CompTIA

IT Industry Outlook 2026

Research Report

January 2026 release

概要

過去12か月間、経済の不確実性とデジタルトランスフォーメーションへの慎重なアプローチが相まって、企業は自社のテクノロジーアーキテクチャの将来について検討せざるを得なくなりました。人工知能はその解決策の重要な要素と見なされていますが、サイバーセキュリティ、データ、インフラへの同等の投資なしには、その真価を発揮することは困難でしょう。当然ながら、こうした投資には特定のツールに限定されるものではなく、それらを効果的に統合するために必要なスキルも含まれます。

CompTIAのIT Industry Outlook 2026レポートでは、今後12ヶ月間にわたってテクノロジーとビジネス戦略を牽引する主要トレンドを分析しています。テクノロジーコンポーネントに関する教育と進化、そしてスキルベースの人材育成アプローチにおける成熟度の向上が、組織を自動化と生産性向上という最終目標へと導くでしょう。

77%	1年間の組織の見通しについて「良好」と回答した割合 (net)
94%	2026年にAIに特化したトレーニングへの投資が少なくともある程度あり得ると回答した割合 (net)
#1	2026年サイバーセキュリティ戦略の推進要因としてプライバシーへの懸念が第1位に、より強力なガバナンスの必要性を示す
52%	高度な能力を備えると回答するデータ領域における最高評価（データセキュリティ）
54%	ワークフローの部分的なデジタル化を報告している割合。平行して自動化の取り組みが進められている
83%	デジタルスキルを高めた従業員を支援するため、さらなるスキル向上を図ることがテクニカルサポート部門に期待されている

See Methodology page for survey administration and sample details

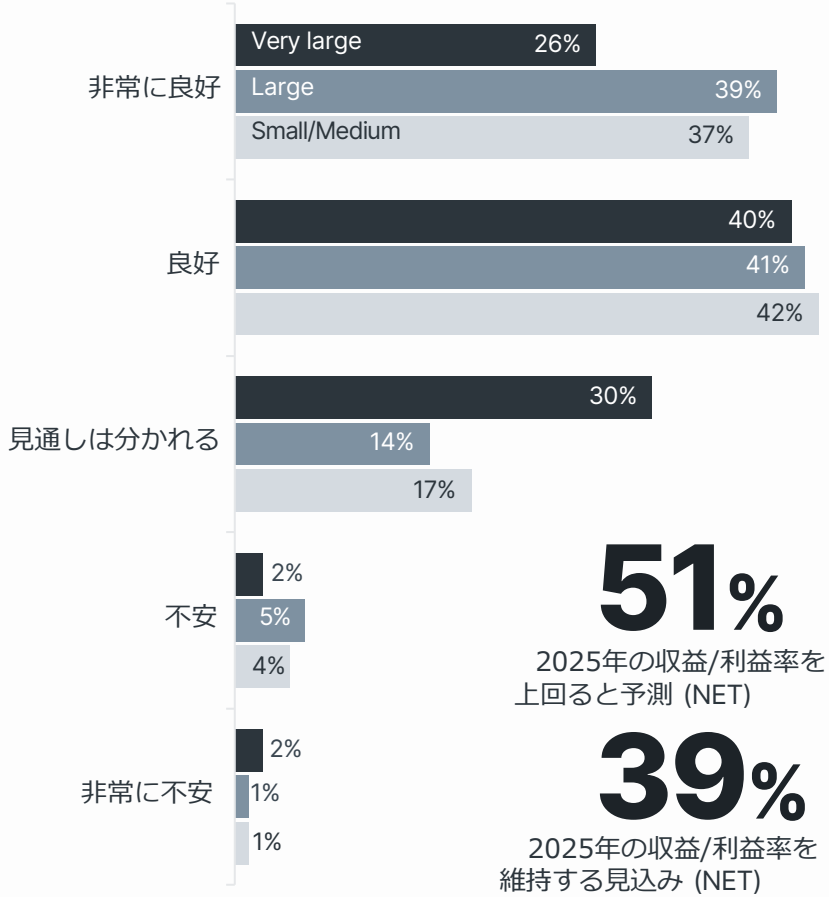
2026のトレンド

1. AI推進が続く…組織的価値の追求とともに
2. サイバーセキュリティ領域は拡大し…トレーニングも進化して対応する
3. 企業はデータ活用を強化し…戦略的目標に向けて構築を進める
4. 自動化がワークフローの刷新を推進…強力な技術チームがその取り組みを支える
5. 人材パイプラインが焦点となる…企業がスキルを業務に落とし込む中で

CompTIA

景気見通しは依然として慎重

経済混乱が続いた1年により多くの購入が先送りされた後、企業は来年に向けてやや慎重な姿勢を維持しています。CompTIAが昨年実施した景気予測は、IT業界企業を対象としたものでしたが、今年のより幅広い業種を対象としたデータも従来の見解と一致しており、効率性の追求と投資の選択的実施を求める意向が示されています。



51%
2025年の収益/利益率を上回ると予測 (NET)

39%
2025年の収益/利益率を維持する見込み (NET)

社内改善計画が楽観的な見通しを牽引

2026年の予測における楽観要因トップ5のうち3つは、業務改善に関連しています。AIの導入がこれらの改善における主要因となる可能性がありますが、ワークフローの変革とスキル構築も必要不可欠な要素となります。

1. 業務効率の向上 [51%]
2. AIを使った生産性の向上 [45%]
3. 新たな顧客層へのアプローチ [45%]
4. セールス/マーケティングの改善 [42%]
5. 新規事業または新製品 [37%]

経済要因が企業業績の予測を圧迫

関税やその他の予期せぬ出来事を含む経済の不確実性が、依然として購買決定に下方圧力をかけています。世界情勢は大半の企業にとってコントロール不能ですが、スキルを備えた労働力確保のための強固な計画を策定することは、不確実性を乗り切るための重要な戦略となります。

1. 広範な経済不確実性 [49%]
2. 貿易摩擦/関税 [45%]
3. 顧客の支出減少 [37%]
4. スキルを備えた労働者の確保 [30%]
5. 予期せぬショック（混乱） [30%]

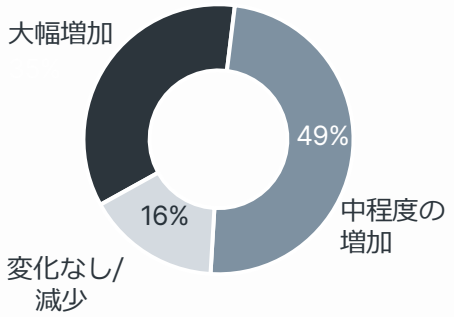
AI導入においてカスタム開発は重点ではない

60% 従業員個人による チャットボットの利用

60% アプリに統合された AI機能

39% ツールのカスタム 社内開発

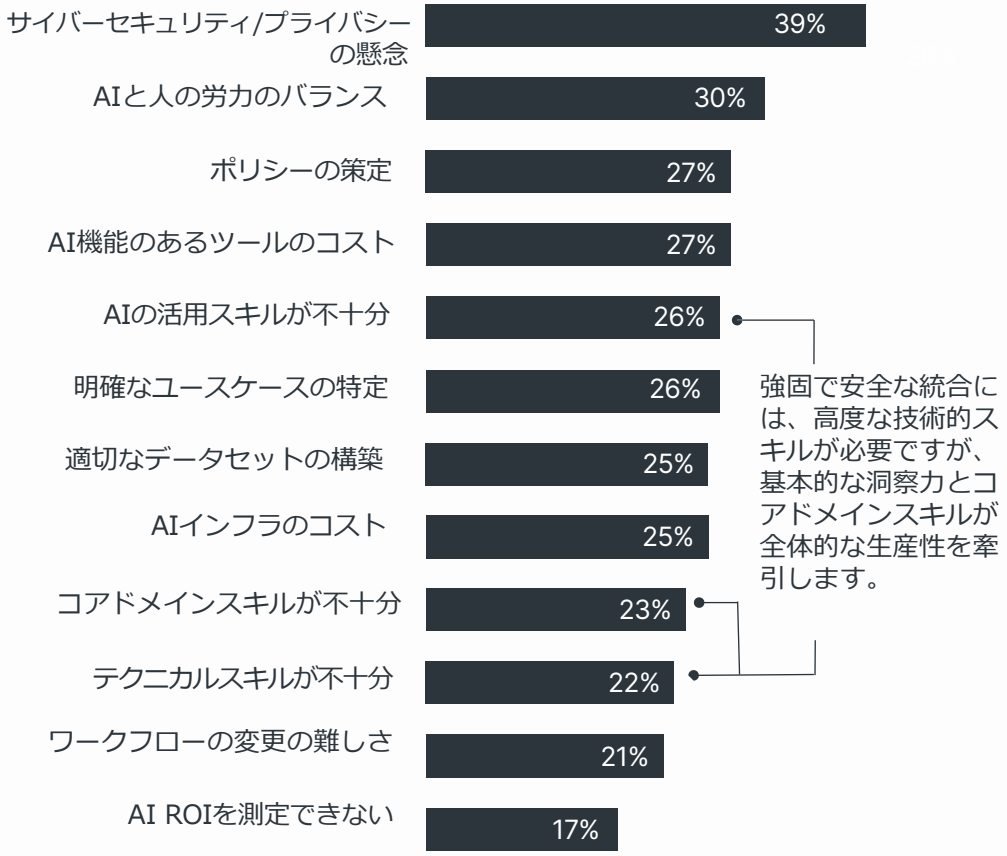
AI投資は2026年に増加する見込み



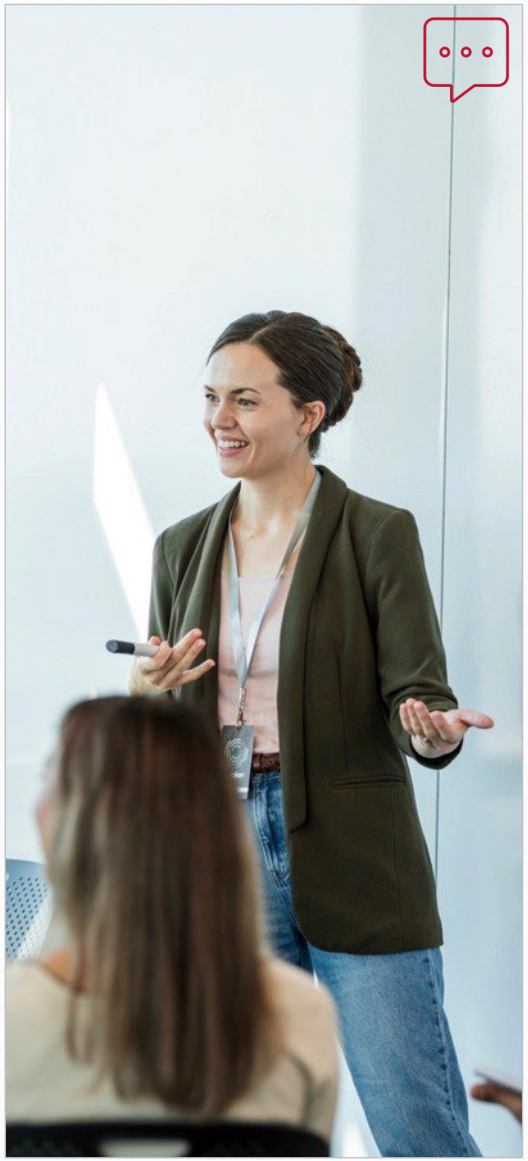
企業がAIの導入を推進するにつれて、AIの習熟度（フルーエンシー）と既存スキルのAI拡張が潜在能力を最大化するために重要になります。

AI導入における課題は、完全な実装に向けて解決すべき幅広い問題を反映している

AI関連の課題は、サイバーセキュリティのような技術的問題から、ポリシーやワークフローのような運用上の問題まで多岐にわたります。投資が増加するにつれ、AI導入の総コストを理解し、ビジネス価値を創出できる人材を確保することが重要になります。



強固で安全な統合には、高度な技術的スキルが必要ですが、基本的な洞察力とコアドメインスキルが全体的な生産性を牽引します。



企業は、全従業員のAIスキル向上に注力している

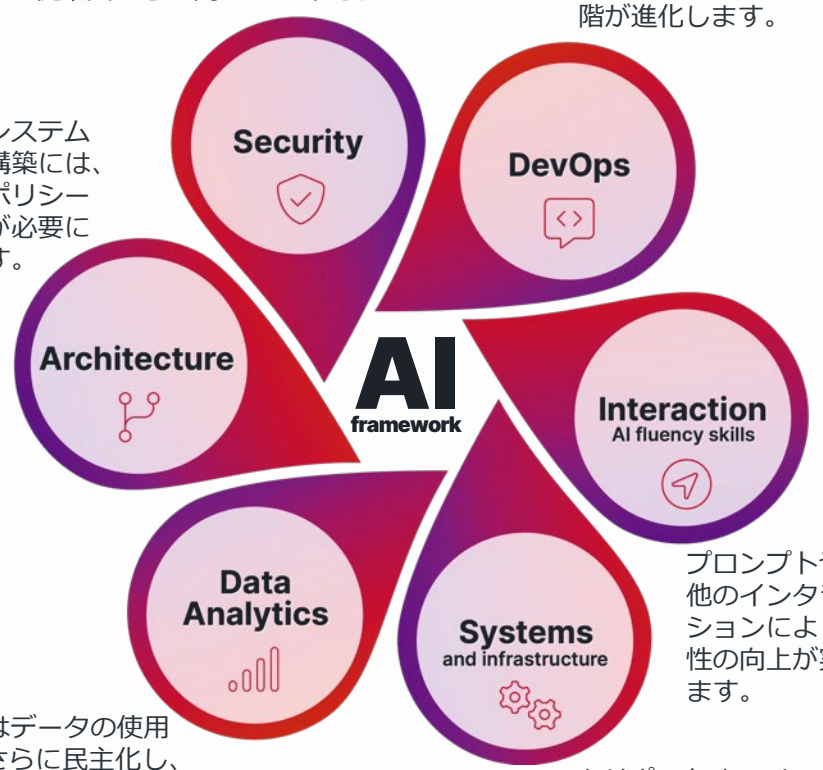
AI機能の基本的な理解	46%	従来のソフトウェアとは異なる動きを示すAIを適切に操作するには、AIに精通している必要があります
AIを活用したコア業務機能の拡張	43%	AIの導入の大半は、既存のスキルや知識を拡張するものです
AI駆動のセキュリティ脅威への認識	40%	AIが内部効率を向上させるのと同様に、脅威の有効性と範囲も向上させることができます
自動化のためのAI活用テクニック	40%	自動化は多くの企業にとって最終目標ですが、ワークフローに関する深い知識が必要です
AIを活用したデータ分析の拡張	39%	データが適切に管理されることで、AIはデータ分析を加速し、強化することができます
AIシステムのセキュリティ確保のためのベストプラクティス	38%	データとシステムの保護に加えて、AI利用に関する強力なガバナンスが必要です
AIインプット/トレーニングのためのデータの準備	37%	AIのアウトプットはインプットに依存しており、適切なデータセットの構築はデータ管理の一部です
AIへのインプット/プロンプトの構築	35%	従業員がAIを日常業務に取り入れるようになれば、効率的なプロンプトにより生産性が向上します
AIエージェントの作成	31%	エージェントは複雑なプロセスを処理できますが、監視と調整も必要です

AIフレームワークの領域は様々な職務に影響を与える

セキュリティ専門家はAIを活用し、新たな脅威から防御する方法を知る必要があり、AIセキュリティの基礎知識は従業員の意識向上の一環です。

AIコーディングツールの出現により、ソフトウェア開発ライフサイクル（SDLC）のすべての段階が進化します。

新しいシステム設計の構築には、新しいポリシーと構造が必要になります。



プロンプトやその他のインタラクションにより生産性の向上が実現します。

AIはデータの使用をさらに民主化し、モデリングと洞察を強化します。

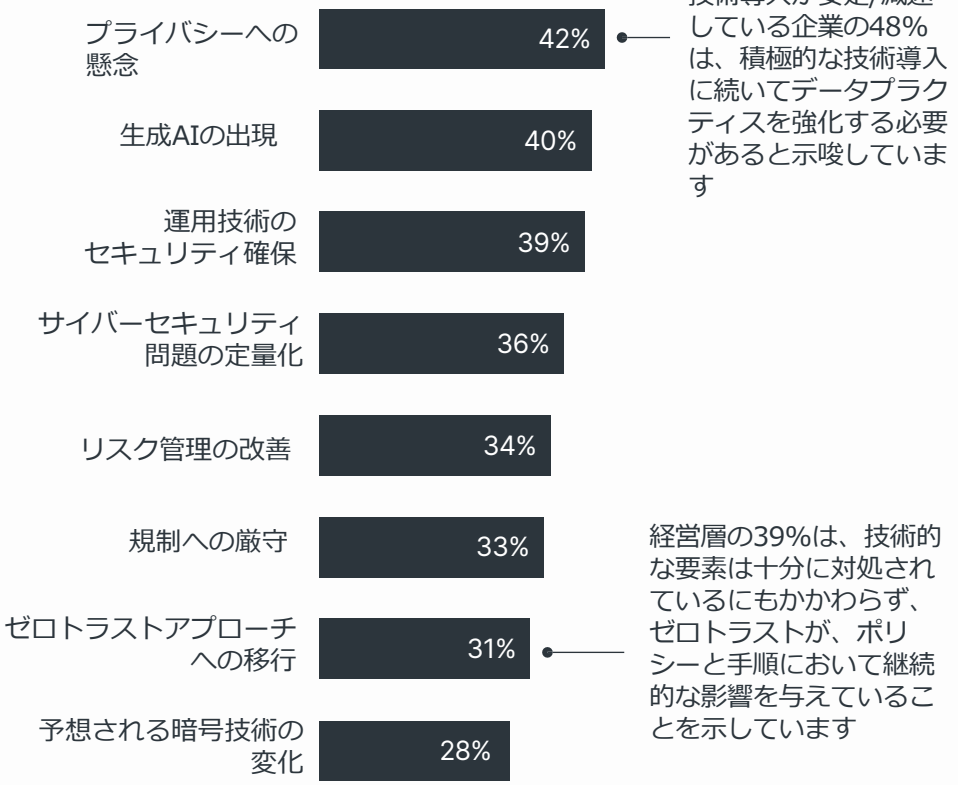
AIをサポートするインフラを構築するには、強力なクラウドスキルが必要です。

CompTIA

サイバーセキュリティ戦略は、急速に変化するデジタルビジネス環境に対応する必要がある

サイバーセキュリティという領域は、デジタルワークフローの複雑さと重要性から生まれました。組織が新興テクノロジーの影響や、業務を成功させるための要件に対処する中で、その複雑さと重要性は、戦略を推進し続けています。

サイバーセキュリティ戦略に影響を与える要素



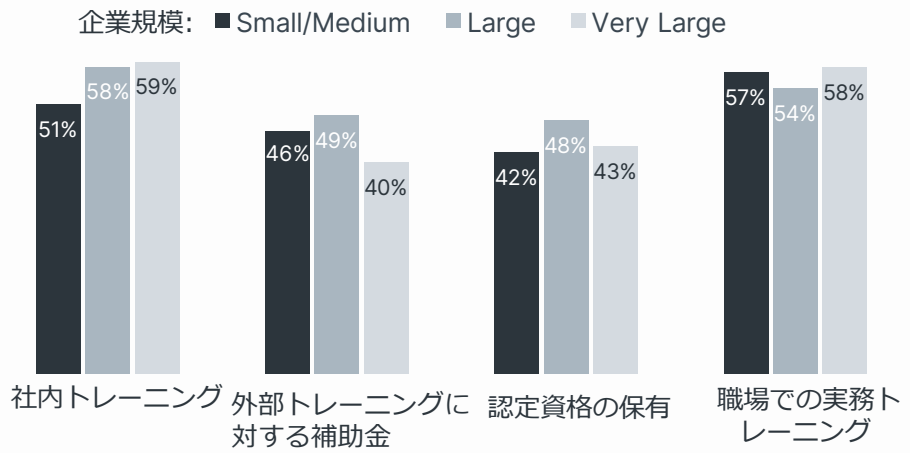
技術導入が安定/減速している企業の48%は、積極的な技術導入に続いてデータプラクティスを強化する必要があると示唆しています

経営層の39%は、技術的な要素は十分に対処されているにもかかわらず、ゼロトラストが、ポリシーと手順において継続的な影響を与えていることを示しています

ポスト量子に向けたサイバーセキュリティ対策の策定

暗号技術は、CompTIAのレポートにおいて最優先事項として取り上げられたことは一度もありません。過去のCompTIAのState of Cybersecurityレポートでは、暗号技術は「強化すべきスキル」としては低い順位に留まり、本レポートでも予想される暗号技術の変化は今後のサイバーセキュリティ計画の主要要素とはならないと予測されています。同様に、量子コンピューティングは長年にわたり注目を集めていますが、経営陣がその潜在的な影響を十分に理解するのは困難です。しかし、既存の暗号技術に対する量子コンピューティングの脅威は無視できないほど大きくなっています。量子システムが現在のアルゴリズムを解読できるようになれば、アーキテクチャ全体が瞬時に脆弱化します。企業は、ポスト量子暗号（PQC）アルゴリズムの詳細をすべて理解する人材を必要とはしないまでも、リスクを説明し、移行計画ができる人材は必要です。これには、標準規格に応じて進化可能なクリプトアジリティを備えたシステムの構築、政府規制やベンダー実装へのコンプライアンス確保、そしてPQC鍵と署名の潜在的に大きな負荷を処理できるネットワークの構築など、複数の専門領域が含まれます。この作業は、量子システムが広く利用可能になるまで待つことはできません。悪意のある人物は、後で暗号化されるデータを収集している可能性があり、運用技術コンポーネントにはアップグレードに重大な課題があるためです。

サイバースキル構築に向けた複数の選択肢が期待される



需要の高いスキルは、強固なサイバーセキュリティ人材と供給体制の必要性を示している

サイバーセキュリティの専門家は従来、より広範なインフラチームの一部門として位置付けられてきました。これは、サイバーセキュリティのより高度な性質を反映するものであり、サイバーセキュリティのニーズを満たす経験豊富な人材の需要を促進するものです。しかし、現代のサイバーセキュリティの複雑さにより、企業は、キャリア初期の人材からエキスパートレベルのアーキテクトに至るまで、どのように人材を育成していくかを検討せざるを得なくなっています。

- **54%** データセキュリティ
- **29%** OTセキュリティ

デジタルアーキテクチャのコンポーネントを保護することは、サイバーセキュリティ戦略の基盤となる要素です

- **42%** リスク管理
- **34%** 脅威インテリジェンス
- **30%** インシデントレスポンス
- **22%** ペネトレーションテスト

セキュリティ チームが従う知識ベースとプロセスにより、サイバーセキュリティの健全性が組織の成功に結びつき、セキュリティインシデントへの対応を待つのではなく、プロアクティブな行動が促進されます

- **43%** セキュリティデータ分析
- **42%** AIを駆使した運用
- **31%** プロセス自動化

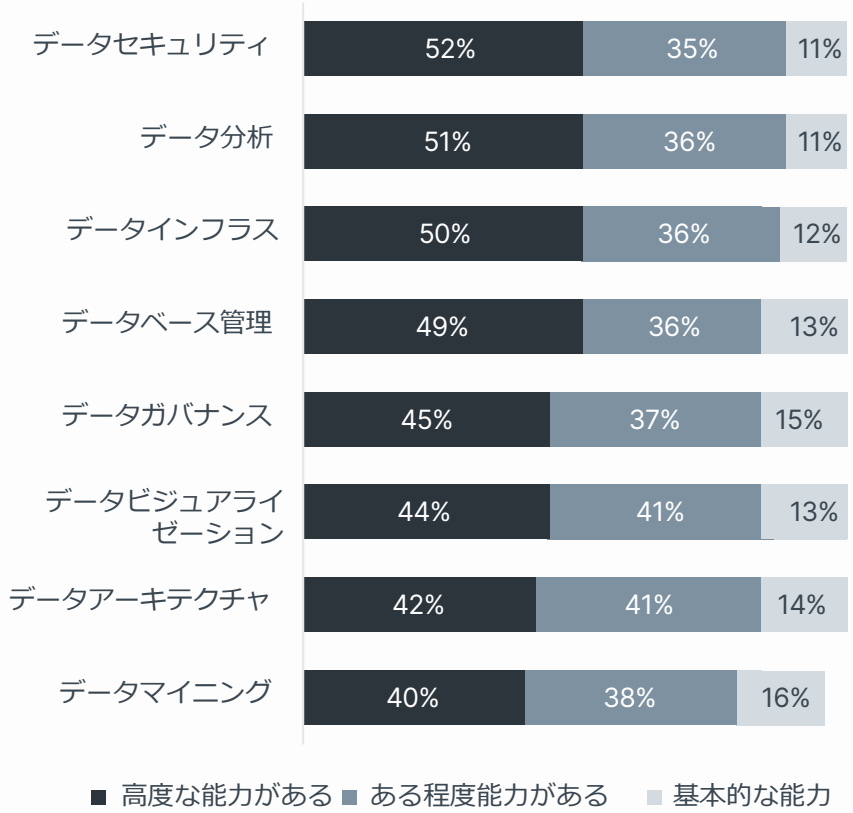
セキュリティ チームが組織内さまざまな重要事項に分散する傾向があるなか、業務の効率化は非常に重要です

- **34%** 人材の教育

現代のデジタル環境では、人材の育成が極めて重要

ほとんどの企業はデータ活用能力が十分ではない

データ領域は、テクノロジーの中でも最も新しい独立した分野であるため、多くの組織がデータ活用の実践において未だに学習曲線にあるのも当然です。サイバーセキュリティと同様に、業務全体におけるデータの重要性は、技術力だけでなく、組織の計画とポリシーにも影響を与えます。クラウドファーストの環境において、データセキュリティは重要な焦点となっており、データ分析の向上はここ数年間、最優先事項となっています。しかし、高度な戦略を成功させるには、データ管理のより基礎的な要素、すなわちデータベース管理、データガバナンス、データマイニングに取り組む必要があります。



データの課題には包括的な戦略が必要

データ管理とデータ分析という2つのスキルセットは、データ課題として挙がったリストの大半を占める技術的プロセスを推進するのに役立ちますが、企業はインフラの構築の波及効果や部門間の調整も考慮する必要があります。

1. データ分析の高速化
2. AI要件を理解する
3. データポリシーの構築
4. データ分析スキルの構築
5. サイロからのデータ統合
6. 新しいデータ形式の管理
7. データ規制の取り扱い
8. データ管理スキルの構築
9. ネットワークアーキテクチャの構築
10. ストレージアーキテクチャの構築
11. 自動化の欠如

技術的プロセス　組織的プロセス　人材育成

データ活用の改善に向けた計画的なステップ

52% データスペシャリストの育成トレーニングに投資する

51% 全従業員を対象としたデータ基礎知識のトレーニングに投資する

49% データアーキテクチャを改善するためハードウェア/ソフトウェアに投資する

44% データ管理/分析に特化した職務を構築する

43% データ使用に関する企業ポリシーを構築する

CompTIA

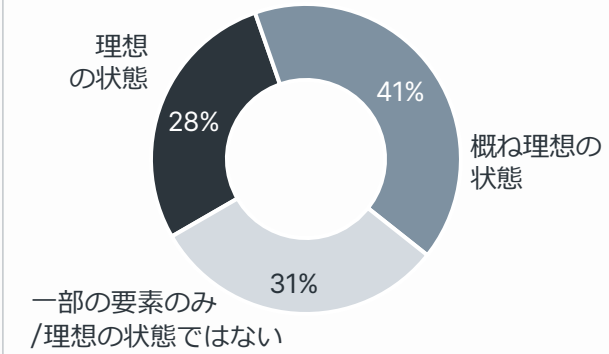
ワークフローの進化と自動化はデジタルトランスフォーメーションの高度な段階です

デジタルトランスフォーメーションは、ワークフローを変える性質上、長いプロセスを要します。ワークフローのあらゆる構成要素を深く理解している企業は少なく、デジタル強化によって文書化されていない変更が行われることがよくあります。

54%

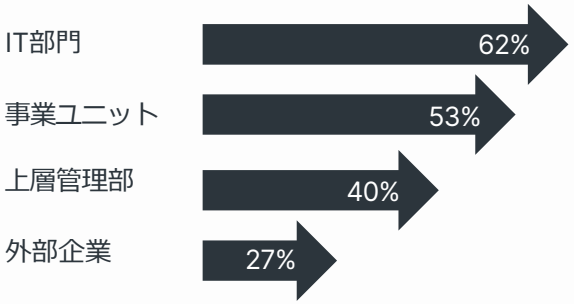
ワークフローは部分的にデジタル化されており、さらなるデジタル化と自動化に並行して取り組んでいる

自動化の現状

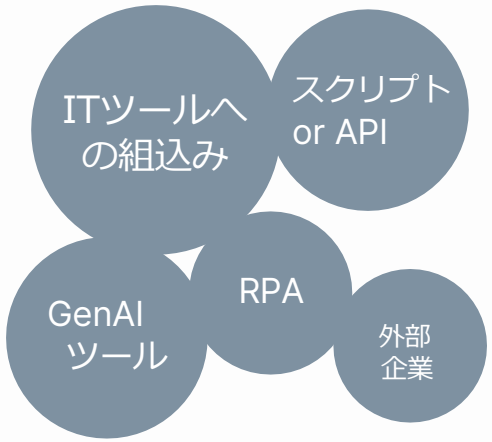


自動化のアプローチは、動機や目的に基づいて異なる場合も

自動化の推進要因

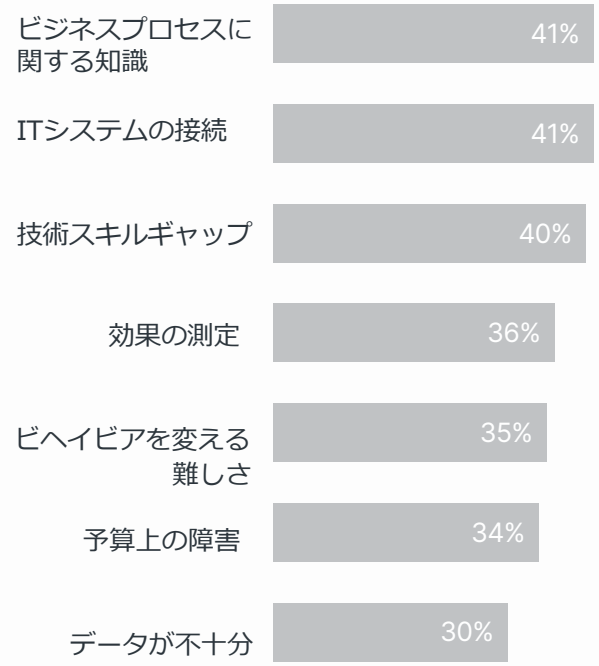


自動化の方法



自動化における課題は技術を超えた問題点を浮き彫りに

ユビキタスコンピューティングと高度にデジタル化された環境により、極めて複雑なプロセスの自動化が可能になり、ほぼあらゆるプロセスを自動化できるという認識が生まれています。しかし、現実には、多くのビジネスプロセスは依然として非常に複雑であり、問題解決や意思決定の過程を記録するデータはほとんどありません。適切なシステムやスキルを装備することは確かに課題ですが、多くの自動化の取り組みは、自動化を真に活用する従業員の新たなビヘイビア（行動）を考慮する前であっても、完全なコンテクストに沿うものにするのが難しいといえるでしょう。



テクニカルサポートは、デジタル業務において依然として重要な役割を担う

83% デジタルスキルを高めた従業員の要求に対応するため、テクニカルサポートスキルの構築を計画している企業の割合

92% テクノロジー導入に積極的な企業における割合

90% 経営幹部層における割合

テクニカルサポートにおける重点的活動

#1 エンドユーザーへのテクノロジーとセキュリティの適切な使用方法に関する教育

#2 AIを活用してユーザーリクエストの解決策やパターンを発見する

#3 エンドユーザーのリクエストパターンを理解し、問題領域を特定する

#4 チケットシステムとプロセスの改善（使いやすさ、応答時間など）

#5 特定の注目度の高いアプリケーションのサポート提供

企業はテクノロジー分野を横断したキャリアパスの構築において相対的な強みがあると主張している

1から10の評価スケールで、テクニカルサポートから他のテクノロジー分野へのキャリアパスの構築に関して、8以上と評価する企業が相当数あります。

インフラストラクチャ — 59%

テックサポートからの最も典型的なパスですが、この領域は他が優先されるにつれ、注目度は低下しています

ソフトウェア開発 — 58%

企業は、AI実装とアプリケーションのカスタマイズのための社内開発の取り組みを構築し、進化させています

データ — 65%

データの管理と分析はどちらも、テックサポートの基盤から構築される専門分野です

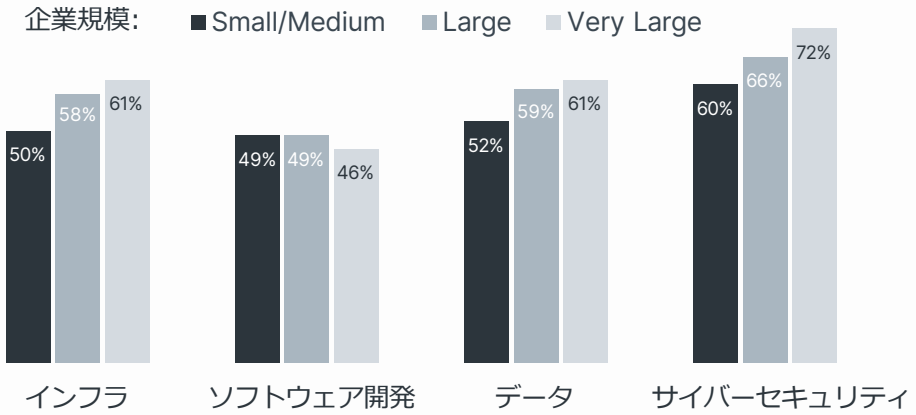
サイバーセキュリティ — 65%

企業によっては、キャリア初期向けのサイバーセキュリティロールを検討しているところもあれば、テックサポートを人材のパイプラインとして活用しています

テクニカルプロジェクト管理 — 57%

プロジェクト管理には幅広いテクニカルおよび組織的知識が必要であり、テックサポートからの自然なステップとなります.

デジタルワークフローの構築とサポートには、すべてのテクノロジー領域が重要



CompTIA

スキルに関する懸念への対応策

既存従業員へのトレーニングは、今年1年におけるスキルギャップ解消策として最も一般的な計画です。特に業界で認知の高い認定資格と組み合わせることで、企業は既に保有する知見を活用しながら、AI環境における新たな課題に取り組むための専門知識とベストプラクティスを拡充することができます。

64% 現在のスキルセット内でのトレーニング

47% 業界認知の認定資格取得を目指す

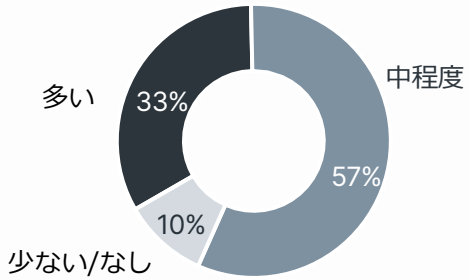
45% 新規雇用

42% 新しい職務への転向

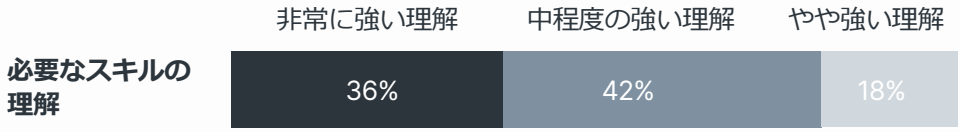
35% 外部企業との連携

スキルベースのアプローチは優先事項であるがさらなる定義が必要

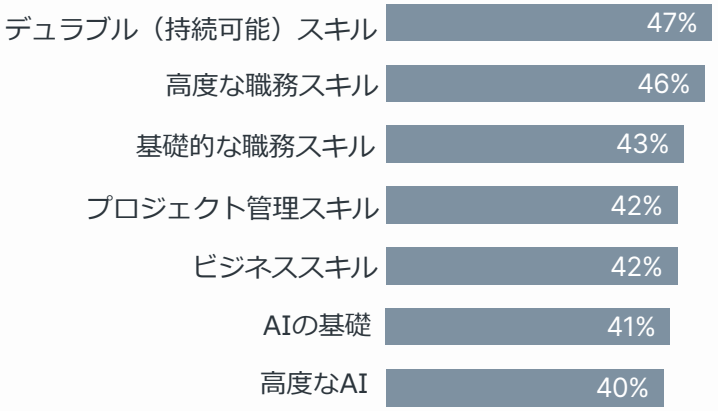
現在のスキルベース投資



10社中9社が、スキルベースの人材育成アプローチに多額または中程度の投資を行っていますが、これらの投資が期待される結果を生み出しているかを判断するのは難しい場合があります。



重要スキル領域



スキルベースのアプローチを完全に追求するには、企業は必要なスキルに対する理解を深める必要があります。必要なスキルは依然として、デュラブル（持続可能）スキルや特定の職務に関連したスキルが主流です。

企業が人材育成を変革する中であらゆる選択肢が模索されている

今日の急速に変化する環境において、人材育成は極めて柔軟である必要があります。

1. 既存テクニカルスタッフのアップスキリング
2. 既存テクニカルスタッフのクロススキリング
3. テクニカルおよびビジネススタッフのリスキリング

CompTIA

Methodology

CompTIAのIT Industry Outlookは、2025年10月から11月に、オンラインで実施された定量調査をもとに作成されました。ビジネスおよびテクノロジーの専門家1,012名が回答し、95%の信頼性でサンプル誤差は±3.1%ポイントでした。データのサブセットおよびセグメント化によっては、推定サンプリング誤差率がより高くなる場合があります。

どの調査でもそうであるように、標本誤差は起こり得る誤差の原因の一つにすぎません。非標本誤差を正確に計算することはできないため、その影響を最小限におさえるために調査設計、データ収集と処理のあらゆるフェーズで予防的ステップがとられました。

さらなるトレンド情報については、前年度のCompTIAのIT Industry Outlookリサーチをご参照ください。

CompTIA, Inc. は、市場調査業界のInsights Associationの一員であり、世界的に尊重されているその標準および倫理規定を順守しています。本レポートに関するいかなる質問は、CompTIA Research and Market Intelligenceが対応します。research@comptia.org.