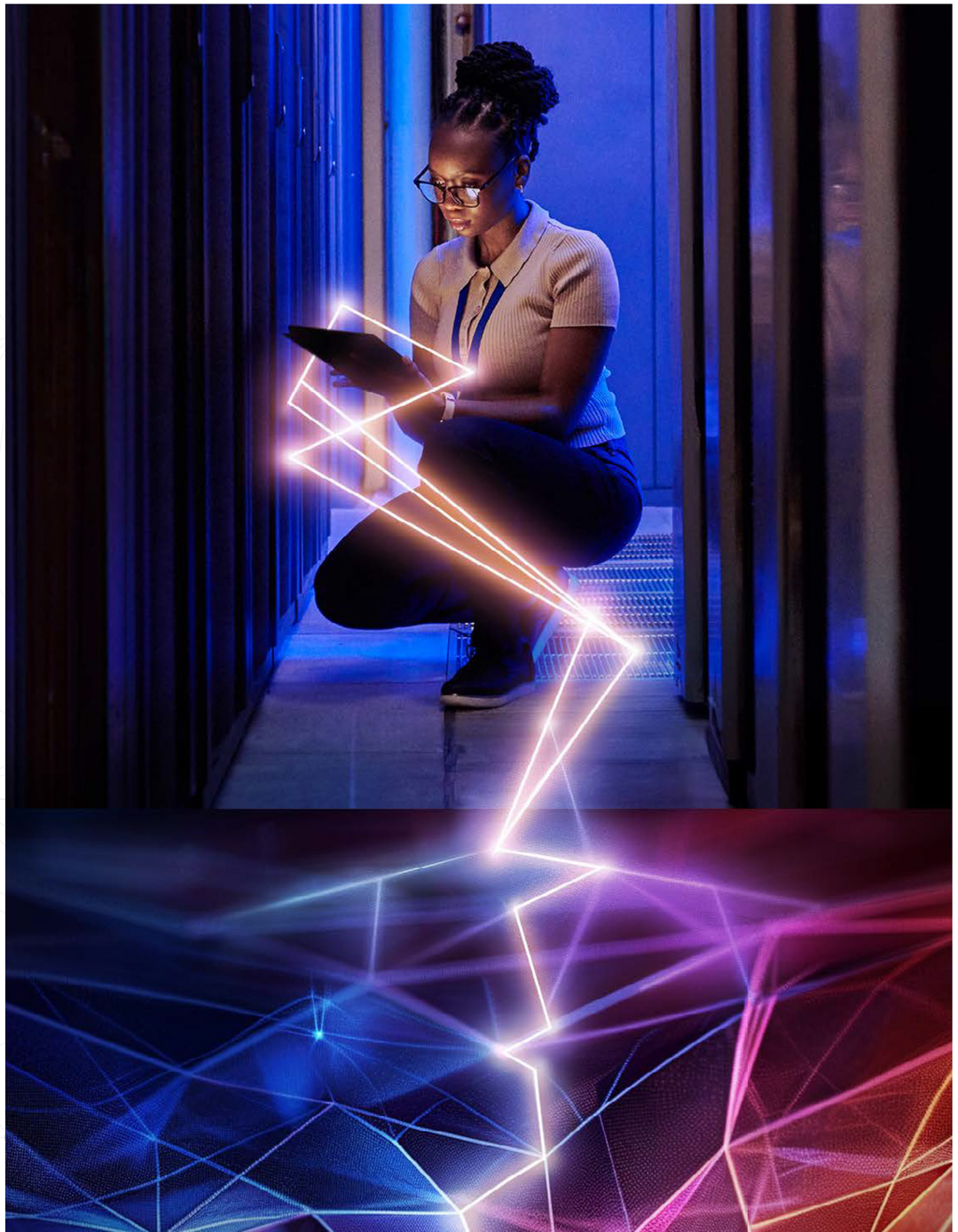
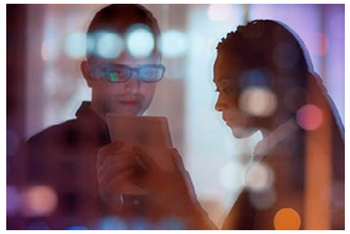
GenAI時代のデジタルコア

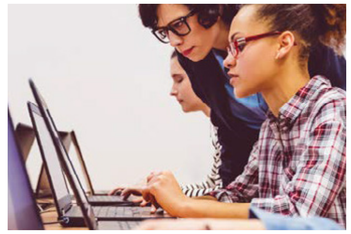
サイバーセキュリティ：
ビジネスの再創造のための
戦略的な推進力

accenture



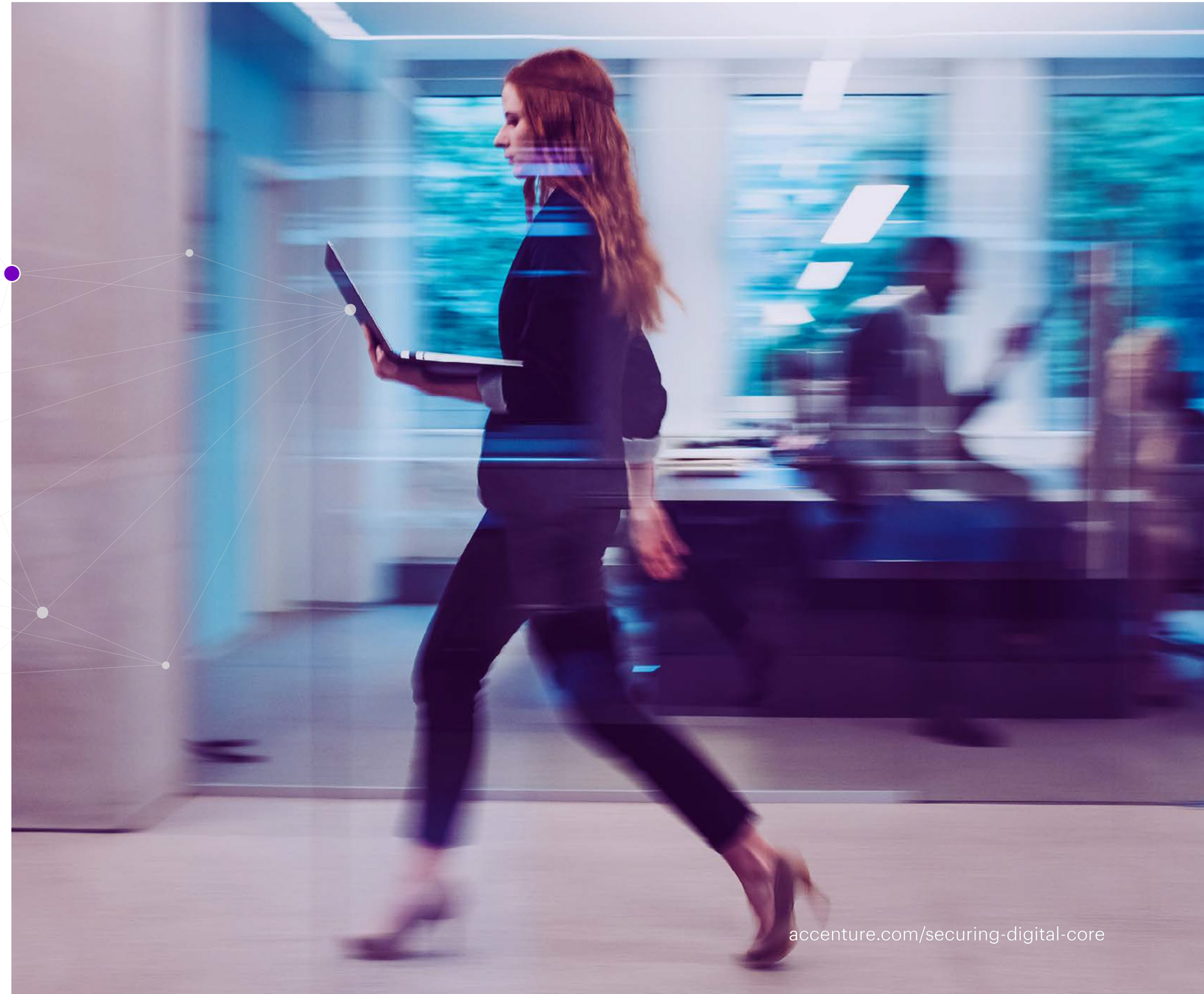
コンテンツ





エグゼクティブサマリ

企業は、生成AIを活用してビジネスのあらゆる部分を変革するために、デジタルコアの構築を競っています。しかし、重要なテクノロジー・レイヤーを不正アクセスや攻撃から守ることに関しては、多くの企業が遅れをとっています。



セキュリティはデジタルコアにとって、不可欠です。デジタルプラットフォーム、データとAIのバックボーン、そしてセキュリティが存在するデジタル基盤という3つのテクノロジーセットが常に相互作用し、再創造を推進します。最近公開されたアクセンチュアの調査「デジタルコアによる再創造」では、業界をリードする能力を持つ企業 (デジタルコア・インデックスの上位4分の1と定義) は、収益成長率が20%高く、収益性も30%増加していることがわかりました。

業界をリードするためには、俊敏性とイノベーションを実現するツールと活用方法を適切に組み合わせ、セキュリティ機能とレジリエンスを兼ね備えることが必要です。この方法では、セキュリティは静的な防御メカニズムを超えることができます。進化するデジタル環境下で、セキュリティ対策を組み込むことができれば、ビジネス成長と変革の推進力にできます。

しかし、言うが易し。アクセンチュアのデジタルコア・インデックス (指数) に基づくと、デジタルコアをまだ実装していない業界トップ企業のセキュリティ機能には、平均で23ポイントの遅れがあることがわかりました。彼らは、開発・セキュリティ・運用の連携(Dev Sec Ops)、ゼロトラストIDおよびネットワークモデルの実装、セキュリティ構成の自動化、脅威モデリングの実施、サイバー・フィジカル・システムやエッジ・システムの保護など、主要な分野で競合他社に遅れをとっています。

生成AIやその他革新的なテクノロジーがイノベーションを加速させ、業界を再定義します。それにつれて、脅威の範囲も拡大し、悪意ある行為者にさらなる道が開かれます。テクノロジーを導入する競争の中で、企業はセキュリティよりもスピードを優先することが多く、早期段階でのセキュリティの統合を怠りがちです。これによりリスクが増大し、修復作業が長引きます。この事後対応型のアプローチでは技術的負債も蓄積され、セキュリティが初めから組み込まれていた場合よりもはるかに高いコストが発生します。

現在、組織はセキュリティ体制を管理するために平均76種のセキュリティツールに依存しており、その数は増加しています[2]。たとえば、クラウド・サービスプロバイダーからの新規または変更された設定の数は毎月数千件に上っており、セキュリティチームがシステムを安全かつ最新の状態に保つために奮闘しています。このような複雑さによって冗長性が生じ、誤設定のリスクが高まり、統合作業を複雑にします。そして、セキュリティの効果が低下します。人材不足も相まって、世界中で約480万ものサイバーセキュリティ職が埋まらず、セキュリティソリューションの効果的な拡大が妨げられています[3]。

デジタルコア指数は、デジタルコアの7つの要素それぞれにおいて企業のテクノロジースタックを評価し、40個のサブコンポーネントを使用して100段階評価で表したものです。

「ケイパビリティポイント」は、特定のテクノロジーの相対的な洗練度を表し、「ギャップ」は次のレベルのケイパビリティに達するために必要なテクノロジーの最新化に向けたアクションを示しています。

セキュリティ成熟度のギャップを解消するには何が必要か？

セキュリティは市場での差別化要因であり、信頼性やレジリエンス、適応性が重視される環境を育みます。これにより、組織は自信を持って変革を進め、新たな進展と競争優位性の機会を獲得することができます。

強固なセキュリティを構築することは、短距離走ではなく、長い旅路です。組織は、ビジネスが求めるスピードと規模でセキュリティを運用しながら、コストを削減し技術的負債を減らすために、まず3つの戦略的な手段を実行することから始めましょう。

手段1
効率化

組織はベンダーを統合し、レガシーツールを廃止しながら統合ツールを導入する必要があります。生成AIの機能を活用することで、使用するセキュリティツールの数を大幅に削減することができます。このテクノロジーにより、高度な洞察と脅威分析が可能になり、プロセスを効率化してルーティンタスクを自動化し、意思決定を強化できます。

手段2
最新化

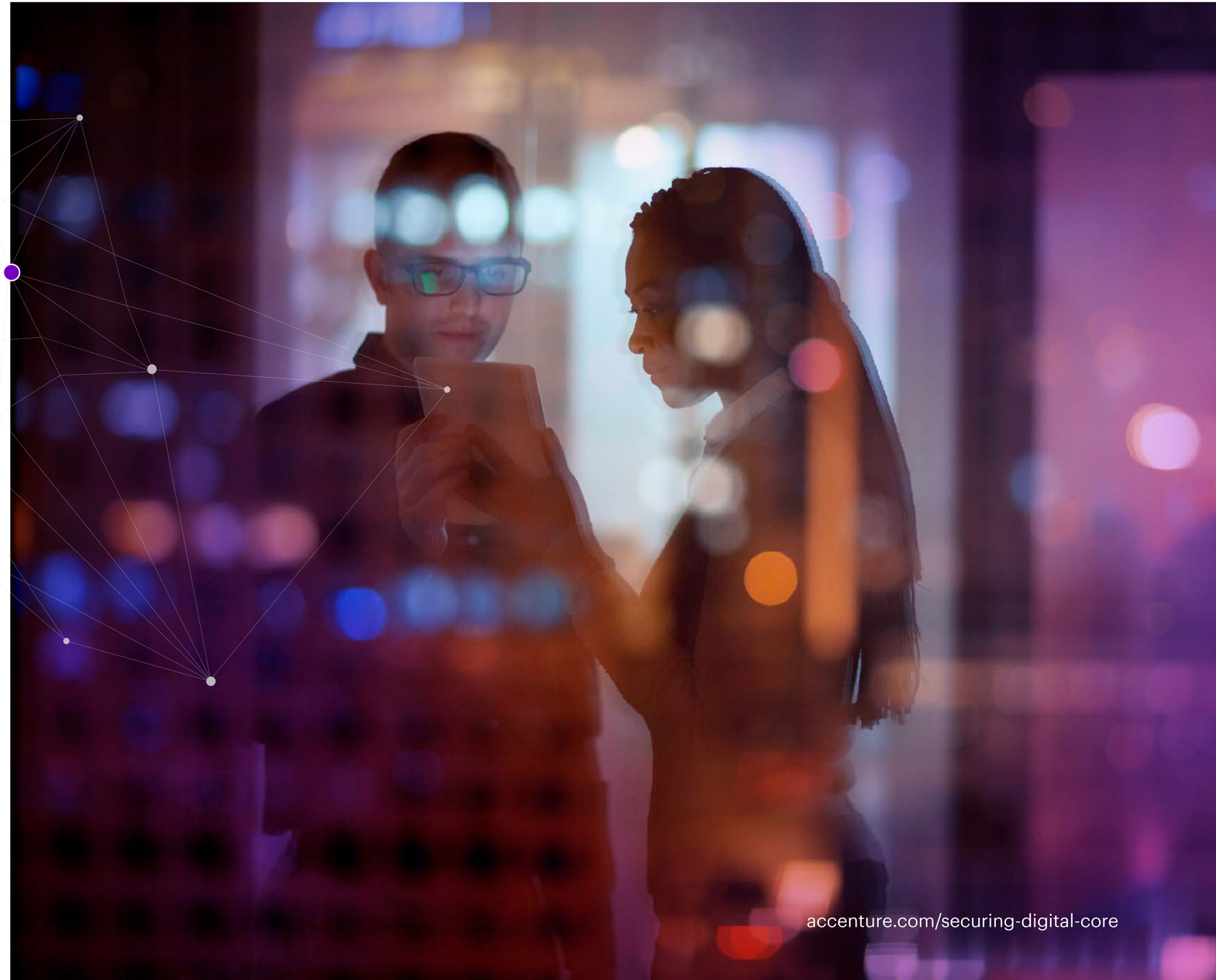
セキュリティは進化するデジタル環境に対応するために、ツールや戦略を最新化する必要があります。例えば、コード・リポジトリとパイプラインのセキュリティ・スキャンが組み込まれたInfrastructure as Code（IaC）を採用することで、セキュリティ設定を標準化し、開発プロセスの中に、テストをシームレスに統合できます。ソフトウェアアズアサービス（SaaS）およびクラウドホスト型のセキュリティ管理システムに移行すると、ハードウェア、サーバー、および更新等の管理に関連する時間やコストを削減できるだけでなく、脅威検出を強化し、コンプライアンスを改善して、展開を加速することも可能になります。

手段3
拡大と進化

自動化とサイバーセキュリティ・アズ・ア・サービス（CSaaS）は、セキュリティの拡大に役立ちます。例えば、生成AIを活用した防御ソリューションを使用して、自動化されたレッドチーミングやペネトレーションテストといった脅威テストを行います。これらのツールは、テクノロジー規制が進昨今、特に最適です。これらの規制は、セキュリティリスク、差別や偏見、プライバシーの懸念、キャリアや労働市場への潜在的な影響に対処することを目的としており、大手プラットフォーム企業やハイパースケーラーは、すでにこれらに対応したセキュリティ機能を展開しています。

再創造はなぜリスクを伴うのか

セキュリティを適切に実装することは、再創造への準備を整えるための主要な推進力の一つです。というのも、セキュリティは信頼性とレジリエンスの基盤を構築し、自信を持って変革を進めることを可能にするためです。



企業は新しいテクノロジーがビジネスにどのような変化をもたらすのかし、そしてデジタルコアにどう確実に組み込み、変革を加速させられるか模索しています。アクセンチュアでは、再創造に向けた準備とは、「既存ビジネスを支援しつつ、効率性と有効性を常に高められる状態」と定義しています。同時に、組織の継続的なニーズに応え、最新のテクノロジー・イノベーションを迅速に採用します。したがって、セキュリティも同様に俊敏でなければならず、新しい脅威やニーズに対応する必要があります。

生成AIと企業テクノロジーの変革の力を最大限に活用するには、再創造に対応できるデジタルコアが必要です。デジタルコアは、常に機能する7つの要素で構成されており、組織が自ら変革を続けるのを助けます。これらの要素には、デジタルプラットフォーム、データとAI、そしてクラウドファーストインフラストラクチャー、セキュリティ、コンポーザブルインテグレーション、そして連続体コントロールプレーンを含むデジタル基盤が含まれます (図1)。

再創造に対応できるデジタルコアを持つ組織は、以下3つの原則に従います。業界をリードするレベルの能力を維持すること、投資を戦略的なイノベーションに集中すること、そして技術的負債を積極的に管理することです。

セキュリティはデジタルコアに不可欠な部分で、基盤そのものに組み込まれており、各層にわたり統合されています。セキュリティがなければ、デジタルコアは脆弱になり、再創造と競争力の推進が困難かつ高コストになります。今日、継続的なビジネスの再創造は通常、ビジネス内部や複数のプラットフォーム、パートナー、顧客にまで及ぶ技術的な支援によって推進されます。アクセンチュアの調査によると、83%の組織が再創造に向けた取り組みを加速させており[4]、99.7%の経営幹部が業界における新たなパフォーマンスレベルの確立に注力していると回答しています[5]。

54%

ビジネスの変革または再創造、カスタマー・エクスペリエンスの向上を図る取り組みにより、テクノロジーのリスクが増加したと述べた金融サービス業界の経営幹部の割合[6]。

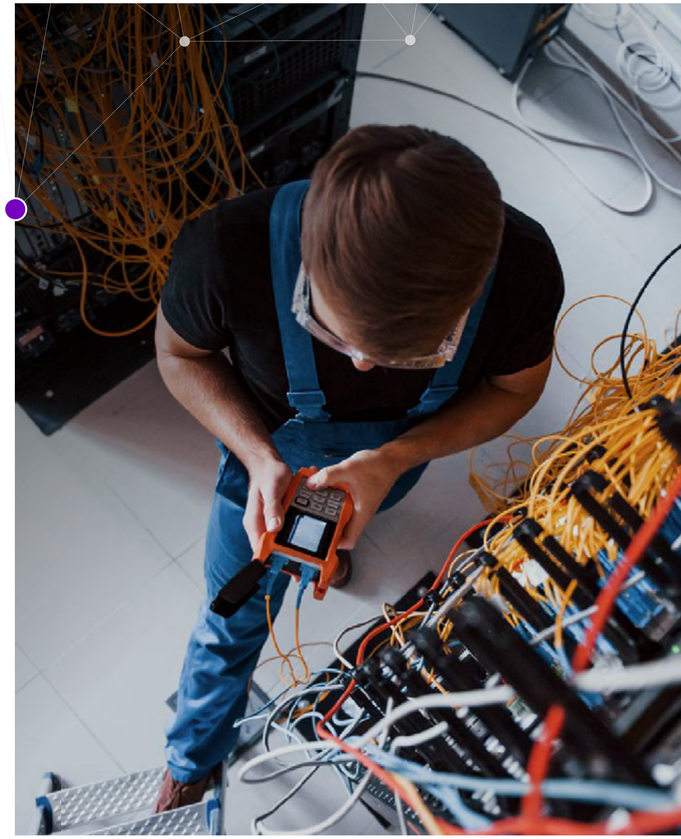
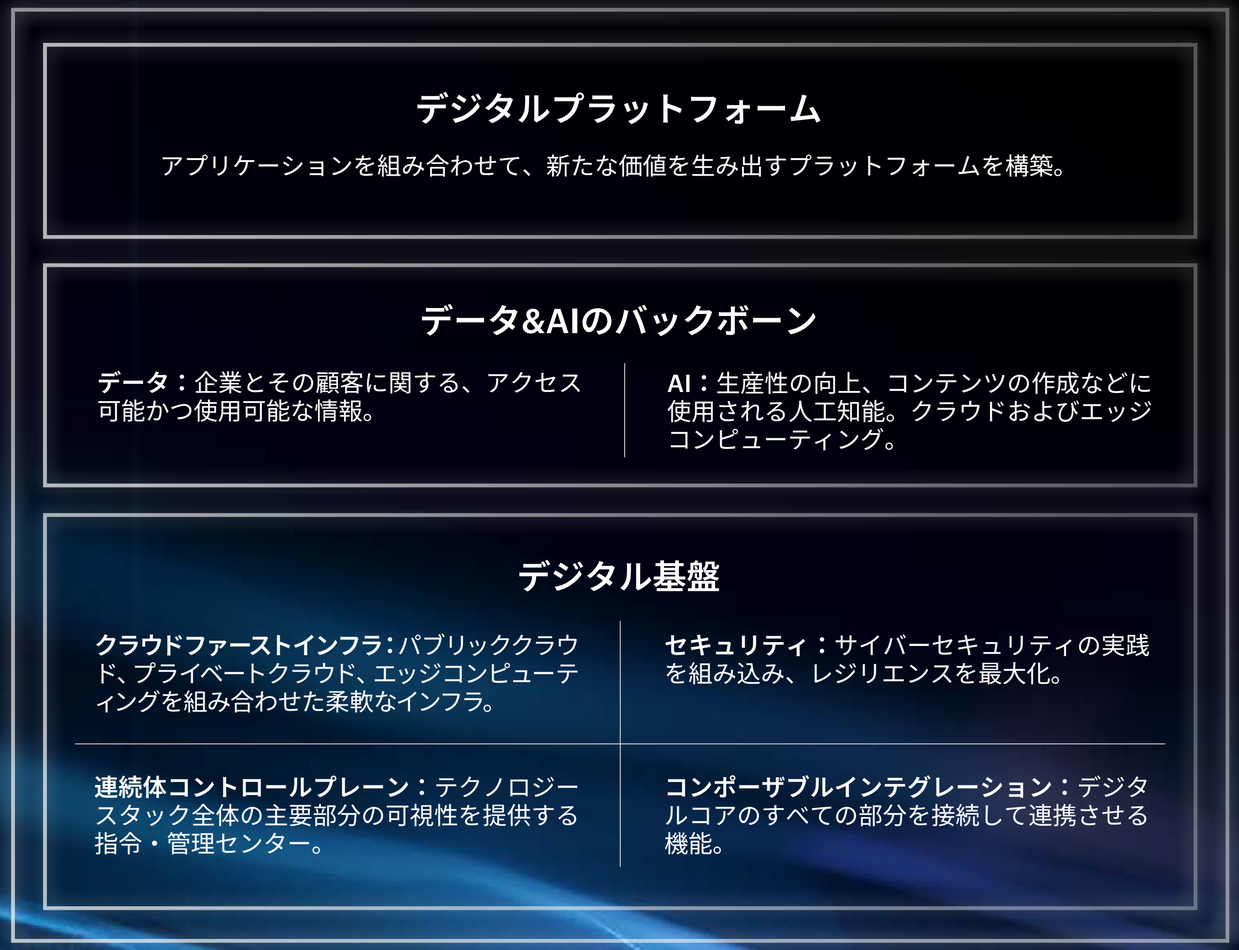


図1：デジタルコアの構成要素



デジタルコアとは

デジタルコアは、テクノロジーについて考え、
そして活用する新しい方法です。

アクセンチュアは、デジタルコアを「組織それぞれに合致した再創造の目的とやる気を育み、実現するために必要なテクノロジー・ケイパビリティ」と定義しています。このカスタマイズされたデジタルコアを構築するには、高度なデジタル基盤、シームレスなデータとAIのバックボーン、そして革新的なエンジニアリング原理を使用した安全な基盤を統合する必要があります。

この「目的に適したデジタルコア」により、組織は競争を優位にし、最も効率的に目的を達成することができます。具体的には、俊敏性とイノベーションのためのクラウドを適切な組み合わせ、差別化のためのデータとAI、成長を加速するためのアプリケーションとプラットフォーム、次世代エクスペリエンスと最適化されたオペレーションを使用し、セキュリティを各レベルで設計に組み込むことで実現します。

セキュリティは対応しているか

組織が新しいサービスやエクスペリエンスを実現するために、新興テクノロジーの導入を競い合う中、しばしばセキュリティよりもスピードが優先されます。

平均して、デジタルコアをまだ実現していない「業界をリードする」組織は、セキュリティ機能において23ポイント遅れがあります。

実際、10人中7人の経営幹部は重要な機能にのみセキュリティ対策を実装する。もしくは変革後、脆弱性が検出された後に導入すると答えています[7]。これは連鎖的な影響を引き起こします。企業が新しいテクノロジーを採用する際に、最初から強固なセキュリティ対策と戦略が「設計」に組み込まれていない場合、企業のデジタルコアは脅威に対して脆弱になり、部分的なセキュリティソリューションのリストが拡大するにつれて技術的負債が増加します。これにより、修復にかかるコストと時間がますます増加し、ビジネスの俊敏性が制限されます。

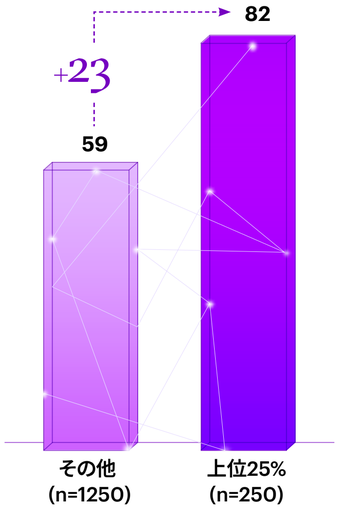
平均すると、デジタルコアを持つ「業界をリードする」組織（アクセンチュアのデジタルスコア指数の上位25%）と、下位4分1に位置する組織（図2）との間では、セキュリティ機能に23ポイントの遅れがあります。ほとんどの組織は、DevSecOps (開発・セキュリティ・運用の連携) やゼロトラスト・アイデンティティ及びネットワークの使用、セキュリティ構成、脅威モデリング、サイバー・フィジカル・システムのセキュリティ対策などの点で遅れをとっています。

このギャップは、技術的負債の課題によってさらに悪化しています。米国だけでも技術的負債の総額は1.5兆ドルを超えると推定されています[8]。セキュリティもこの問題の一部であり、アクセンチュアの調査によると、34%の組織がセキュリティを技術的負債の最大の原因として挙げています。これは、セキュリティ課題に対してできるだけ迅速に対応した結果、それが根本的な解決にはならないために、やり直しとなることに起因します。さらに、他のセキュリティツールと統合されない、またはコンテキストを提供しないセキュリティツールは、セキュリティの体制と可視性を低下させ、コストを増加させます。

さらに、セキュリティの複雑さと人材不足という難題もあります。組織は、セキュリティ体制を管理するために平均76種のセキュリティツールに依存していると報告しています[9]。これによって変革への取り組みが複雑化、さらには人材不足 (世界中で480万のサイバーセキュリティ職が埋まっていない) と相まって[10]、この複雑さは組織が効果的に拡大する能力を著しく妨げています。

図2：セキュリティ成熟度のギャップ

デジタルコア・インデックス - セキュリティ成熟度スコア



サイバー攻撃による損失

サイバーセキュリティは依然として世界最大のビジネスリスクであり、顧客の信頼やビジネスの成長、そして企業価値にまで影響を及ぼします。

侵害は金銭的な損失を増やすだけでなく、評判にも大きく影響を及ぼします。サイバーセキュリティの専門家の79%が、攻撃の際に最も懸念しているものは評判だとランク付けしています[11]。

組織がセキュリティサービスへの投資を増やす準備をする中で、成長戦略にあった投資を優先することが重要な課題となっています。96%のCEOがサイバーセキュリティは成長に不可欠であると考えている一方で、74%は潜在的なサイバー攻撃による被害を最小限に抑えることに依然として懸念を抱いています[12]。さらには、サイバーセキュリティは企業のESG（環境、社会、ガバナンス）評価の重要な要素となっており、格付け、取引、合併や買収にも影響を及ぼしています。データが漏洩した上場企業では、平均して7.5%の株価下落を経験しています[13]。

こうした懸念が急を要することは、急速に進化する脅威の状況によって明らかになっています。

セキュリティの専門家も経営幹部も同様に、その増大する危険性を認識しています。

- セキュリティの専門家の75%が過去1年間にサイバー攻撃が増加したと報告しており[14]、経営幹部の56%は生成AIが攻撃者に明確な優位性を与えると考えています[15]。
- ChatGPTのリリース以来、フィッシング攻撃は1,265%急増し[16]、生成AIを使用したディープフェイクの試みは2023年には前年比で3,000%急増しました[17]。
- アクセンチュアのサイバーインテリジェンス（ACI）の研究者も、2023年第1四半期から2024年第1四半期にかけて、ダークウェブフォーラムでのディープフェイク関連ツールの取引が223%増加したと指摘しています[18]。さらに、クラウド環境への侵入も2022年から2023年にかけて75%急増しており、脅威アクターはクラウド特有の機能を悪用して攻撃を開始しています[19]。

こうした懸念の重大さは、最近注目を集めたいくつかの事件にも反映されています。

- 中華圏の多国籍企業は、高度なディープフェイク詐欺によって2,500万ドルの損失を被りました。詐欺師たちは、会社の最高財務責任者と他の従業員をデジタル的に再現し、電話会議にて同僚に送金指示をしました[20]。
- あるアジアの航空会社のソフトウェアには脆弱性があり、乗務員の個人情報を含む6.5テラバイトという大規模なデータ漏洩が発生しました。この漏洩は、誤って設定されたAmazon Web Services バケットに起因していました。安全調査員は、機密性の高いフライトチャート、ナビゲーションデータ、プレーンテキストのパスワードなど2,300万件のファイルを発見しました[21]。
- 2023年5月、世界的な自動車会社は、クラウド環境の設定ミスによって、日本・アジア・オセアニアにいる約26万人の顧客に影響するデータの漏洩が発生したことを報告しました。自動車会社は速やかに外部からのアクセスをブロックし、すべてのクラウド環境にわたって調査を開始しました[22]。

これら3つの事件は、脅威の状況が進化し続ける中で増大するセキュリティ上の課題を浮き彫りにしています。しかし、再創造を急ぐ中での組織のセキュリティポリシーや行動も、セキュリティ上の課題の増加に大きく寄与しています。

79%

のサイバーセキュリティの専門家が、攻撃を受けた際の最大の懸念事項として評判を挙げています[11]。

セキュリティギャップを解消する

デジタルコアにおけるセキュリティの成熟度高め、 ビジネスの再創造に備えるため、企業は3つの戦略的な手段を実行することが必要です。

手段1

セキュリティを効率化して、コストを削減し、投資を改善する

セキュリティを標準化すると、冗長性やコストを削減し、プロセスを合理化できます。結果、投資の最適化に繋がります。 統合された効率的なソリューションは、より良いリソース配分と強力なセキュリティ体制につながります。

取るべきアクション:

ベンダーとツールの統合

複数のベンダーやツールを使用する代わりに、信頼性の高い少数のベンダーや統合されたツールセットに集約することで、管理が容易になり、コスト削減や効率化が図れます。また、共通のセキュリティポリシーの適用も可能になります。

これを実現するには、既存のセキュリティ・ソリューションを徹底的に評価し、それらを統合して冗長性を排除し、全体的なセキュリティを強化する統一されたシステムにする必要があります。生成AIの機能を活用することで、セキュリティ運用の効率性と有効性を新たなレベルに引き上げることができます。例えば、生成AIは、侵入検知や脅威インテリジェンス、インシデント対応など、さまざまなセキュリティツールの機能を1つの統合システムに組み込むことができます。

単独ツールより統合プラットフォームを採用

管理を簡素化し、新たな脅威に対する防御を強化するために、単独のツールに頼るのではなく、統合プラットフォームに投資します。統合プラットフォームは、運用を効率化するだけでなく、ゼロデイ脅威の防止に不可欠なリアルタイムの情報共有も可能にします。多様なデータポイント、ダッシュボード、ユーザー体験を統合することで、これらのプラットフォームはセキュリティチームに対して組織のリスク状況を包括的に把握するための手段を提供します。この統一されたアプローチにより、チームは脅威をより迅速かつ効率的に特定して軽減することができます。さらには、データとツールを一元化することで、見落としのリスクが軽減され、異なるシステム間でのイベントを関連付ける能力が向上し、より強固でレジリエンスのあるセキュリティ戦略につながります。

レガシーツールを廃止し、最良のソリューションへ投資

管理を効率化し、リソースの最適配分を実現するために、最新のツールにアップグレードします。まずは、現代の業務プロセスに合わなくなったレガシーツールから移行することで、組織のセキュリティ変革を加速させることができます。この戦略的な移行によって、複雑さが軽減されるだけでなく、冗長性を排除し、全体的なセキュリティ体制が大幅に強化されます。最新の脅威に対して、強力な防御を提供する高度なテクノロジーにリソースを集中させます。

事例

公共交通機関の
ゼロトラストへの取り組み

ある公共交通機関は、ハイブリッドクラウド環境全体にゼロトラストの原則を導入し、サイバーセキュリティを強化する必要がありました。アクセンチュアは、サイバーセキュリティプログラムを評価してギャップを特定。そして、ゼロトラストのビジョンを定義することで、実践可能な計画を共同で作成し、アイデンティティや証明書の管理のためのサイバーセキュリティメッシュなど、主要プロジェクトを優先する戦略的なプロジェクトカタログを開発しました。その結果、ビジネスの中断リスクが軽減され、資産の可視性が10%から90%以上に向上、また、サイロ全体にわたってチームの役割とガバナンスが再定義され、コストが削減されました。これには、投資戦略の最適化や自動化の追加、ソフトウェアライセンスの統合などが含まれます。

手段2

ビジネスと統合して最新化する

再創造に対応したデジタルコアを構築するためには、セキュリティを再考して見直すとともに、イノベーションへの投資や技術的負債を解消する必要があります。組織は、セキュリティを犠牲にしてまで、急速な成長を優先することはできません。強固なセキュリティを確保するためには、新しいイノベーションに対応するための対策をアップデートするだけでなく、専用のセキュリティプログラムや最新化を通じて、従来のシステムにも対処する必要があります。

セキュリティには、包括的なアプローチが不可欠です。セキュリティプロセスの多くは、従来のセキュリティ機能の枠を超え、ビジネスと連動しながら最新化する必要があります。俊敏なセキュリティプログラムによって攻撃に対して迅速に対応し、シームレスな運用の確保とコストの削減ができます。

取るべきアクション:

クラウドネイティブ・アプリケーションプロテクション (CNAPP) の保護とエコシステム全体への組込み
独自のテンプレート、事前定義されたスクリプト、プレイブック、および技術統合を活用することで、既存環境（ブラウンフィールド）と新規環境（グリーンフィールド）の両方で強固なセキュリティを確保します。セキュリティの運用を迅速にクラウドに移行することで、組織は高度なツールや構築済みのアセットにアクセスできるようになり、セキュリティインフラを最新化できます。例えば、IaC、セキュリティ・スキャン、自動化された継続的インテグレーションと継続的デリバリー/デプロイメント (CI/CD) パイプラインを実装することで、開発ライフサイクルの初期段階でセキュリティ設定を標準化して統合できます。生成AIは、セキュリティパラメーターが組み込まれたTerraform IaCテンプレートを提供することで、設定ミスを削減します。また、クラウドセキュリティをさらに強化し、コンプライアンスに準拠した安全なインフラ構築を簡素化することも可能になります。また、Azure OpenAI、Gemini for Google Cloud、Amazon Bedrockのような独自のAIサービスを安全に導入するためには、生成AIクラウド・サービスプロバイダー（CSP）環境のセキュリティも重要です。これらの戦略的な動きにより、セキュリティは俊敏性と拡張性を持ち、変化する脅威の状況に対応できるようになります。

データとAIの保護
AI環境で進化する脅威に対抗するには、法務、規制、人事、オペレーションなど、すべての主要部門のサポートが必要です。これを実現するためには、AIの導入、監査、セキュリティを監督するための部門横断的なチームを結成し、明確なポリシーと管理を確立することが重要です。AIセキュリティは、ガバナンス・リスク管理・コンプライアンス (GRC)に組み込む必要があります。また、組織は特定のビジネスニーズに基づいてAIガバナンスの原則を定義し、法務部門とコンプライアンス部門に共通の責任を割り当てる必要があります。政府や同業他社とのコラボレーションは、将来を見据えたサイバーセキュリティポリシーの形成に役立ちます。

統一されたセキュリティ基盤を共通のデータモデルと統合された運用で持つことは、シームレスなAI統合を確実にします。

AIモデルが急増する中、組織のポリシーに合わせてカスタマイズされたAIによるファイアウォールは、強力な第一防衛線となり、インタラクションを保護し、データ漏洩を防ぎ、悪意のあるまたは不正な使用をブロックします。

しかし、AIによるファイアウォールだけでは十分ではありません。完全な防御戦略としては、オーケストレーションレイヤー、RAGデータベース、及びAPIなどの領域における脆弱性を防ぐために、安全なアーキテクチャ、データ保護、アクセス制御、継続的な監視を含める必要があります。データレイヤー、基盤モデル、AIアプリケーション、ならびにIDアクセスと制御など、AIスタック全体を保護することが不可欠です。

さらに、レッドチーミングやペネトレーションテストなどを通じてリスク状況を強化することで、AIモデルを実際の攻撃シナリオに対して厳密にテストし、弱点を明らかにし、より強固な防御を構築することができます。このアプローチによって、リスク評価が急速に変化するセキュリティ環境に合わせて進化することができます。AIのセキュリティをさらに強化するためには、自動化が重要な役割を果たします。自動化によって防御メカニズムが効率化され、組織が大規模なAI関連の脅威に迅速に対応できるようになります。アクセンチュアのデジタルコア指数におけるセキュリティ成熟度スコアによると、リーダー的組織は他の組織に比べて、セキュリティの自動化という点で15ポイント上回っていることがわかります (図3)。

サイバー・フィジカル・システム（CPS）の保護

サイバー・フィジカル・システムは価値創造において重要であり、システムの不具合は生産停止やミッション失敗につながる可能性があります。接続性が増すにつれて、ランサムウェアやマルウェア攻撃に対する組織の脆弱性も増大します。すべてのCPSを特定し、定期的に脆弱性評価を実施しましょう。アクセンチュアの調査によれば、情報技術 (IT) および運用技術 (OT) のインシデントをリアルタイムで検出する機能を備えている組織は、わずか39%に過ぎませんでした[23]。

アクセンチュアのデジタルコア指数によると、業界のリーダーはCPSセキュリティに優れており、同業他社を18ポイント上回っています[24]。

ゼロトラスト原則の実装

ゼロトラストは、セキュリティモデルを根本的に再定義し、最新のアプリケーションの活用を促します。このアプローチでは、ユーザーID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潜在的に不正なものとみなします。デジタルコア指数によると、ゼロトラストの実践でリードする組織は、同業他社よりも31ポイント高いスコアを獲得しています。

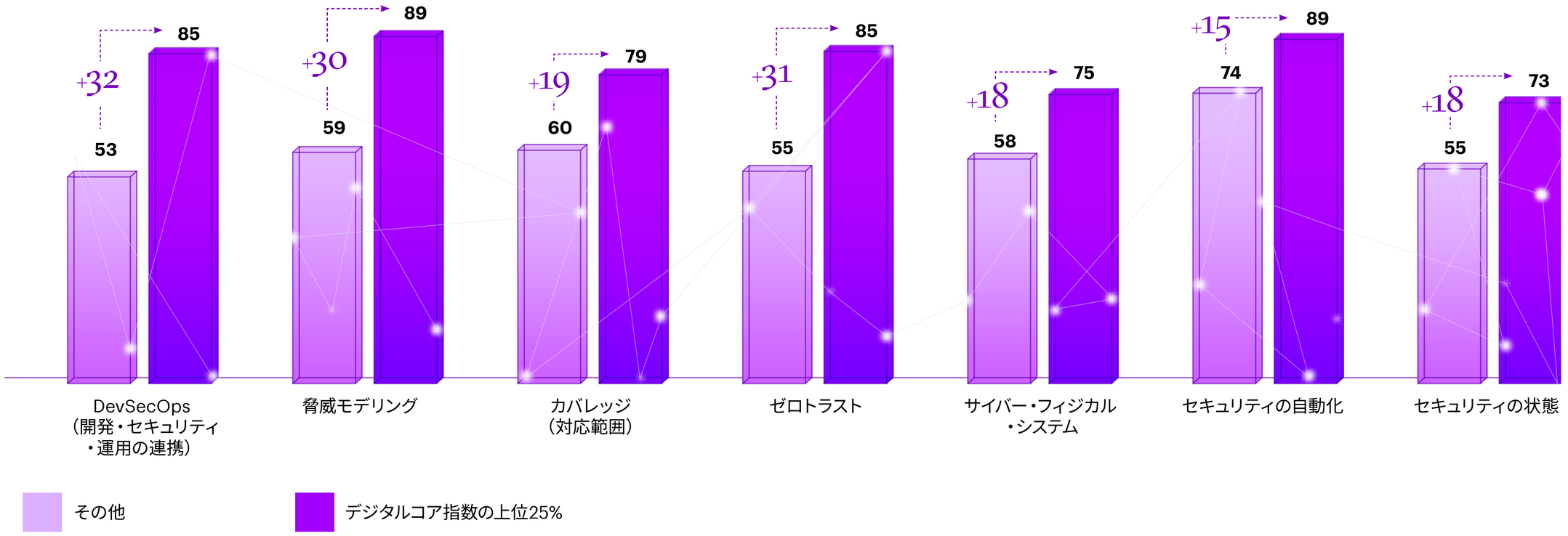
環境構築のためには、まずセキュアアクセスサービスエッジ（SASE）から始めましょう。SASEは、ネットワーク上のすべてにアクセスできる従来のVPNとは異なり、クライアントが最新のアプリケーションに接続する方法を改善します。

SASEは、ネットワーキングとセキュリティを統合し、クラウドサービスとして提供します。これにより、組織がセキュリティをクラウドに移行する際の複雑さが軽減され、俊敏性が向上し、マルチクラウドのSoftware Defined-Wide Area Network（SD-WAN）アーキテクチャが保護されます。

サイバーレジリエンスを構築し、信頼性を強化

従来の方法を超えてデータとAIを活用し、脅威への準備、予測、防御を積極的に行います。この戦略の重要な要素として、高度なアイデンティティおよびアクセス管理（IAM）の実装があります。これは、テクノロジーリソースに適切なユーザーが適切にアクセスできるようにするためのポリシーとテクノロジーのフレームワークです。その一例として、パスワードレス認証があります。パスワードレスソリューションは、パスワードの盗難や悪用に関連するリスクを排除してセキュリティを強化し、検証済みのユーザーのみが機密システムやデータにアクセスできるようにします。積極的な脅威検出や自動化されたインシデント対応、および高度なセキュリティ対策と組み合わせることで、これらのIAMイノベーションはサイバーレジリエンスを大幅に強化し、顧客の信頼とロイヤリティを強化します。デジタルコア指数のセキュリティ成熟度スコアによれば、リーダー組織は脅威モデリングに関しては30ポイント差、セキュリティの状態に関しては18ポイント差で、他を上回っています。

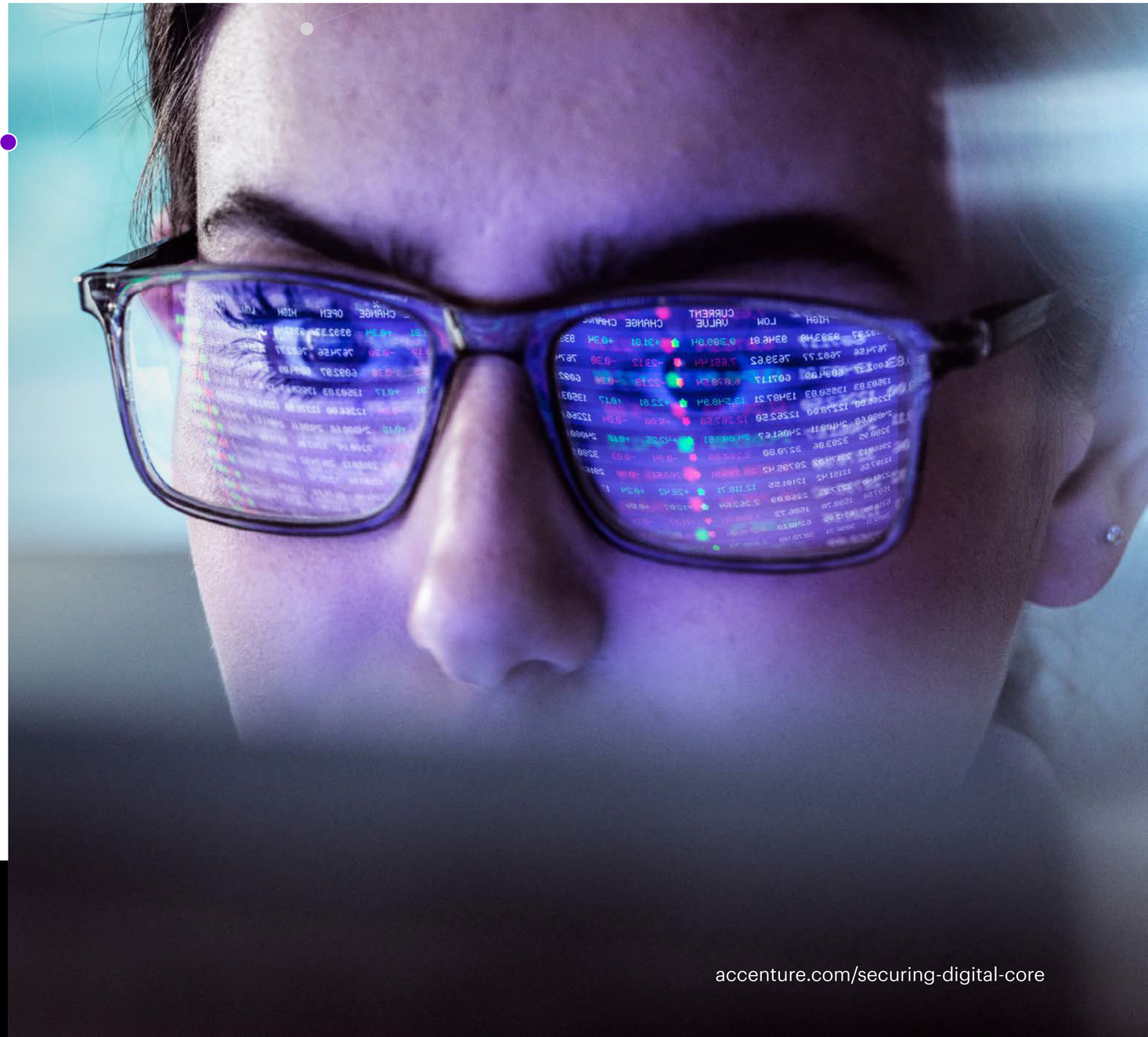
図3：セキュリティ成熟度スコア



事例

グローバル製品メーカー向けの包括的なクラウド、アイデンティティ、およびマネージドセキュリティサービスの変革

ある世界的な製品メーカーは、デジタル変革の一環として、ビジネスアプリケーションとデータをクラウドに移行しつつ、 ITのセキュリティ体制を改善するために、アクセンチュアセキュリティを採用しました。アクセンチュアのアプローチは、設計段階からセキュリティを重視したクラウド変革の加速、可視性の向上、サイバーリスクの軽減でした。アクセンチュアは、8週間以内にクライアントのAWSクラウド環境を改善し、アイデンティティコントロールとガバナンスの自動化によって、企業データレイク内の機密データを保護しました。さらに、検出機能やインシデント対応機能の強化、MITRE ATT&CKフレームワークとの整合により、クライアントのセキュリティ運用が大幅に改善されました。主な成果としては、36万件を超える脆弱性の修復、誤検知アラートの85%超の削減、可視性の向上（最小レベルから約90%）が挙げられます。新しいアプリケーションチームのオンボーディング時間は2週間から48時間に短縮され、安全なグローバルコラボレーションが可能になりました。最終的に、クライアントチームが重要なセキュリティコントロールを独自に管理できるようにスキルアップしました。



手段3

自動化とサイバーセキュリティ・アズ・ア・サービス（CSaaS）を活用して拡大する

人材とスキルの不足は、セキュリティの近代化における大きな課題です。対応策として、企業はAIとCSaaSを活用して、セキュリティプログラムを更新し、拡大する必要があります。

71%

情報セキュリティアナリストが行う業務のうち、生成AIを使用して自動化または強化することができる割合

取るべきアクション:

自動化による拡大

AIを利用した脅威が高度化するにつれ、従来のセキュリティソリューションでは不十分になりつつあります。AIを活用した防御技術を採用し、レッドチーミングやペネトレーションテストなどの脅威テストに自動化ツールを利用します。これらは、AI規制が進む中で特に重要です。大手プラットフォーム企業やハイパースケーラーは、すでにAIベースのセキュリティ機能を展開しています。例えば、 アクセンチュアのManaged Detection and Response（MxDR）サービスは、Google CloudのAIによって強化されており、さまざまなセキュリティ環境やクラウドプラットフォームとシームレスに統合されています。

生成AIによるセキュリティを強化・自動化

生成AIを業務に実装し、手作業によるセキュリティタスクを変革します。アクセンチュアの分析によると、情報セキュリティアナリストが実行する業務の71%は、生成AIを使用して自動化 (28%) または強化 (43%) することができます。このアプローチは効率性を高めるだけでなく、セキュリティ体制も強化できます。アクセンチュアのデジタルコア指数で上位の組織は、平均よりも15ポイント高い89ポイントを獲得しています。

サイバーセキュリティ・アズ・ア・サービス（CSaaS）の採用

CSaaSはデジタルトランスフォーメーションにとって欠かせないものです。変化し続ける脅威の状況に適応できる、拡張可能な専門家によるセキュリティソリューションを提供します。セキュリティ管理をアウトソースし、多数のセキュリティツールや人材の維持に伴う複雑さとコストを削減し、イノベーションに集中します。このモデルは全体的なセキュリティを強化するだけでなく、コンプライアンスとコストの効率も確保し、デジタル時代における成功の鍵となります。

事例

小売企業がビジネス成果を向上させるためにCSaaSを活用

ある小売チェーンの企業が上場した際、ITの運用を全面的に見直す必要がありました。アクセンチュアは、脅威インテリジェンス機能やセキュリティ・オペレーションセンター (SOC) などのセキュリティ・オペレーションの実装と管理を通じて、この小売企業の情報セキュリティチームを支援しました。現在アクセンチュアは。データの保護やIDの管理、ネットワークセキュリティや脆弱性管理、セキュリティなどの包括的なサービスを提供しています。この小売企業は、サイバーレジリエンスの強化と、安全で優れたビジネス成果の恩恵を受けています。

さぁ、はじめよう

昨今のデジタル時代において、効果的なセキュリティは単なる防衛手段ではなく、市場での存在感を際立たせる戦略的な資産です。信頼性、レジリエンス、適応力に富んだ環境を育むことで、組織はデジタルコアを安全に進化させ、新たな機会を捉え、競争力を高めることができます。

accenture.com/securing-digital-core

デジタルコアを保護するために、脆弱性を特定し、行動を促しましょう。

すべての企業が自問すべき質問:

簡素化

- セキュリティ体制を管理するために、いくつのセキュリティツールを使用していますか?
- サイバー脅威から身を守るために、依然として従来のセキュリティツールに依存していますか?

最新化

- 組織のサイバーセキュリティは、セキュリティツールの導入と構成を加速するように設計されたアセットを含めて、クラウドに移行されていますか?
- 組織のサイバーセキュリティプログラムは、現代の脅威に効果的に対処するために十分な成熟度と俊敏性を備えていますか?

拡大と進化

- 組織は、自動化を通じてセキュリティを拡大するためにAIを活用していますか?
- CSaaSの専門知識を活用してセキュリティ運用を進化させていますか?

出典

1. Reinventing with a Digital Core | Accenture
2. Security Leaders Peer Report | Panaseer
3. 2024 Cybersecurity Workforce Study | ISC2 Research
4. Reinvention in the age of generative AI| Accenture
5. Reinventing with a Digital Core Survey 2024 | Accenture
6. Guardian of Trust Survey 2024 | Accenture
7. Cyber Resilient CEO: Cyber-Resilient CEO | Cybersecurity | Accenture
8. The Invisible $1.52 Trillion Problem: Clunky Old Software |The Wall Street Journal
9. Security Leaders Peer Report | Panaseer
10. 2024 Cybersecurity Workforce Study | ISC2 Research
11. State of Cybersecurity 2023 Report | ISACA
12. Cyber Resilient CEO: Cyber-Resilient CEO | Cybersecurity | Accenture
13. The Devastating Business Impacts of a Cyber Breach | Harvard Business Review
14. Voice of SecOPs 2023| DeepInstinct
15. World Economic Forum Cybersecurity Outlook 2024| WEF and Accenture
16. The State of Phishing 2023 | SlashNext
17. Identity Fraud Report 2024 | Onfido
18. Beyond the illusion—unmasking the real threats of deepfakes | Accenture
19. Global Threat Report 2024 | Crowdstrike
20. Deepfake scammer walks off with $25 million in first-of-its-kind AI heist | Ars Technica
21. Pegasus Airline breach sees 6.5TB of data left in unsecured AWS bucket | TechMonitor
22. Cloud misconfiguration causes massive data breach at Toyota Motor | Chief Security Officer
23. Reinventing with a Digital Core Survey 2024 | Accenture
24. Reinventing with a Digital Core Survey 2024 | Accenture
25. Research Modelling and Analysis | Accenture

調査に関して

経営幹部への定量調査

使用されたデータは、アクセンチュアの調査「デジタルコアによる再創造」内のセキュリティ関連データに基づいています。

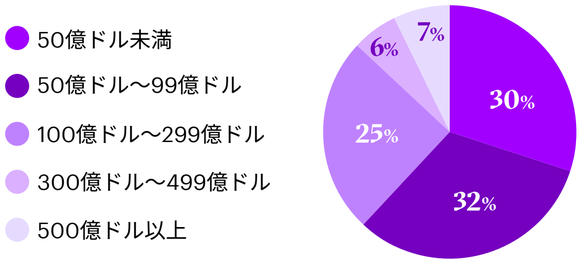
全世界1,500名の幹部層

技術変革が完了している52%の企業

19の業界

CxOレベルのみ

会社規模



業界の範囲

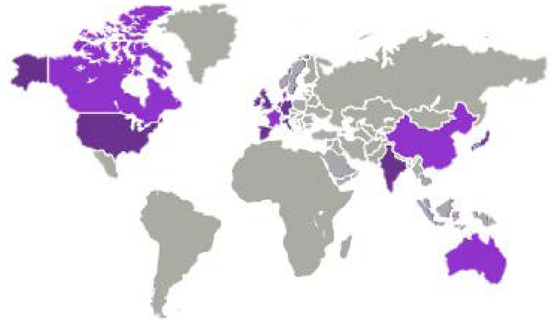
金融サービス
銀行業（83）
資本市場（45）
保険（86）

メディアとテクノロジー
メディア・通信（80）
ハイテク（82）
ソフトウェアとプラットフォーム（86）

リソース
ユーティリティ（83）
エネルギー（石油・ガスを含む）（83）
化学（84）
天然資源（81）

医療・公共サービス
ヘルスケア（78）
公共サービス（40）

製品
小売業（115）
消費財・サービス（113）
航空・旅行・輸送（80）
航空宇宙・防衛（41）
産業機器（80）
ライフサイエンス・製薬（79）
自動車（81）



10か国

オーストラリア（50）
カナダ（70）
中国（80）
ドイツ（130）
フランス（90）
インド（80）
イタリア（50）
日本（100）
イギリス（130）
アメリカ（720）

セキュリティ・インデックス

アクセンチュアは、39個の評価質問（うち7つはセキュリティに重点を置いた質問）に基づいて、企業のデジタルコア能力の強さを測定するための複合指標（インデックス）を構築しました。デジタルコアの構成要素の定義に対応した2段階の集計プロセスを適用し、全体のスコアを0〜100の尺度で評価しました。この尺度では、100がすべての要素で最大の強さを意味し、0はそれが存在しないことを意味します。次のステップとして、全体的なデジタルコア指数のスコア分布に基づき、3つのグループ組織を作成しました。上位グループはデジタルコア指数の上位4分の1に相当し、リーダーと呼びます。次に、リーダーとそれ以外のグループ間で、各構成要素におけるセキュリティ成熟度のスコアを比較しました。この指数は、各構成要素の能力の平均としてデジタルコアの総合的な強さを表します。能力ポイントとは、特定のテクノロジーの相対的な洗練度を表し、ギャップは次のレベルを達成するために必要なテクノロジーの最新化に向けたアクションを示します。ギャップが大きいほど、目標レベルに達する、あるいは関連する価値を引き出すために必要な時間と投資が増えます。

著者

Paolo Dal Cin

Global Lead –
Accenture Security

Rex Thexton

Chief Technology Officer –
Accenture Security

Andrew Winkelmann

CTO of Cyber Protection
Team – Accenture Security

Yusof Seedat

Global Research Lead –
Accenture Security

謝辞

Research Lead:
Manav Saxena

Research team:
Gargi Chakrabarty, Arlene Lehman, Shachi Jain

Marketing team:
Mark Klinge, Kamilla Giedrojc, Eileen Moynihan, Ewa Szkudlarek

この研究に対する洞察と貢献に対して、John Delmare、Muthu Raja Sankar、Ganesh Devarajan、Sadhana Joliet に特別な感謝の意を表します。

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774,000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を、アクセンチュア株式会社（日本法人）の詳細はwww.accenture.com/jp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差し迫ったビジネス課題について、ソートリーダーシップを創ります。データサイエンス主導の分析などの革新的な調査手法と、業界およびテクノロジーに関する深い知識を組み合わせ、20カ国300人ものリサーチャーとアナリストで構成されるチームが毎年数百件のレポート、記事、および見解を公表しています。世界有数の組織と共同で実施した示唆に富む調査は、顧客企業が変化を受け入れ、価値を創造し、そしてテクノロジーと人間の独創性を発揮できるよう支援します。詳細は、www.accenture.com/researchをご覧ください。