティが一過性の取り組みではないことを理解しており、サイバーディフェンスを強化し、時代の最先端を行くために継続的な取り組みの必要性を認識しています。

「サイバーレジリエントCEO 行動指標」の「継続的なレジリエンス向上」の側面では、サイバーレジリエントCEO は、サイバーラガード企業を 39%、サイバーフォロワー企業を15%上回っています（図12）。

図12.
サイバーレジリエントCEO はサイバーセキュリティを継続的な取り組みとして認識している



出典：2023年アクセンチュア サイバーレジリエントCEO 調査（n=1,000）

実践的なステップ：継続的なレジリエンス

1. リスクプロファイルの再定義

変化するリスク状況を考慮し、ビジネスの優先事項に沿った業界をリードするサイバーセキュリティ対策を継続的に確立することにコミットしましょう。サイバーレジリエントCEO は、進化するサイバー脅威の状況に対応するため、常にサイバー・パフォーマンス・ベンチマークを強化しています。リスクの定義と許容範囲を拡大することでサイバーレジリエントCEO の60%は、このような積極的なアプローチを採用することで、他社との差別化を図っています。一方、サイバーラガード企業は34%にとどまっています。

2. 第三者によるレビューを受けながら、セキュリティプログラムを継続的に強化する。

第三者によるレビューを受けることにより、組織のセキュリティ・プログラムを客観的に評価し、進化するサイバー脅威の状況に合わせて強化策を講じることができます。サイバーレジリエントCEO の3分の2がこの手法を導入しており、サイバーラガードCEO に27ポイントも上回っています。

3. サイバーセキュリティによるブラックアウトに対する準備

経営陣による意思決定、社内外のコミュニケーション・プロトコル、社外の法律顧問、法執行機関、第三者のサイバーセキュリティ・インシデント対応チームとの連携など、重要な側面を網羅した包括的なサイバー危機対応プレイブックを作成し、実施しましょう。このプレイブックは、広範なランサムウェア攻撃や標的型攻撃、ゼロデイ脆弱性などの深刻なシナリオに対する効果的な対応を保証します。さらに組織は、重要なアプリケーションのバックアップを安全なサイバー保管庫内に隔離し、本番システムを再構築しながら業務を再開できるようにする必要があります。

4. プロアクティブなサイバー脅威防御のためのAIと高度な機械学習の活用

サイバー攻撃に対するプロアクティブな事前準備、予測、防御のために、データ、生成AI、高度な機械学習を活用するよう経営層を導いてください。統合はサイバーレジリエンスに革命をもたらし、プロアクティブな脅威の検知、自動化されたインシデント対応、適応型防御、予測分析を通じてセキュリティ対策の強化を可能にします。サイバーレジリエントCEOは皆、データ、生成AI、高度な機械学習を活用してサイバー攻撃を事前に検知・防御し、競争上の優位性を獲得するために、従業員を導くべくトレーニング機会の提供をしています。

サイバーレジリエントCEO のためのチェックリスト

戦略

- 戦略的イニシアチブと企業価値を守るためのサイバー保護戦略を確立する。
- サイバーセキュリティは、組織のリスクを低減し、能力を最適化するものであり、財務業績と同等に重要であるべきです。

人材と文化

- ビジネスリーダーは、各部門でサイバーセキュリティを導入し、従業員にサイバーセキュリティについて学ぶ機会を提供しサイバーセキュリティ教育を行うことが求められます。
- 全ての従業員がサイバーセキュリティに関して正しく理解できる文化を醸成する。
- チームをスキルアップさせるために必要なトレーニングを実施し、必要に応じて、マネージドセキュリティサービスプロバイダを導入する。

テクノロジー

- デジタルコアは、セキュリティを考慮して設計・構築されるべきであり、セキュアにアクセスできなければならない。
- 顧客データはデジタルの信頼構築の鍵であり、その保護は重要である。

エコシステム

- サードパーティのリスクを理解し管理することで、サイバー攻撃リスクを回避することができる。
- サイバーリスク評価は、特定の部門や機能に限らず、全社に実施されるべきです。
- サイバー攻撃を想定したシミュレーションを実施し、サイバーレジリエンスをテストする。
- サイバー脅威を検出するまでの時間と、封じ込めるまでの時間を注視する。

継続的なレジリエンス向上

- 深刻なインシデントを経験したことのある人材を起用し、潜在的なサイバー攻撃に対する教育や準備に役立てる。
- サイバー脅威に関する情報を共有し、国内外のサイバーセキュリティ対策を形成するための協力関係を今すぐ構築する。
- 業界をリードするセキュリティ・ベンチマークを設定し、テクノロジーを駆使してサイバー脅威を事前に予測する。

調査について

多角的なアプローチを採用

アクセンチュアのサイバーレジリエントCEO 調査は2023年6月に実施され、19業種15カ国から1,000人のグローバルCEO が回答しました。本調査では、サイバーセキュリティに関する知識と理解を図るためのテストを実施したうえで、サイバーレジリエンスを判定するための質問と、サイバーセキュリティのビジネスプラクティスに対する組織のアプローチについてインタビューを実施しました。北米、南米、ヨーロッパ、アジア太平洋地域、中東にまたがる、年間売上高10億ドル以上の企業を対象にしています*。

世界の有力企業のCEO 1,000人が回答

15カ国

- オーストラリア (68)
- ブラジル (67)
- カナダ (67)
- フランス (67)
- ドイツ (68)
- アイルランド (68)
- イタリア (65)
- 日本 (66)
- オランダ (66)
- ノルウェー (66)
- サウジアラビア (63)
- スペイン (67)
- アラブ首長国連邦 (64)
- イギリス (67)
- アメリカ (71)

年間売上高10億米ドル以上の企業が対象

19業種

- 航空宇宙 (55)
- 自動車 (52)
- バンキング (53)
- 資本市場 (53)
- 化学 (53)
- 消費財・サービス (53)
- エネルギー-石油・ガス (54)
- 医療機関 (52)
- 医療従事者 (52)
- ハイテク (52)
- 産業機器 (53)
- 保険 (53)
- ライフサイエンス (51)
- 公共サービス (47)
- 小売 (54)
- ソフトウェア＆プラットフォーム (54)
- テレコム (52)
- 旅行 (54)
- ユーティリティ (53)

*回答における年間売上高5億ドルから10億ドル規模の企業は1%未満です。

サイバーレジリエントCEO 行動指標

アクセンチュアは、サイバーセキュリティに関連する 25個の CEO の実践活動を調査した結果、5 つの主要な行動テーマが明らかになりました。これらの行動テーマは、企業が世界レベルのサイバーセキュリティレジリエンスの基盤を構築するために必要な戦略の評価と、その再定義に役立ちます。

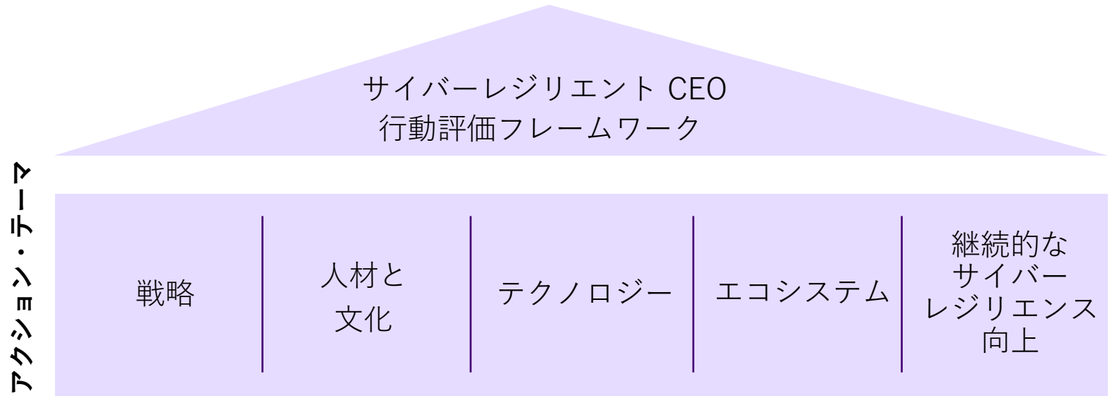
特定方法

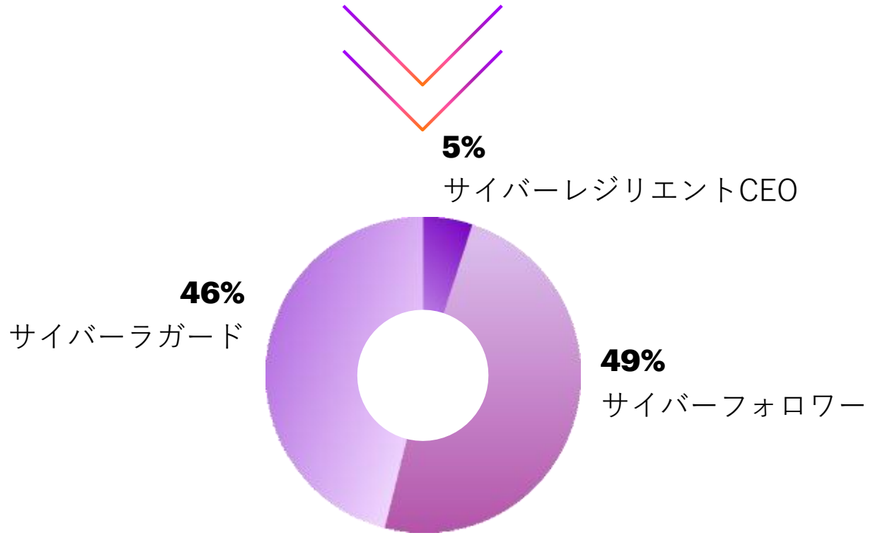
サイバーレジリエントな企業が実践しているサイバーセキュリティ対策の上位25項目を特定するために、サイバーセキュリティに関する実証的な文献を調査し、このテーマに関する社内外の専門家から情報を得るとともに、高い業績を上げている企業と協働してきたアクセンチュア自身の経験に基づき、広範な調査を実施しました。そして、25個の実践活動を5つの行動テーマに分類し、診断アセットである「サイバーレジリエントCEO 行動指標」を策定しました。この指標によって、企業のセキュリティ行動導入スコアをベンチマークし、算出することが可能です。アクセンチュアはインデックスを、ある連続体に沿った企業のパフォーマンスを測定する指標として定義しました。本調査で使用した連続体は、1点から5点までを基準としています。この指標は、企業のベンチマークとして使用され、この連続体における各企業の相対的な評価を理解するために使用されます。採点メカニズムを決定するため、各質問に対する回答には、指数に寄与する「採点」が与えられました。

この指標を検証するため、世界の有力企業のCEO1,000人を対象に、5つの行動テーマにわたる25個の実践活動の採用状況を調査し、統計的に検証しました。

この調査の結果、私たちは3つのCEO アーキタイプを特定しました：

- **サイバーレジリエントCEO**：回答対象のわずか5%に過ぎませんが、これらの企業は平均スコアより1つ高い標準偏差を獲得し、少なくとも60%以上のアクションを採用しています。
- **サイバーフォロワー**：回答対象の49%を占め、平均スコアより1つ高い標準偏差を獲得したが、5つのアクションのうち60%未満しか採用していない企業。
- **サイバーラガード**：回答対象の46%を占め、どの行動においても平均スコアの標準偏差を上回ることができなかった企業。





グローバル・ディスラプション・インデックス

アクセンチュアは、外部のビジネス環境のボラティリティと変化の度合いを評価するため、総合的な創造的破壊（ディスラプション）指標を作成しました。この指標は、経済、社会、地政学、気候、消費者、テクノロジーの各領域をカバーする6つの要素の平均値に基づいています。各要素は、さまざまな指標を指数化したスコアに基づいています。経済要素は、経済リスク評価、ボラティリティ・インデックス（VIX）、国内総生産（GDP）ボラティリティ、インフレ・ボラティリテに基づいています。地政学要素は、地政学的不安定リスクに基づいています。社会的要素は、社会不安と労働市場への不参加を反映しています。環境要素は、気候に関連する災害の頻度と気候変動リスクを反映しています。消費者要素は、OECDの消費者信頼感指数の逆数に基づき、グローバル・レベルでの悲観論を反映しています。最後に、テクノロジー要素は24個の指標で構成される指数に基づいており、創造的破壊要因の存在と既存企業の業績を、産業における創造的破壊イノベーションのレベルを示す指標として用いています。

投資家向けコミュニケーションのデータサイエンス分析

プロンプトエンジニアリングとGPT3.5を用いて、2017年から2022年にかけての世界最大手2,000社の決算説明会記録を分析しました。CEOのコメントを分析し、サイバーリスク、サイバーセキュリティ、サイバー戦略に関連するキーワードの言及頻度を調査しました。この調査によって、CEOの間でサイバーセキュリティに対する意識が高まっていることが明らかになりました。

360° サイバー・アウェアネス・スコア

本調査では、CEO がサイバーセキュリティをどの程度認識し、どの程度関連付けているかを、以下のパラメータで評価し、点数化しました：

- **持続可能性：**CEO は、持続可能性への取り組みについて、サイバーセキュリティを環境目標の中核部分と見なすような広い視野を持つようになったか。
- 人材：CEO は、サイバーセキュリティにおける人材格差に対処することの重要性をどの程度認識していたか。
- **テクノロジーイノベーション**：CEO は新たなテクノロジーを安全に採用し、導入したか。
- 顧客の信頼：CEO は、サイバー攻撃が顧客の信頼に悪影を及ぼし、顧客離れにつながる可能性があることを理解していたか。

最後に、ケーススタディ分析に加え、文献レビュー、さまざまな情報源にまたがる追加的な二次調査によって調査を補足しました。

参考文献

1 Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Cyber Crime Magazine, November 2020, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

2 Global cybersecurity spending to top $219B this year: IDC, Cybersecurity Dive, March 2023, https: /www.cybersecuritydive.com/news/cybersecurity-spending-increase-idc/645338/#:~:text=Global%20security%20spending%20will%20reach, an%20IDC%20forecast%20released%20Thursday

3 Accenture, Total Enterprise Reinvention, 2023, https: /www.accenture.com/us-en/insights/consulting/total-enterprise-reinvention

4 World Economic Forum and Accenture, Global Cybersecurity Outlook 2023, https: /www.weforum.org/reports/global-cybersecurity-outlook-2023/

5 Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Cyber Crime Magazine, November 2020, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

6 NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs, ZDNet, January 26, 2018, https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/

7 Accenture NLP Transcript Analysis of Top 2000 global companies, 2017 to 2022

8 2022 Colonial Pipeline CEO acknowledges paying hackers to restore pipeline, Reuters, June 7, 2021, https://www.reuters.com/business/energy/colonial-pipeline-ceo-paid-ransom-swiftly- restart-pipeline-testimony-2021-06-07/

アクセンチュアについて

アクセンチュアは、世界有数のプロフェッショナル サービス企業です。アクセンチュアは、世界をリードする企業や、行政機関をはじめとするさまざまな組織の中核にデジタル技術を実装することで、組織運営を最適化し、収益を拡大させ、また市民サービスの向上にも貢献するなど、お客様に対して目に見える成果を圧倒的な規模とスピードで創出しています。 アクセンチュアでは、優れた才能でイノベーションを主導する733,000人もの社員が120カ国以上のお客様に対してサービスを提供しています。 また、テクノロジーが変革の成否を分ける時代において、世界中のエコシステム・パートナーとの緊密な連携を図りつつ、業界ごとの比類のなき知見、専門知識や、グローバル規模のデリバリー能力を最適に組み合わせながらお客様の変革を支えています。アクセンチュアは、ストラテジー＆コンサルティング、テクノロジー、オペレーションズ、インダストリーX、アクセンチュア ソングの領域をまたぐ、幅広いサービス、ソリューションやアセットを活用して成果につなげています。アクセンチュアでは、成功を分かち合う文化や、360度でお客様の価値創造を図ることで、長期にわたる信頼関係を構築しています。またアクセンチュアは、お客様、社員、株主、パートナー企業、社会へ提供している360度での価値創造を、自らの成功の指標としています。

アクセンチュアの詳細は **www.accenture.com/us-en** を、
アクセンチュア株式会社の詳細**は** **www.accenture.com/jp-ja** をご覧ください。

アクセンチュア リサーチについて

アクセンチュア リサーチは、企業が直面する最も重要なビジネス課題についての知見を提供します。データサイエンスに基づく分析など革新的なリサーチ手法と業界やテクノロジーに関する深い知識を駆使し、20カ国300人から成る研究者チームが毎年数百のレポートや記事を発行しています。世界をリードする企業・団体と共に開発する示唆に富むリサーチで、私たちはお客様企業が変化を力に変え、価値を創造し、テクノロジーと人間の創意工夫の力を引き出すお手伝いをします。

詳細は **www.accenture.com/research** をご覧ください。