

# ワークフォース アイデンティティ管理

アイデンティティ管理へのアプローチの  
成熟がもたらす画期的な変化

2024年4月

この電子書籍は、Okta の委託を受けて Enterprise Strategy Group が作成したレポートであり、TechTarget, Inc. のライセンスに基づいて配布されます。

## 目次



調査方法と回答者内訳、成熟度モデルの詳細



# 調査の目的と注目すべき調査結果

## 調査の目的

本レポート（および裏付けとなる一時調査）は、組織がエンドユーザーのアイデンティティを管理するために採用するテクノロジーと戦略が、生産性、企業リスク、組織としての俊敏性に関連する成果に直接影響を与えるかどうか（また、どの程度影響を与えるのか）を理解することを目的としています。

また、この調査では、組織がより優れた成果を実現するために採用すべき、実用的なベストプラクティスを明らかにするため、ワークフォースアイデンティティ管理に対して最も成熟したアプローチを使用している組織に共通する特徴を探ります。

## 注目すべき調査結果

ワークフォースアイデンティティの成熟度を高めている先進的な組織は、ビジネスの成果実現で大きなメリットを得ています。この傾向は、以下の調査結果に示されています。



**3.9 倍**

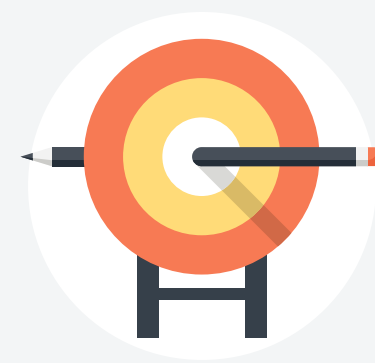
「自社のアイデンティティソリューションは、ビジネスの俊敏性を促進している」を選択した回答者数。



**3.6 倍**

「自社のアイデンティティソリューションは、従業員の生産性を高めている」を選択した回答者数。

ワークフォースアイデンティティの成熟度を高めている先進的な組織は、セキュリティの成果実現で大きなメリットを得ています。この傾向は、以下の調査結果に示されています。



**3.4 倍**


「自社のアイデンティティソリューションは、インシデント対応に大きく役立っている」を選択した回答者数。



**3.2 倍**

「自社のアイデンティティソリューションは、脅威を大幅に緩和するのに役立っている」を選択した回答者数。



A man with a beard and glasses is looking at a screen in a dimly lit room. The screen shows a green interface. In the background, there are other people, including a woman in a patterned top and a man in a brown shirt. The scene appears to be a control room or a meeting room.

今こそアイデンティティの成熟度を  
最大限に高めるべき理由

# アイデンティティの成熟度の重要性を裏付ける 3つのトレンド

ワークフォースアイデンティティの成熟度について、その概念と組織にとっての有用性を論じる前に、組織が置かれている状況を理解することが重要です。

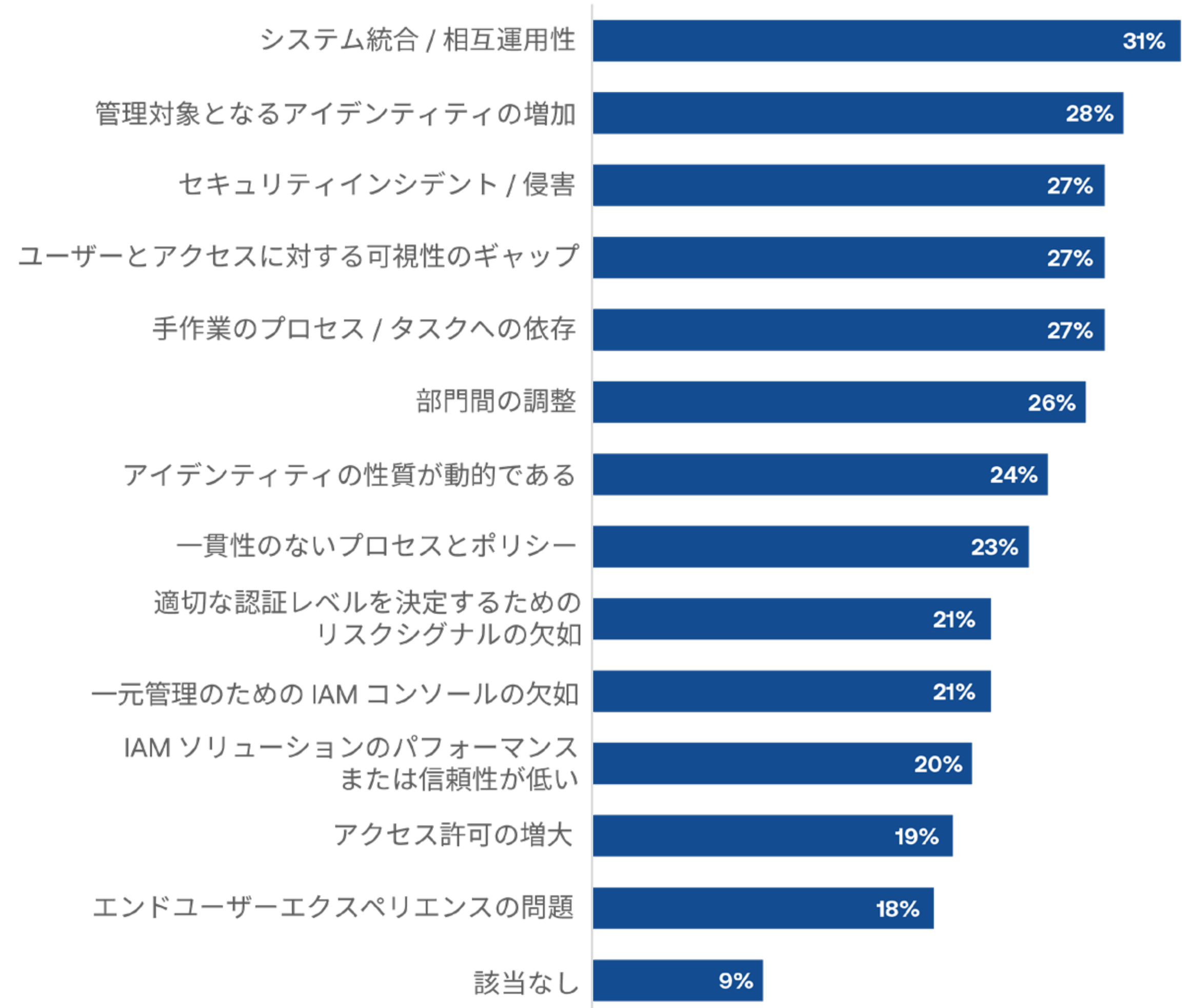
TechTarget の調査部門である Enterprise Strategy Group の調査によると、以下の3つの明確なトレンドが今日の市場で起こっています。これらが複合的な影響を生み出し、効果的で効率的なワークフォースアイデンティティ管理の実現を複雑化させています。

- 1. 管理対象となるアイデンティティの増加：**回答者の83%は、今後12か月間に自社の管理下にあるアイデンティティが増加すると予想しています。一方、アイデンティティが減少すると予想する組織は21分の1にとどまります。また、今日のアイデンティティ管理で組織が直面する課題として、アイデンティティの増加が2番目に多く挙げられています。
- 2. クラウド導入の継続がもたらす複雑化：**Enterprise Strategy Group の調査によると、パブリッククラウドの導入は今後も続く見込まれています。アプリケーションを新規に導入する際に、クラウドファーストのアプローチをとっている企業は35%であるのに対し、オンプレミスファーストのアプローチをとっている企業は16%です。また、アプリケーションの大半をクラウドでホスティングしている企業の割合は、今後数年間で17%から27%へ増加する見込みです<sup>1</sup>。「パブリッククラウドの利用によって、自社のアイデンティティ管理が複雑化した」と考える回答者が73%に上ることからわかるとおり、アイデンティティに焦点を絞って取り組んでいるチームにとって、このトレンドは問題を招いています。
- 3. リモートワークの継続：**平均して、組織内の半数に上る従業員が、ハイブリッドワークまたはリモートワークで勤務していると推定されます。回答者の77%は、リモートワーク体制を維持することでアイデンティティ管理が複雑化していると報告しています。

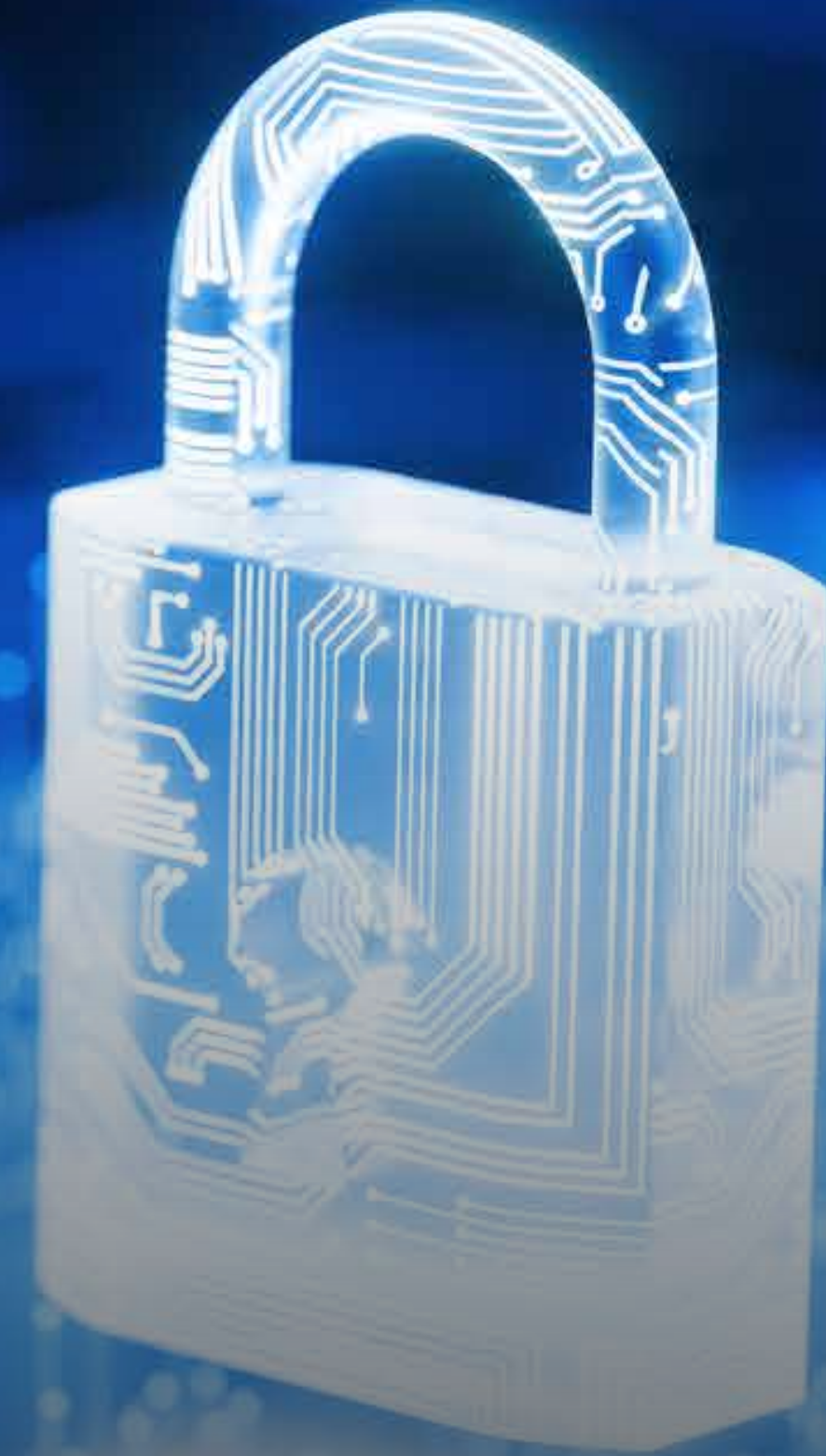
このような市場環境から、アイデンティティのプラクティスとテクノロジーの点検に本腰を入れ、必要な措置を講じることが非常に重要となります。

<sup>1</sup> 出典：Enterprise Strategy Group Research Report、「2024 Technology Spending Intentions Survey」（2024年2月）

ワークフォースアイデンティティ管理で組織が直面している課題。



# ワークフォースアイデンティティの 成熟度モデルの確立



## ワークフォースアイデンティティの成熟度の現状

Okta は、アイデンティティを通じてセキュリティとガバナンスを強化し、生産性を高め、効率を向上させるための[包括的なフレームワーク](#)を開発しました。

Enterprise Strategy Group は、このフレームワークが組織に導入される際の有用性を検証するため、Okta の成熟度モデルに沿って評価する調査を準備し、フレームワークの原則をカテゴリ別の質問 8 項目に置き換えました。回答に基づいて、Okta の成熟度モデルで提唱されるベストプラクティスに組織がどの程度合致しているかを判断できます。次に、ワークフォースアイデンティティの成熟度別（全 4 レベル）に回答者と所属組織を区分しました。組織は、成熟度の高い順に「戦略的」「先進的」「拡張中」「基礎レベル」に分類されます。

Enterprise Strategy Group の分析では、アイデンティティの属性とプラクティスがどの程度成熟しているかがポイントで評価され、結果に応じて成熟度ポイントが割り振られます（100 点満点）。

評価では、以下の属性とプラクティスが考慮されます。

- 包括的なアイデンティティ戦略の有無（10 点）
- シングルサインオン（SSO、10 点）と多要素認証（MFA、10 点）の導入範囲
- アダプティブ認証および / またはパスワードレス認証の使用（10 点）
- ディレクトリサービスの連携（10 点）
- アイデンティティ / アクセス管理（IAM）ソリューションと主要ビジネスアプリケーションの統合（10 点）
- アイデンティティ関連ワークフローの自動化（25 点）
- アイデンティティガバナンス管理（IGA、75 点）および特権アクセス管理（PAM、75 点）ソリューションの採用

全体としては、戦略的（81～100 点）と評価された組織はわずか 20% でした。また、先進的（71～80 点）と評価された組織は 24%、拡張中（61～70 点）と評価された組織は 26%、基礎レベル（60 点以下）と評価された組織は 30% でした。

質問内容、回答の選択肢、関連する成熟度スコアの詳細については、後述の[調査方法と回答者内訳、成熟度モデルの詳細](#)をご覧ください。

### ワークフォースアイデンティティの成熟度別の内訳



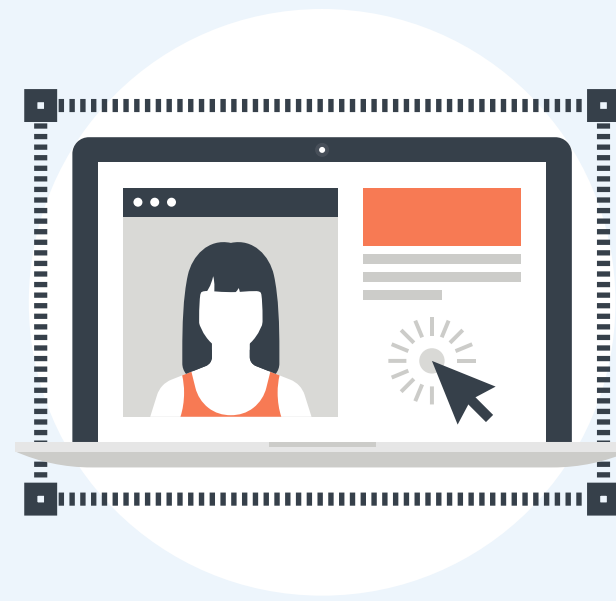


# 「成熟度を高めようとする組織は、 何よりもまず、これらの原則に沿うよう努めるべきである」

## ワークフォースアイデンティティの 成熟度のリーダーに見られる 特徴とは？

Okta のワークフォースアイデンティティの成熟度モデルは、戦略、プロセス、アイデンティティソリューションにまたがる多面的なものとなります。戦略的と評価された組織には、その他の組織と比較したときに右に示す重要な特徴が見られます。

これら3つの組織的特徴を合わせて評価することで、ワークフォースアイデンティティの成熟度モデルにおける位置付けが決まります。成熟度を高めようとする組織は、何よりもまず、これらの原則に沿うよう努めるべきです。



戦略的組織は、  
アイデンティティに関して  
包括的なアプローチを策定  
している。



戦略的組織は、アイデンティティ  
ソリューションをより広範に  
(ソリューションの機能が多い)、  
より深く (対象とする環境の割合が  
高い) 導入している。



戦略的組織は、エコシステムの  
統合とインテリジェントな自動化に  
重点を置いている。

## 戦略的組織は、アイデンティティに関して包括的なアプローチを策定している

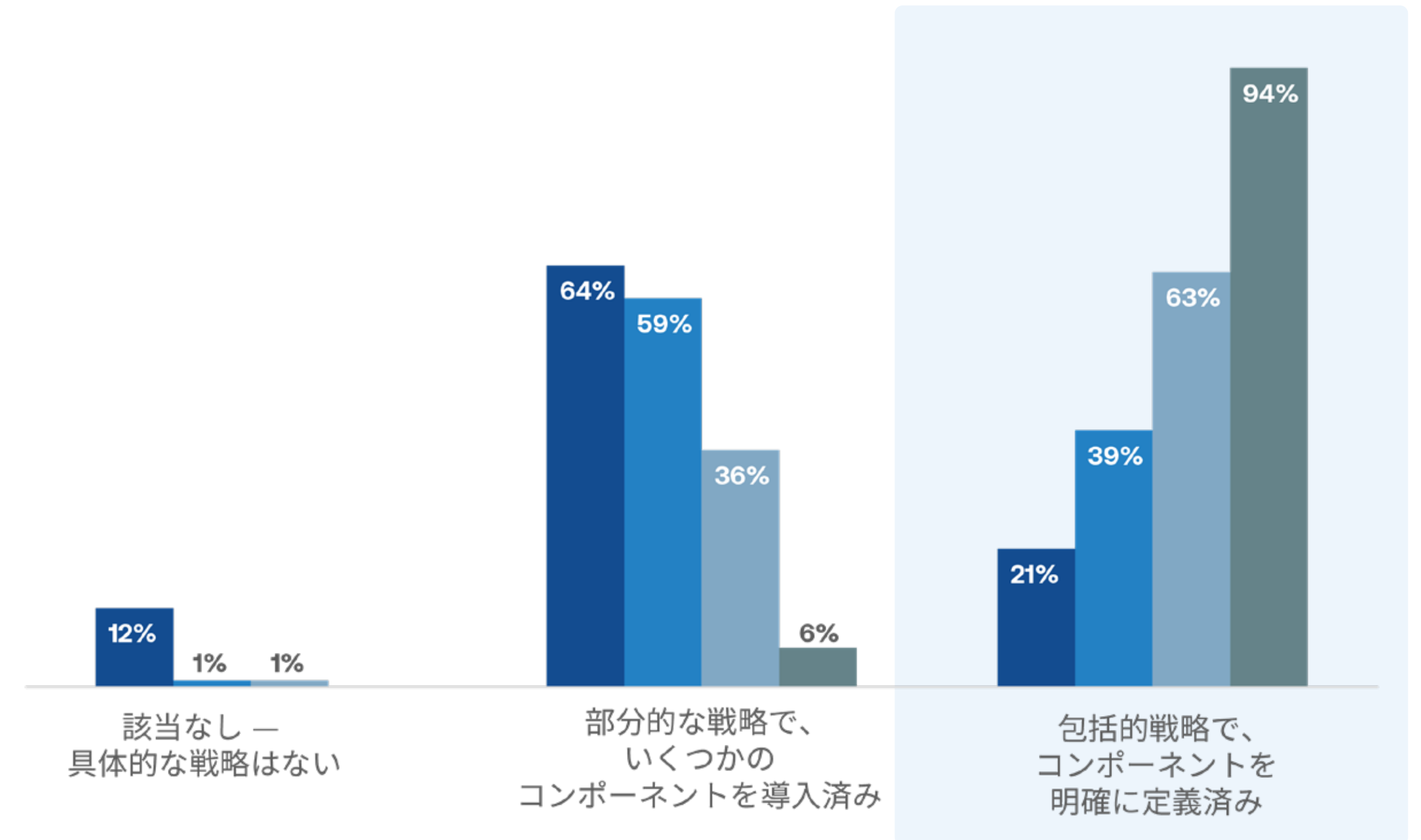
戦略的レベルと評価された組織の 94% は、明確に定義されたテクノロジーロードマップ、予算の見通し、経営幹部の承認を含む包括的なアイデンティティ戦略があると報告しています。対照的に、その他の組織で同様に報告している割合は、先進的組織では 63%、拡張中の組織では 39%、基礎レベルの組織ではわずか 21% にとどまります。

こうした戦略によって、アイデンティティの取り組みと包括的なビジネス目標との整合性が確保されます。

- 予算の見通しが明確であることによって、効果的なリソース配分が可能となり、重要なアイデンティティ能力に十分な資金が確保されます。
- 経営幹部の承認は、ステークホルダーの関与と部門を超えた協力関係を促進する上で役立ちます。また、組織の最高レベルで優先される包括的なビジネス戦略に対して、アイデンティティ戦略を整合させるためにも有用です。

明確に定義され、将来を見据えた、アイデンティティソリューション関連のテクノロジーロードマップを役立てることで、組織の将来のニーズに対して、導入したコントロールで確実に対応できるようになります。

### 貴社のアイデンティティ戦略はどれに該当しますか？

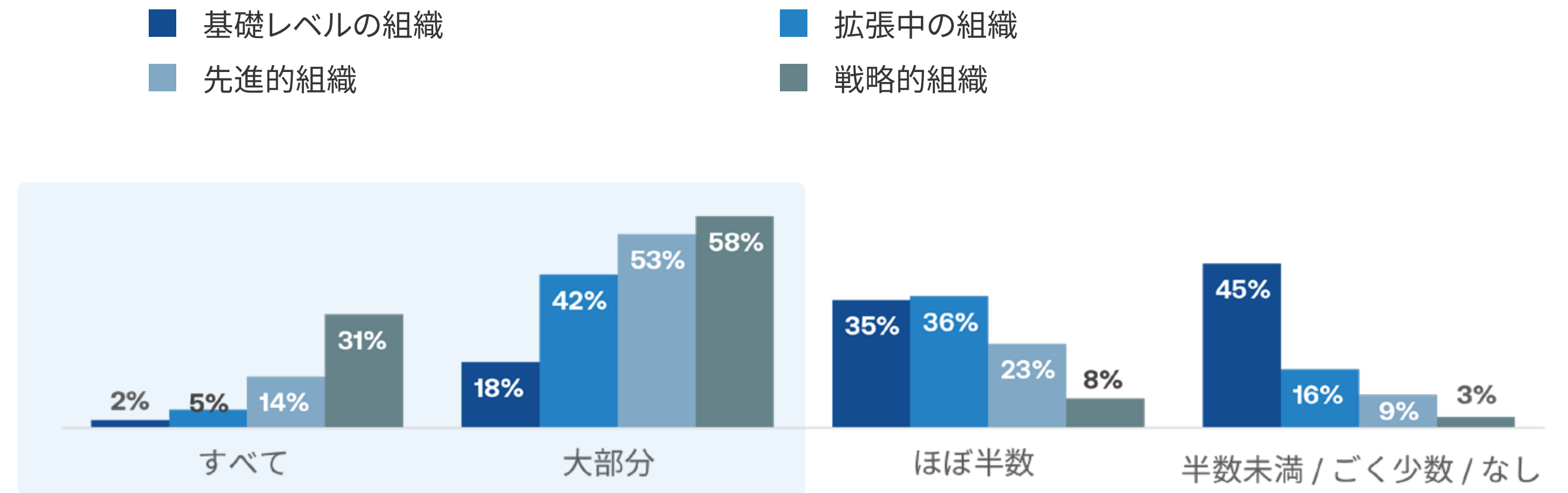


## 戦略的組織は、アイデンティティソリューションをより広範に、より深く導入している

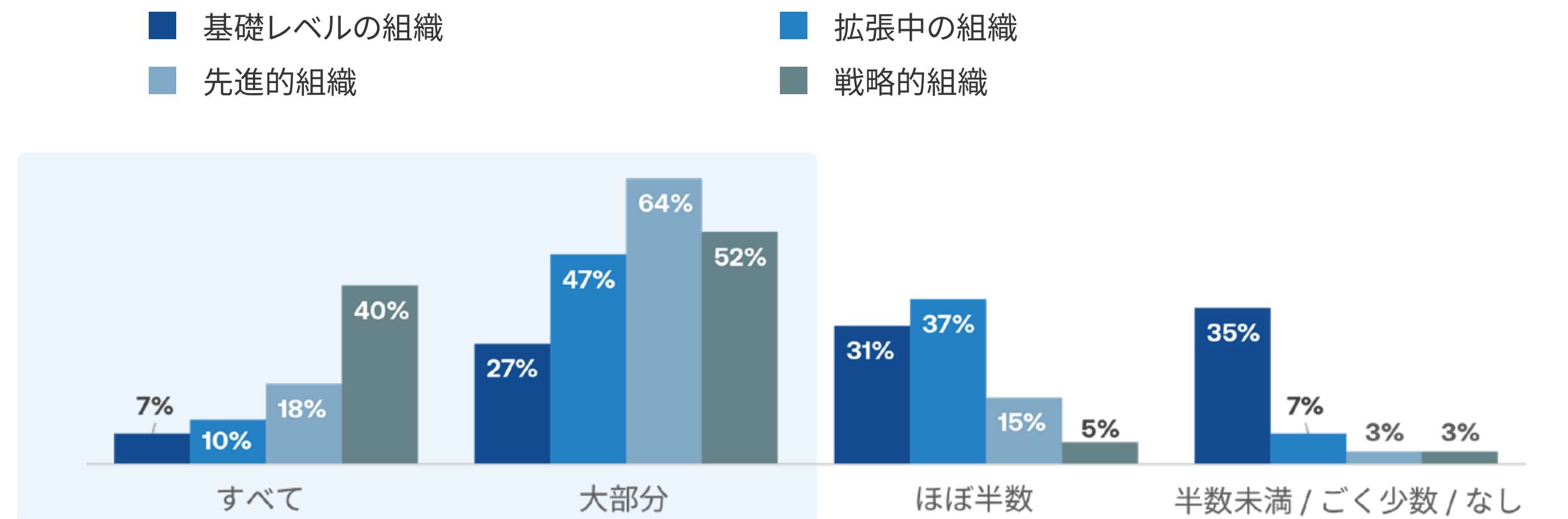
戦略的組織は、複数のアイデンティティ能力をより完全な形で採用している割合が、その他の組織と比べてはるかに高くなっています。たとえば、以下の状況が見られます。

- 戦略的組織の 89% は、ビジネスクリティカルなアプリケーションの大部分（または全部）に SSO 経由でアクセスできるようにしています。一方、基礎レベルの組織のうち、同様に回答した割合は 20% にとどまります。SSO は、ユーザーが単一セットの認証情報でアプリケーションにアクセスできるようにして、利便性と生産性を高めると同時に、不満の原因になる非効率的なパスワードリセットプロセスを最小限に抑えます。
- 戦略的企業の 92% は、ビジネスクリティカルなアプリケーションの全部（または大部分）を保護するために、MFA を導入しています。基礎レベルの組織のうち、同様に対応している割合はわずか 34% です。さらに、戦略的組織の 10 社中 9 社以上が、認証ソリューションにパスワードレス機能またはアダプティブ機能が含まれていると報告しています（基礎レベルの組織の場合は、約半数）。MFA は、複数の認証要素（パスワードと生体認証要素またはワンタイムコードなど）でユーザーを認証することで、不正アクセスのリスクを大幅に低減します。対象範囲を広げ、リスクレベルに応じて MFA 要件を適応させることができるため、戦略的企業はセキュリティ面で大きな優位性を得られます。
- 戦略的組織は、その他の組織と比べて、IGA（77%、基礎レベルの組織では 13%）と PAM ソリューション（61%、基礎レベルの組織では 10%）を採用する傾向がはるかに高くなっています。IGA と PAM はそれぞれ、ユーザーのアクセス権とアクセス許可の監視、特権ユーザーのアクセス制限と監視を提供することで、組織を内部脅威と外部脅威の両方から保護すると同時に、規制コンプライアンスを支援します。

SSO 経由でアクセス可能なビジネスクリティカルなアプリケーションの割合。



MFA により保護されるビジネスクリティカルなアプリケーションの割合。

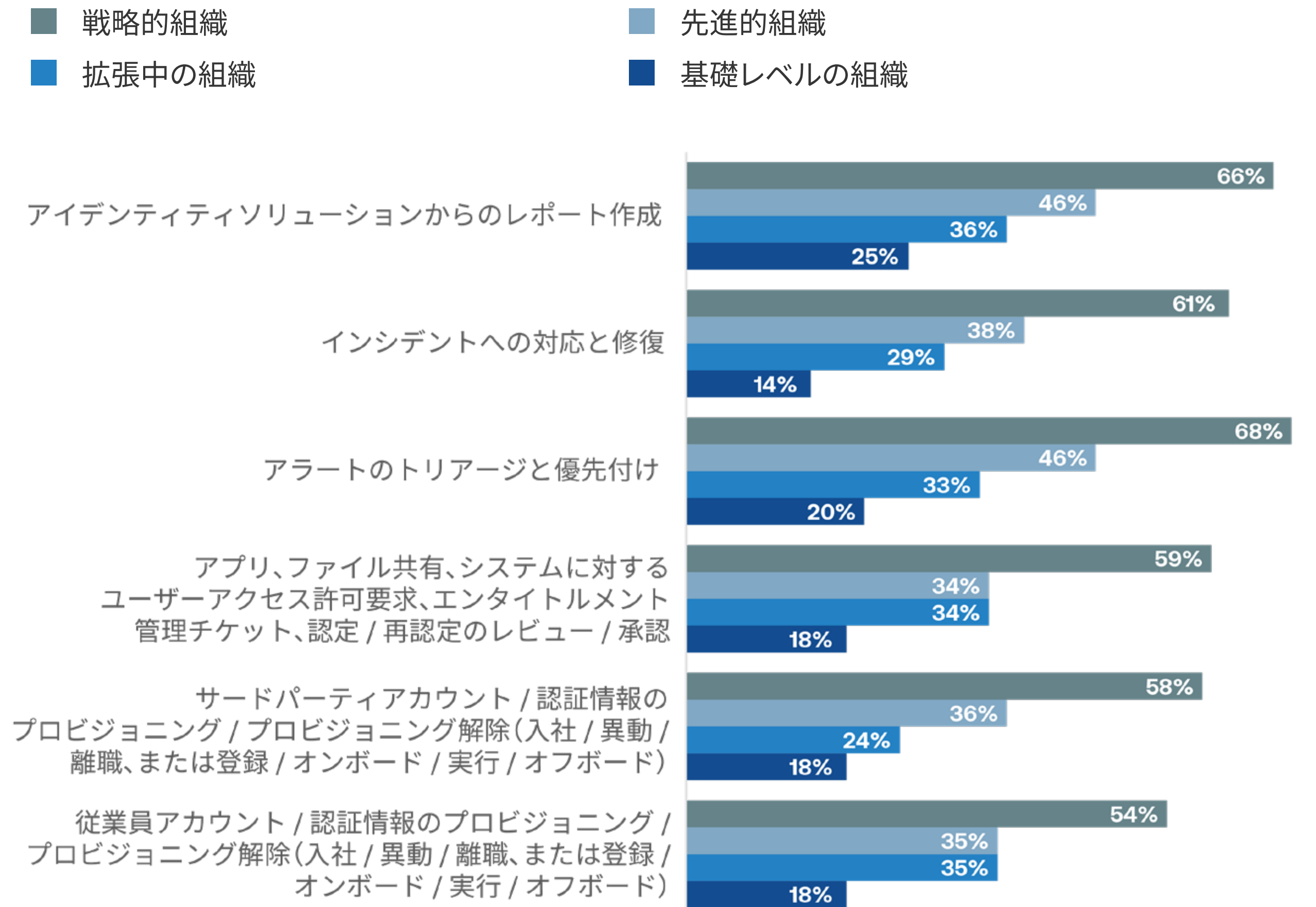



## 戦略的組織は、エコシステムの統合とインテリジェントな自動化に重点を置いている

戦略的組織は、統合の容易さとワークフローの自動化を重視し、効率性を高め、人為的ミスリスクを低減するアイデンティティのアプローチを採用する傾向があります。

- 戦略的組織の91%は、多様なディレクトリサービスを完全に連携させています(基礎レベルの組織では20%)。アイデンティティのリポジトリをこのように相互接続することで、異種のシステムやプラットフォームにわたってシームレスかつ安全な認証と認可が可能になります。
- 戦略的組織は、さまざまなビジネスアプリケーションに対する事前構築済みコネクタを含み、迅速で簡単な統合を実現するアイデンティティソリューションに投資する傾向があります。たとえば、94%が主要IAMソリューションで、コラボレーションツールへのコネクタをベンダーから提供されていると回答し、93%がCRMソリューションへのコネクタがあると回答しています。また、また、財務(88%)や人事(92%)のバックオフィスアプリについても、同様の割合でこうしたコネクタがあると報告しています。
- 戦略的組織では、レポートの作成(66%、基礎レベルの組織では25%)、アイデンティティ関連インシデントへの対応(61%、基礎レベルの組織では14%)、アイデンティティ関連アラートのトリアージ(68%、基礎レベルの組織では20%)のような一般的なアイデンティティ関連タスクの自動化率ははるかに高くなっています。このように自動化を推進することで、戦略的企業は成長する環境に対処し、環境(オンプレミスかクラウドか)やユーザーの場所(オフィスかリモートか)に関係なく一貫性を維持できます。

社内のアイデンティティ関連の各ワークフローが高度に自動化されていると答えた回答者の割合。



A person is shown from the side, looking at a laptop screen. The screen displays a security interface with a profile picture, a lock icon, and the number 26417. In the foreground, a mobile device is held, displaying a login screen with the number 264172. The background is a blurred office setting.

ワークフォースアイデンティティへの  
成熟したアプローチがもたらす直接的影響

## 戦略的組織は、アイデンティティソリューションがビジネスを促進すると考える

調査では、自社のアイデンティティソリューションがさまざまな業務にどのような影響を及ぼしているかを回答者に尋ねました。回答の選択肢は、自社のアイデンティティソリューションが、俊敏性、コンプライアンスの取り組み、コラボレーション、エンドユーザーエクスペリエンス、リモートワークなどを促進しているか、影響を与えていないか、または妨げているかです。

この質問に対する回答に成熟度モデルを適用すると、すべての組織がアイデンティティソリューションによるビジネスへの効果と同じレベルで得ているわけではないことが明らかになります。戦略的組織では、基礎レベルの組織に比べて、自社のソリューションがビジネスを大きく促進していると回答する割合が非常に高くなっています。

### 3.9 倍

自社のソリューションが俊敏性を強力に促進していると回答した戦略的組織の割合  
(59%、基礎レベルの組織では 15%)

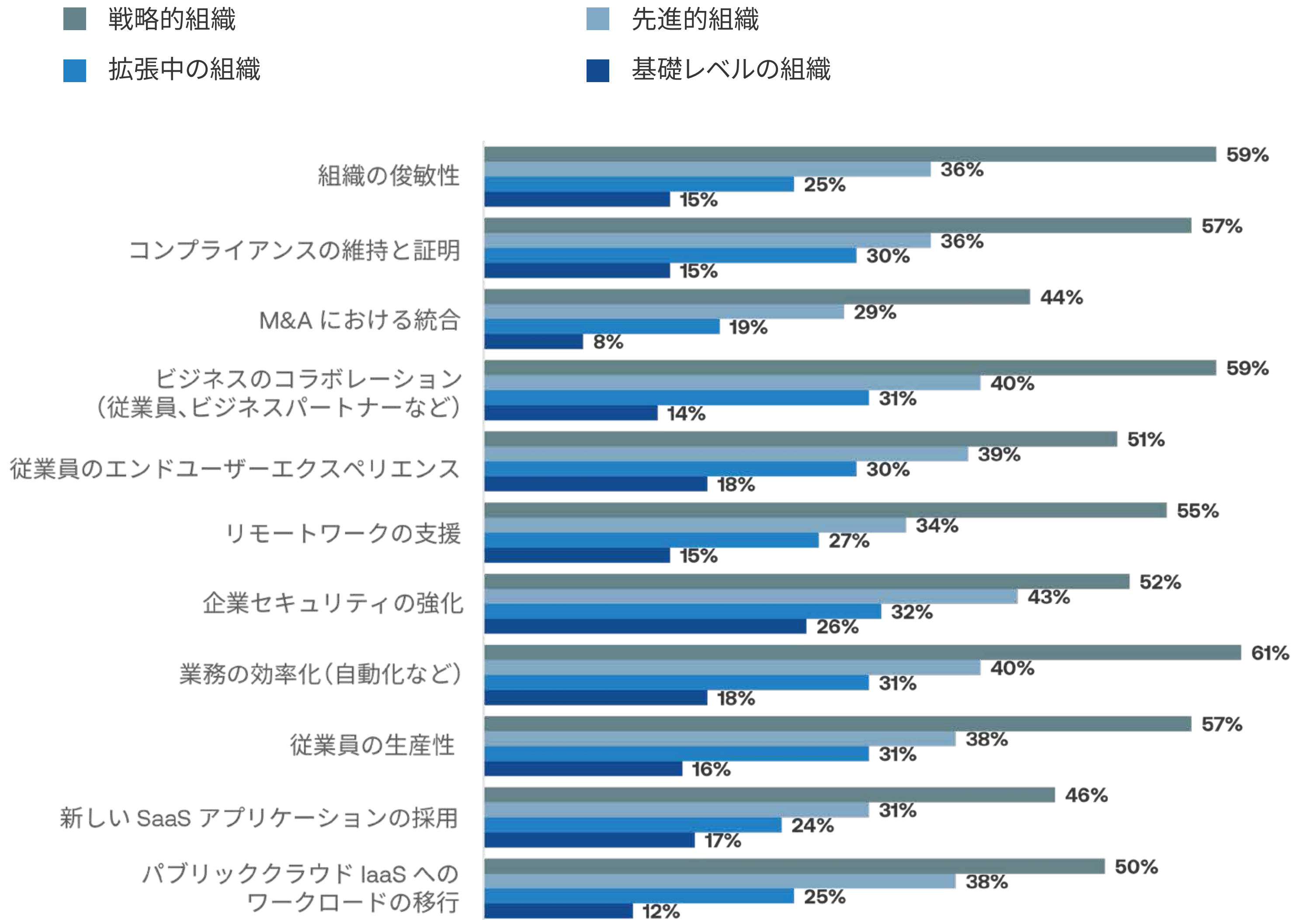
### 4.2 倍

自社のソリューションがコラボレーションを強力に促進していると回答した戦略的組織の割合  
(59%、基礎レベルの組織では 14%)

### 3.6 倍

自社のソリューションが生産性を強力に促進していると回答した戦略的組織の割合  
(57%、基礎レベルの組織では 16%)

アイデンティティソリューションが自社のビジネスの各領域を大きく促進していると考える回答者の割合。



## 戦略的組織は、アイデンティティへのアプローチがセキュリティを強化すると考える

ビジネスの促進で戦略的組織が優位性を達成している状況が、データから明らかになりました。調査ではさらに、アイデンティティへのアプローチとサイバーセキュリティオペレーションとの関係について、回答者に尋ねました。回答の選択肢は、自社のアイデンティティ戦略が、インシデント対応、脅威の検知と緩和などのタスク、さらにはゼロトラスト戦略の採用を支援しているか、影響を与えていないか、または妨げているかです。

ビジネスの促進と同様に、ここでも戦略的組織の優位性は明らかです。戦略的組織では、基礎レベルの組織に比べて、自社のソリューションがセキュリティチームを大きく支援していると回答する割合が非常に高くなっています。

### 3.4 倍

アイデンティティに対する自社のアプローチがゼロトラストへの移行に大きく役立っていると回答した戦略的組織の割合 (61%、基礎レベルの組織では 18%)

### 3.4 倍

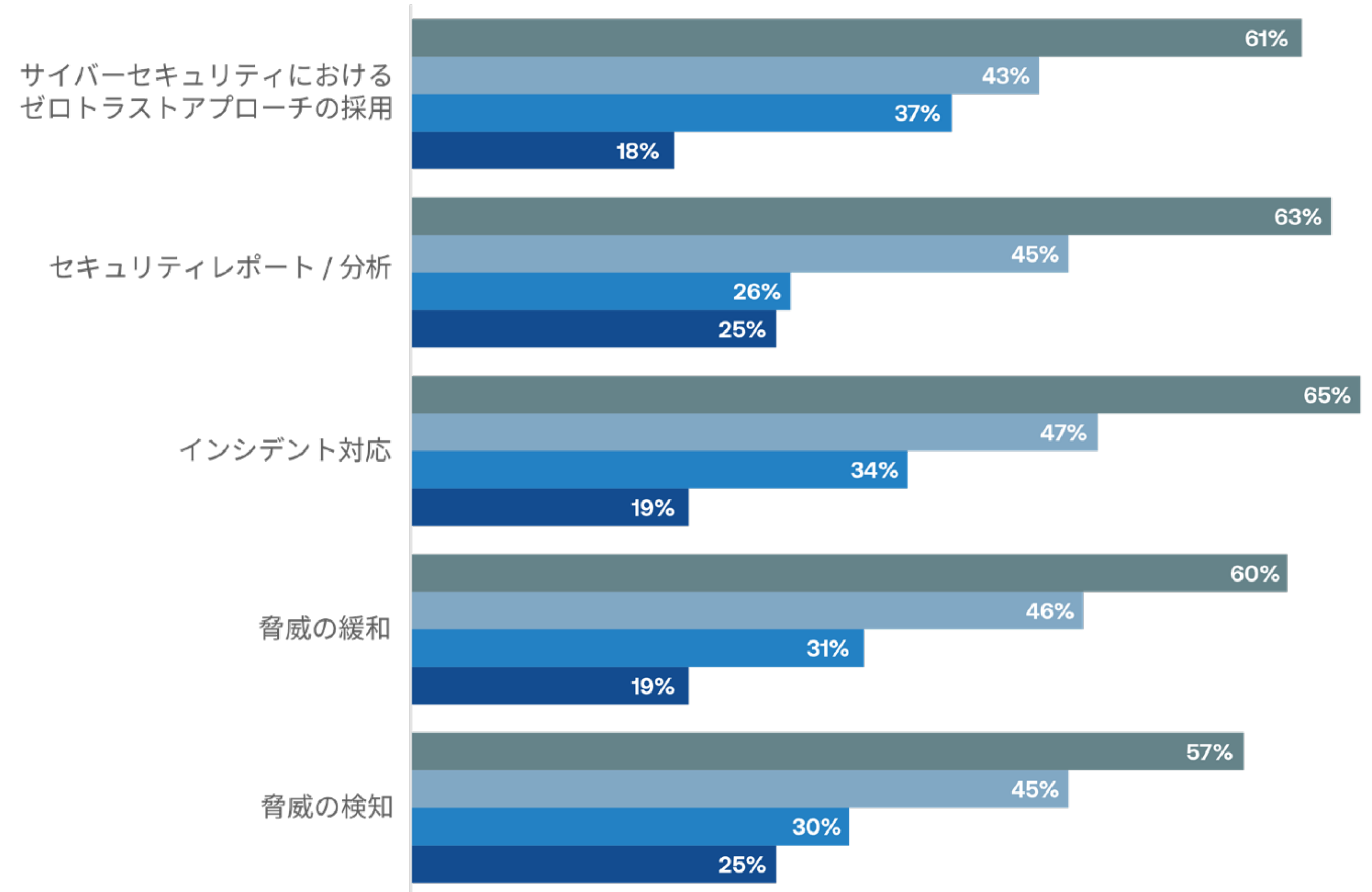
アイデンティティに対する自社のアプローチがインシデント対応に大きく役立っていると回答した戦略的組織の割合 (65%、基礎レベルの組織では 19%)

### 3.2 倍

アイデンティティに対する自社のアプローチが脅威の緩和に大きく役立っていると回答した戦略的組織の割合 (60%、基礎レベルの組織では 19%)

アイデンティティソリューションがセキュリティオペレーションの各領域で大きく役立っていると考える回答者の割合。

- 戦略的組織
- 先進的組織
- 拡張中の組織
- 基礎レベルの組織



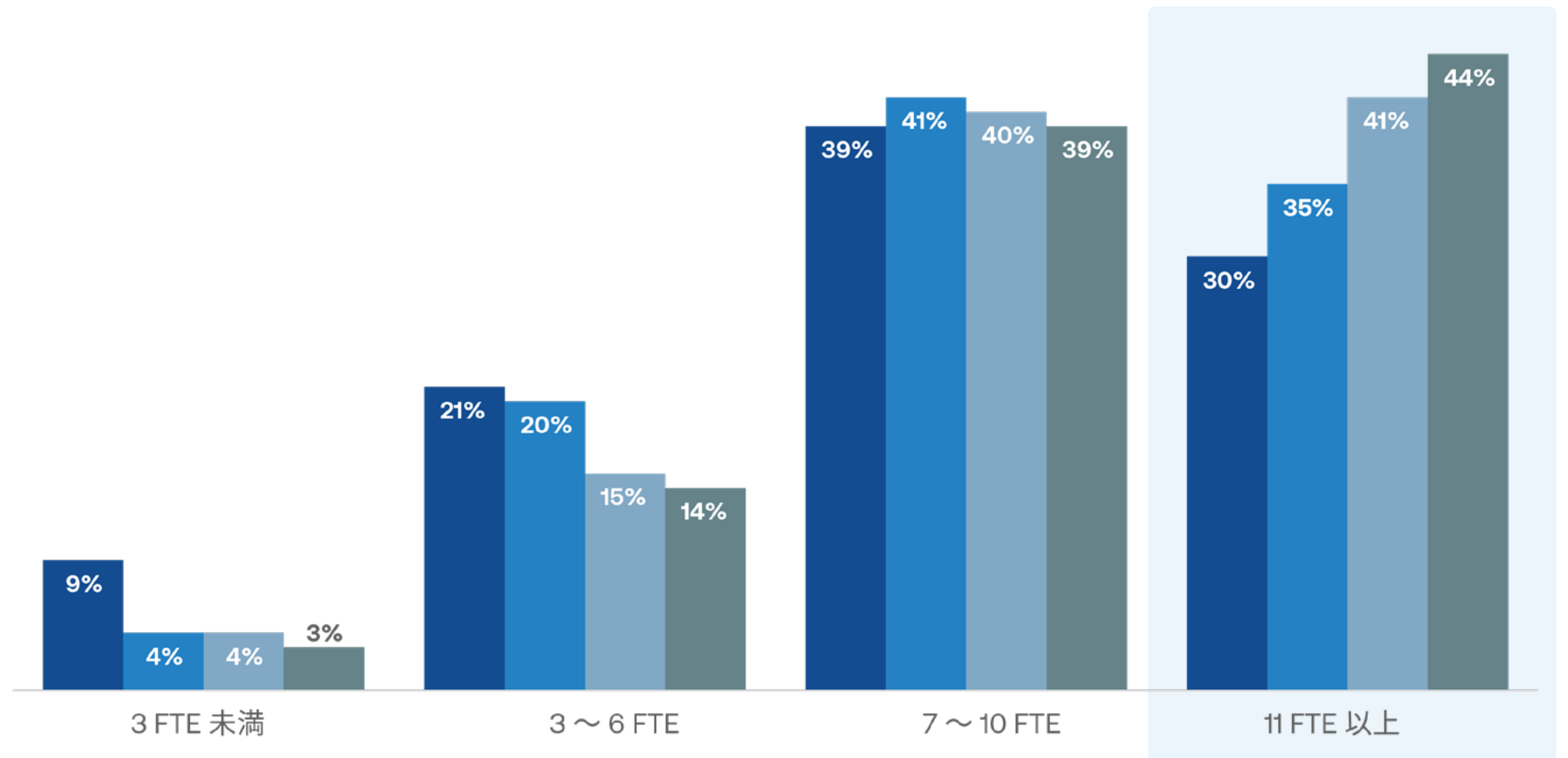
## 戦略的組織はオペレーションを大幅に効率化している

過去 24 か月間に投資したアイデンティティソリューションによって、どの程度の効率化を実現したかを回答者に尋ねました。具体的には、セキュリティの効率化、IT オペレーション、エンドユーザーの生産性といった領域での改善について評価してもらいました。

全体としては、ほとんどの組織が実質的なメリットがあると報告しています。90% が、投資によって 3 FTE（フルタイム従業員 3 人分）以上を削減できたの見積もっています。しかし、ここでも戦略的組織が最も大きな成果を上げており、多くが最近のアイデンティティ関連投資によって 11 FTE 以上を削減できたと報告しています。

過去 24 か月間に行われたアイデンティティ関連の投資によって、どの程度の FTE（フルタイム当量：フルタイム従業員数で換算した仕事量）を削減できましたか？

- 基礎レベルの組織
- 拡張中の組織
- 先進的組織
- 戦略的組織





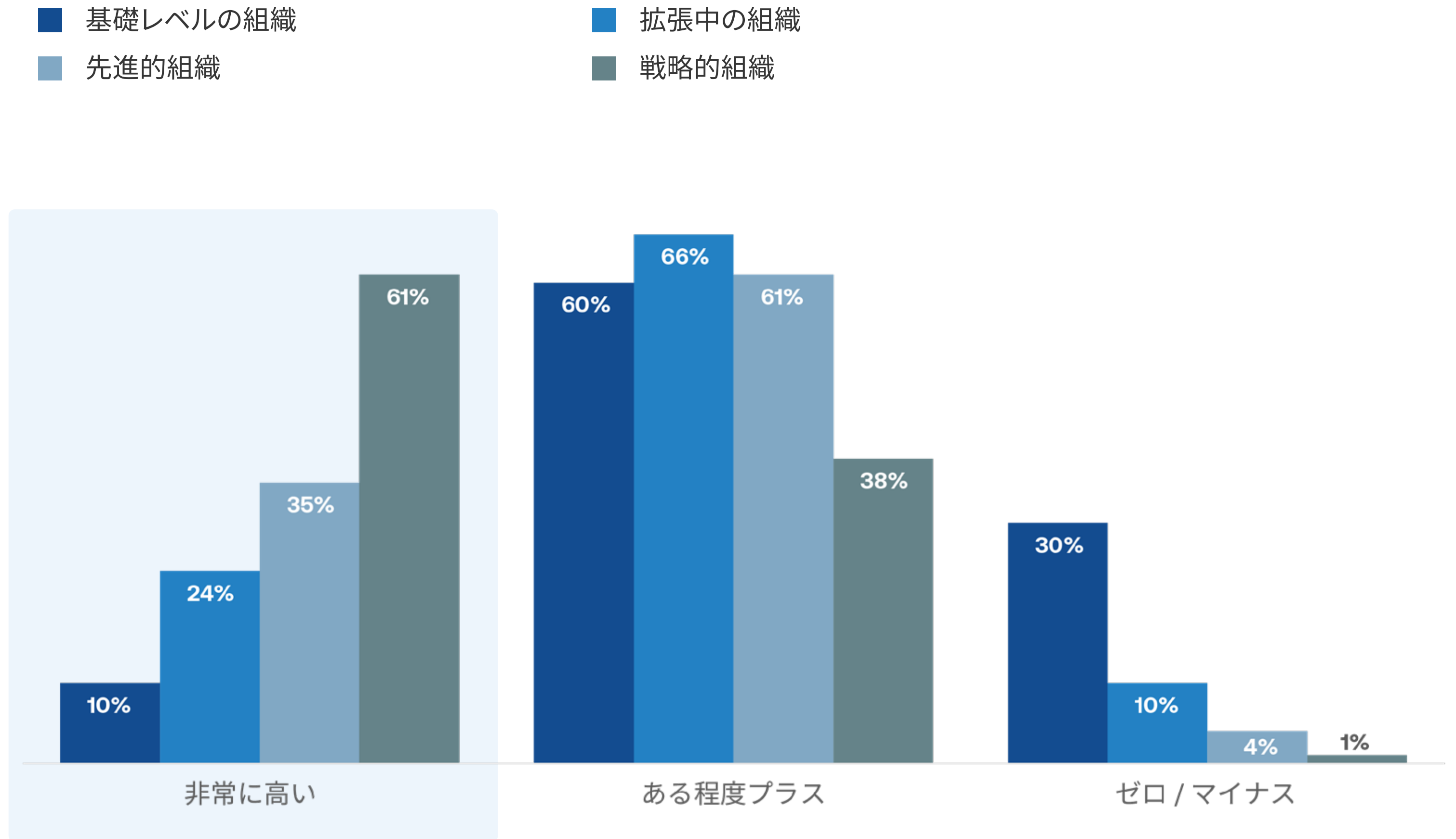
# 6.1 倍

基礎レベルの組織と比べて、アイデンティティ投資の ROI が非常に高い戦略的組織の割合は 6.1 倍に上る。

## 戦略的組織は、アイデンティティソリューションの ROI が顕著に高い

最後に、過去数年間に投資したアイデンティティ関連ソリューションの ROI の評価を回答者に求めました。全回答者の 86% が、アイデンティティソリューションについてプラスの投資回収率を実現していると回答しています。しかし、これまでに紹介したデータを踏まえると、ROI が「非常に高い」と報告する割合が戦略的組織で大幅に高くなっているのも当然であると言えます。実際に、基礎レベルの組織と比べて、アイデンティティ投資の ROI が非常に高いと回答した戦略的組織の割合は 6.1 倍に上ります。

最近のアイデンティティ関連ソリューションの ROI をどのように評価しますか？





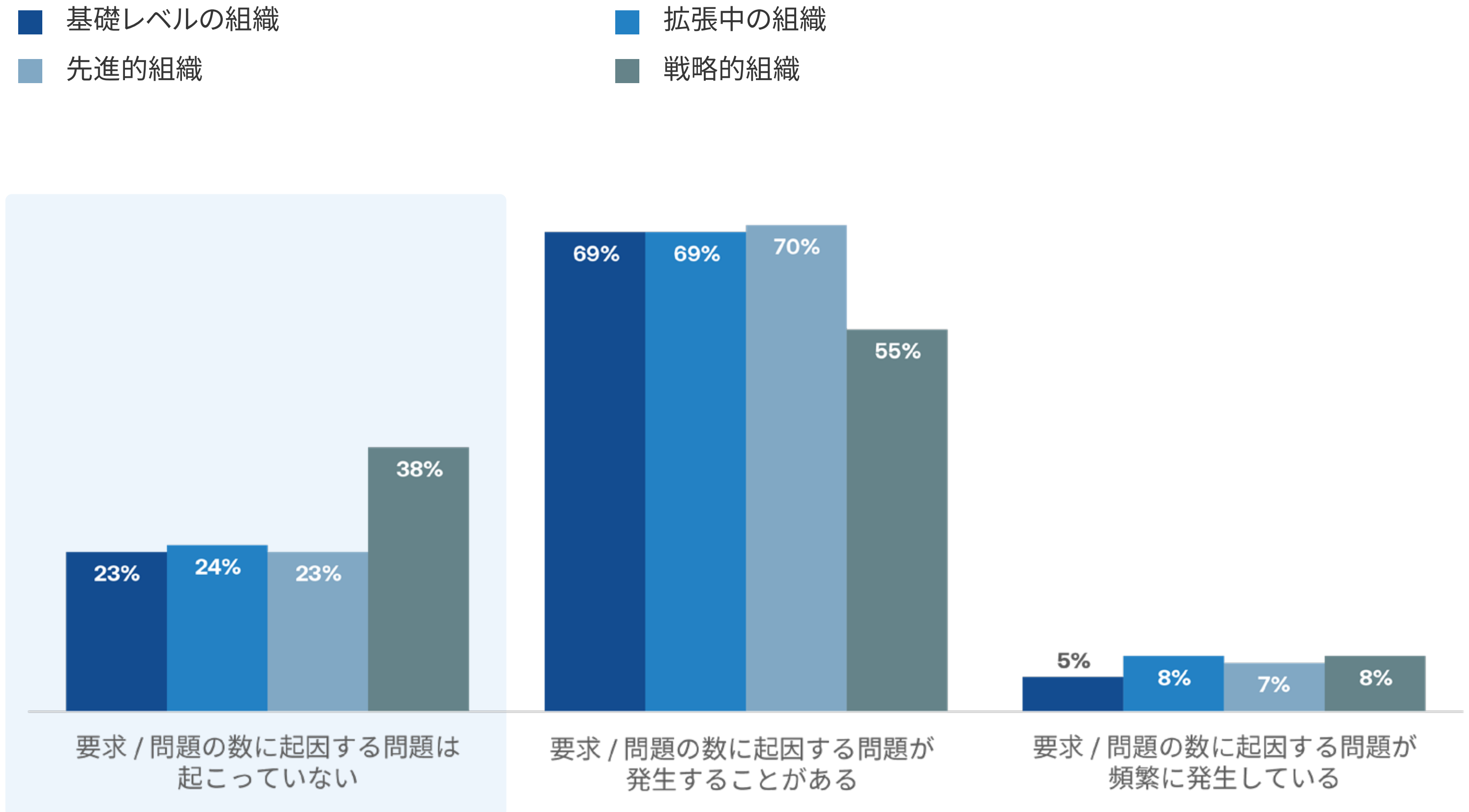
ワークフォースアイデンティティの  
成熟度のリーダーが実現しているその他の成果

## 戦略的組織では、 アイデンティティ管理チームが より効果的に要求に対応できる

前のセクションで述べたように、戦略的組織はその他の成熟度の低い組織と比べて、アイデンティティソリューションが直接的に価値を創出していると評価する割合が高くなっています。本調査では、業務のさまざまな側面についてさらに尋ねました。これらの質問への回答に見られる相関関係は、アイデンティティに対するより成熟したアプローチに合致する機能を優先的に導入すべきであることを裏付けるものとなっています。

エンドユーザーからのアイデンティティ関連の要求/問題の対応数について回答者に尋ねました。戦略的組織の間では、要求数に起因する問題は起こっていないとの回答が多く見られました。エンドユーザーからの要求への対応は、重要な能力です。機敏なアイデンティティチームは、エンドユーザーからの要求に迅速に対応するので、ユーザーの満足度と生産性が高まります。

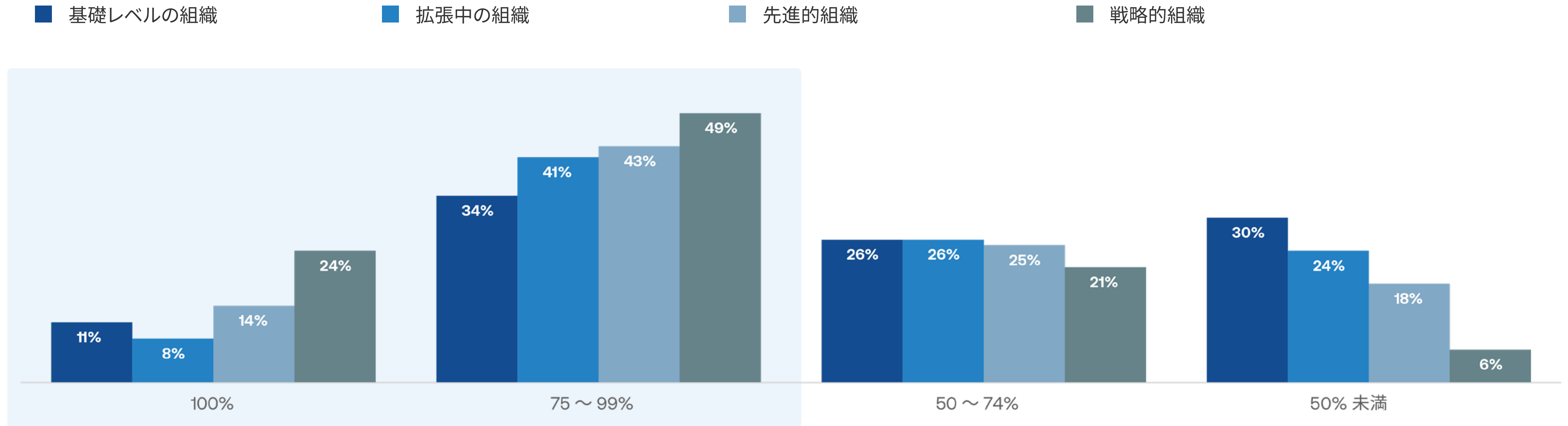
アイデンティティ関連の要求 / 問題の数に起因する問題が管理側で発生する頻度。



## 戦略的組織は、セキュリティアラートにより簡単に対応できる

このデータは、ワークフォースアイデンティティの成熟度に比例して、セキュリティアラートへの対応能力が高くなることも明らかに示しています。自社のセキュリティコントロールによるアイデンティティ関連アラートとして、担当者がトリアージして調査できる数について回答者に尋ねました。戦略的組織では、自社の環境で発生したアラートの75%以上をトリアージして対応していると回答する割合がより高くなっています(73%、基礎レベルの組織では45%)。逆に言えば、基礎レベルの組織では、アラート疲れと誤検知の多さによって、アラートの大半を調査しない割合が高くなっています(30%、戦略的組織では6%)。

アイデンティティ関連で発生するセキュリティアラートのうち、実際にトリアージして対応している割合。



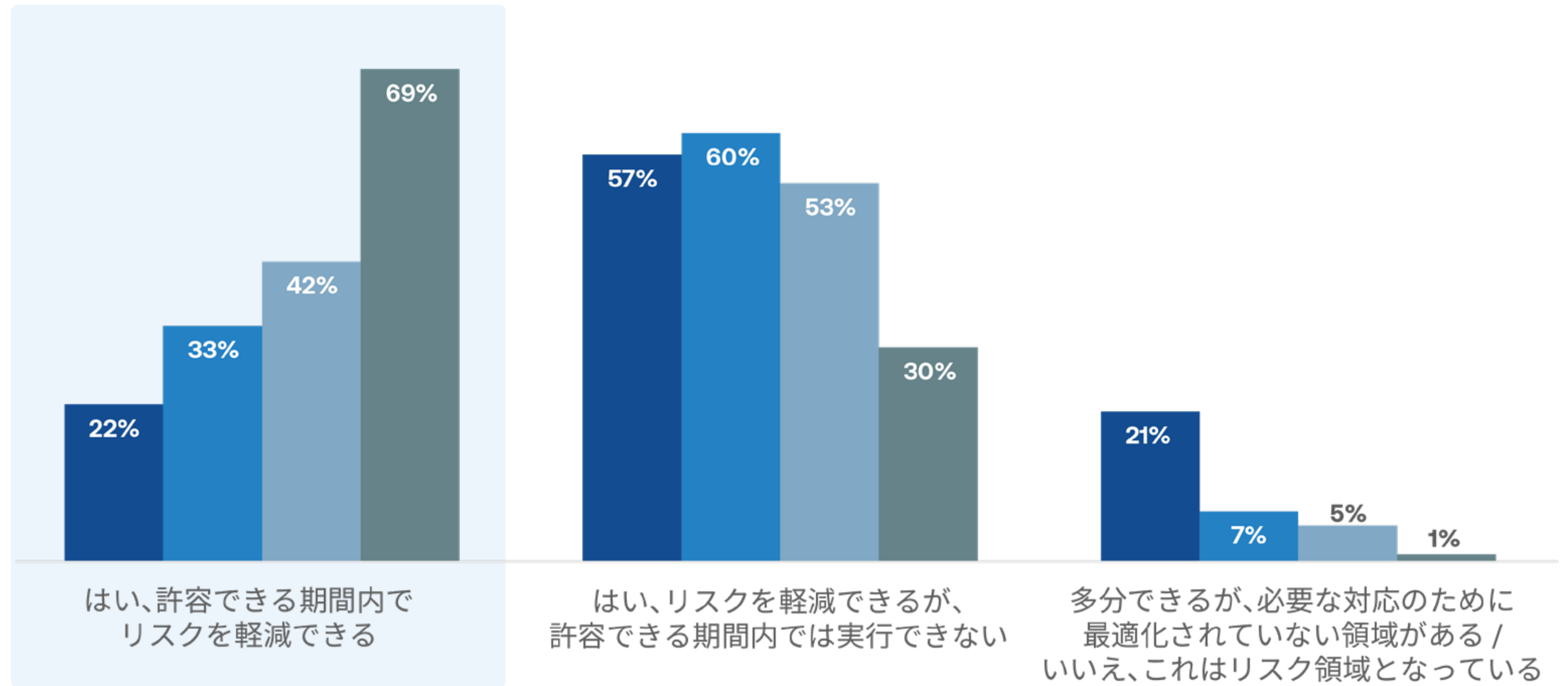
## 戦略的組織は、 アイデンティティ関連リスクへの対応の 俊敏性がより高い


最後の質問として、機密データに影響を及ぼすワークフォースアイデンティティ関連の重大インシデント / 攻撃に気づいた状況を仮定し、リスクを軽減するための人材、スキル、プロセス、テクノロジーが自社にあると感じるかどうかを回答者に尋ねました。

戦略的組織は、自社の能力に対して相対的に大きな自信を持っており、69% が許容できる期間内で効果的にリスクを軽減できると考えています（基礎レベルの組織の 3.1 倍）。

貴社では、アイデンティティ関連の重大インシデントを俊敏に緩和できますか？

- 基礎レベルの組織
- 拡張中の組織
- 先進的組織
- 戦略的組織





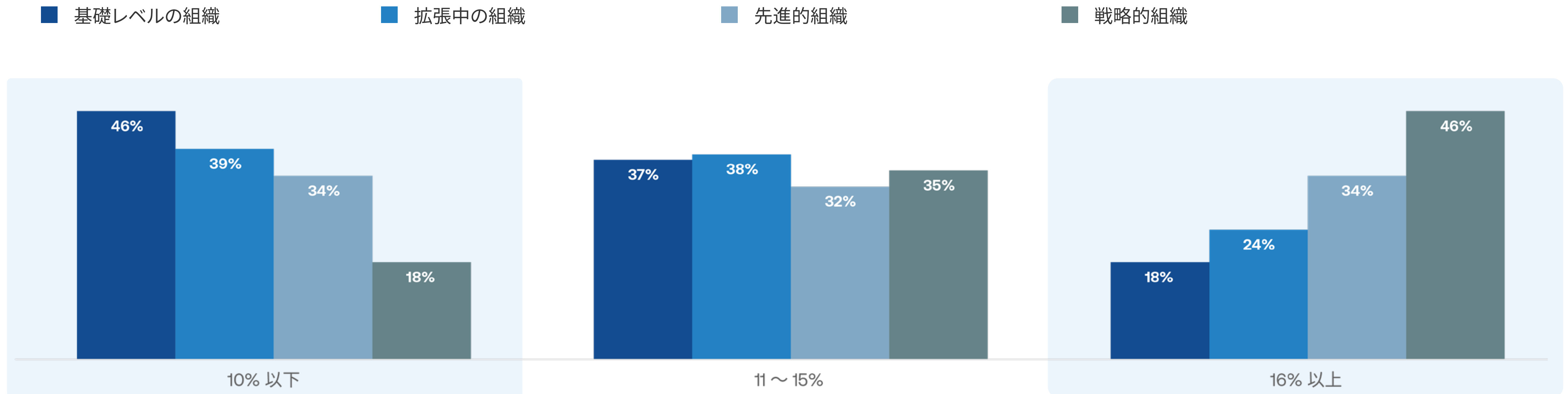
**成熟度の高い組織に学ぶ**

## 戦略的組織は、 アイデンティティソリューションに より多くの予算を割り当てている

成熟度モデルで提唱される具体的な行動やベストプラクティス以外でも、成熟度の高い戦略的組織とそれ以外の組織の間に重要な違いがいくつかあることが、本調査で明らかになりました。

本調査では、年間ITテクノロジー予算（従業員の給与を除く）のうち、アイデンティティソリューションにどの程度割り当てているかを回答者に尋ねました。戦略的組織では平均して、IT予算に占めるアイデンティティツールの割合が、基礎レベルの組織よりも47%近く多くなっています（16%、基礎レベルの組織では10.9%）。

ITテクノロジー予算に占めるアイデンティティソリューションの割合。



# 「戦略的組織では、 基礎レベルの組織と比較して、 6部門中5部門で 責任者が関与している割合が高い」

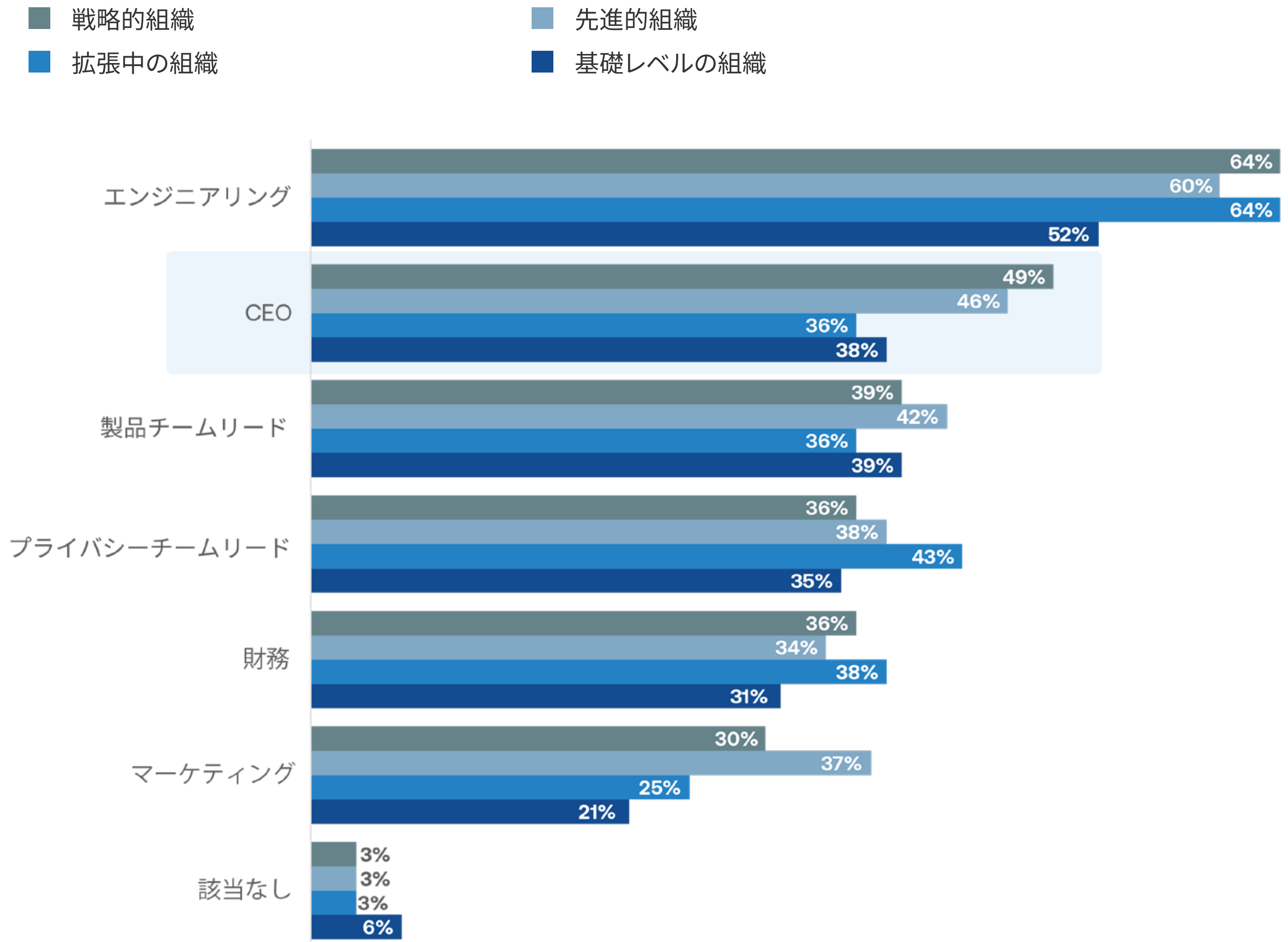
## 戦略的組織では、 経営幹部の関与度が高い

経営幹部の関与も、その他の組織と比較した戦略的組織の差別化要因です。IT / セキュリティ部門以外で、アイデンティティ戦略の策定と実行に積極的に関与している部門責任者について回答者に尋ねました。

データにはいくつかの違いが見られますが、最も注目すべき点は、戦略的組織ではCEOの49%が関与しているのに対して、基礎レベルの組織ではCEOが関与する割合が38%にとどまっていることです。実際に、戦略的組織では、6部門中5部門で責任者が関与していると回答する割合が、基礎レベルの組織よりも高くなっています。

予算を確保し、ポリシーやベストプラクティスを全社的に確実に浸透させるには、経営幹部が高いレベルで関与することが有効です。

アイデンティティ戦略に積極的に関与しているのは、どの部門のリーダーですか？



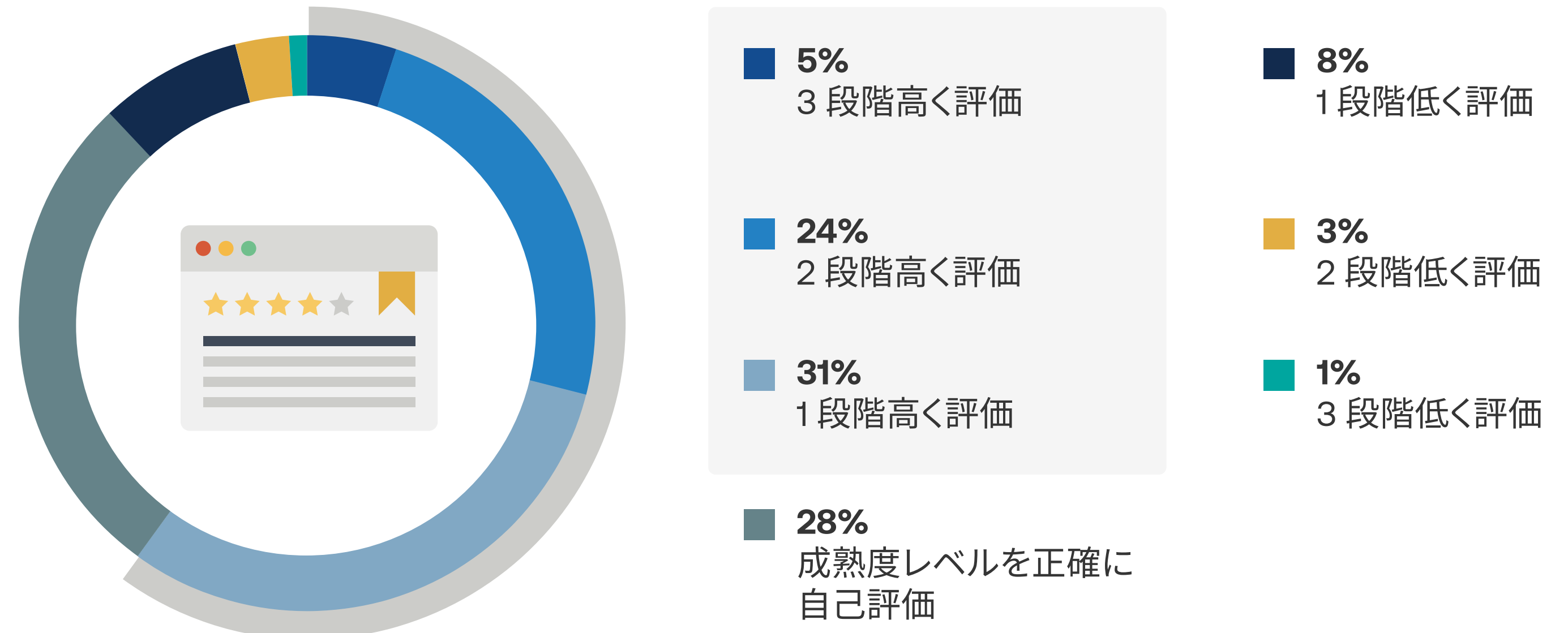


## 組織の評価では客観性が重要となる

本調査には、組織が自社のアイデンティティ能力を過大評価する傾向があることが示されています。回答者には、自社のアイデンティティの成熟度を主観的に自己評価してもらいました（「成熟度が非常に高い」から「成熟度が非常に低い」までの4段階評価）。この自己評価と、成熟度モデルからのアウトプットをEnterprise Strategy Groupが比較したところ、成熟度モデルよりも高く自己評価している組織が60%に上ることが明らかになりました。

こうしたバイアスがあるため、歪んだ意思決定や欠陥のある戦略を客観的な評価によって緩和することの重要性を理解できます。

組織が自社の成熟度を過大評価する傾向を可視化。



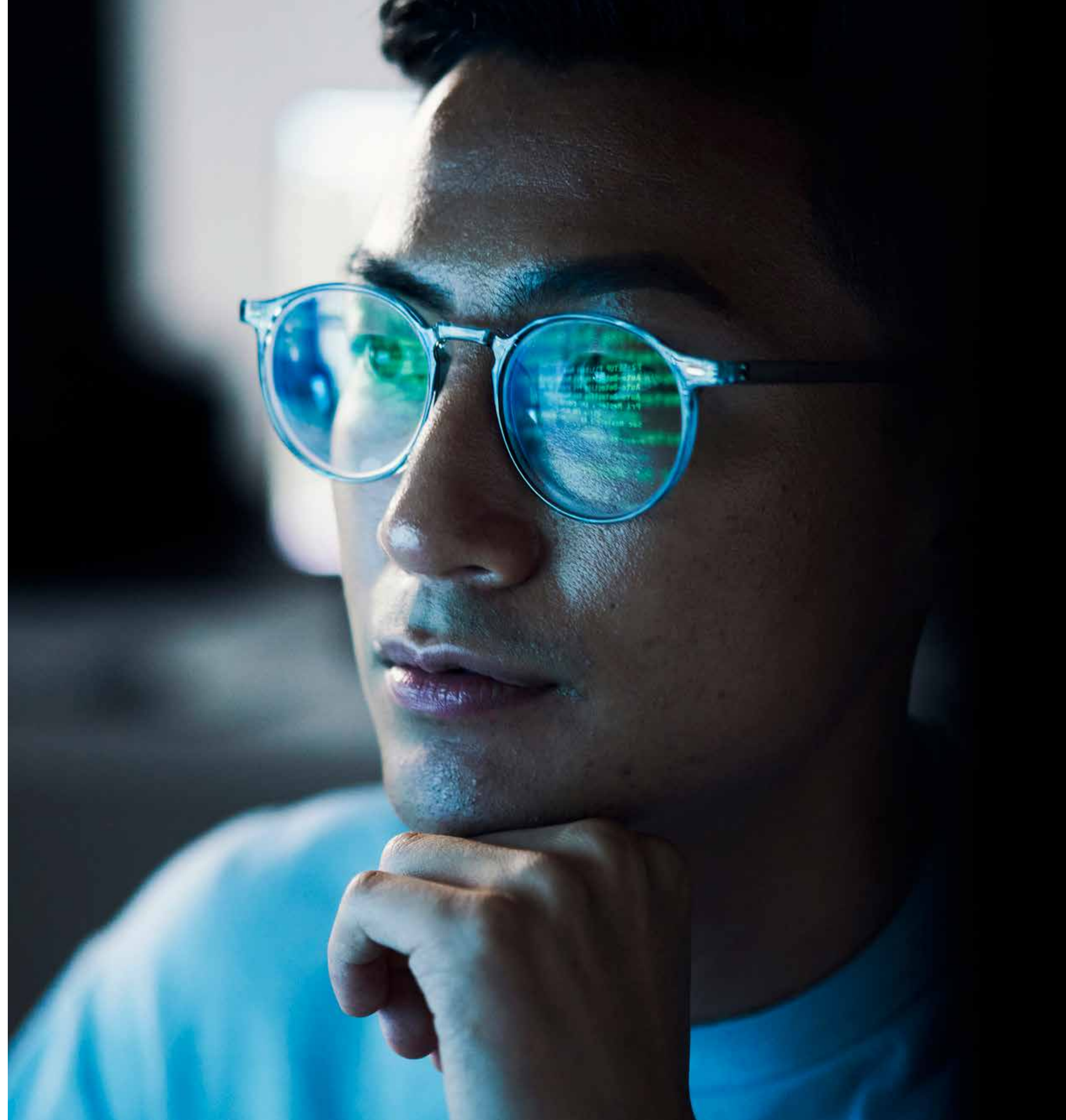
「この自己評価と、成熟度モデルからのアウトプットをEnterprise Strategy Groupが比較したところ、**成熟度モデルよりも高く自己評価している組織が60%に上ることが明らかになった**」



## Okta の活用方法

Okta Workforce Identity Cloud は、利便性と安全性の高いアクセスを提供して、ワークフォースがコスト削減や顧客サービス向上などの戦略的優先事項に集中できるようにします。

[詳しく見る](#)



### 調査方法と回答者内訳

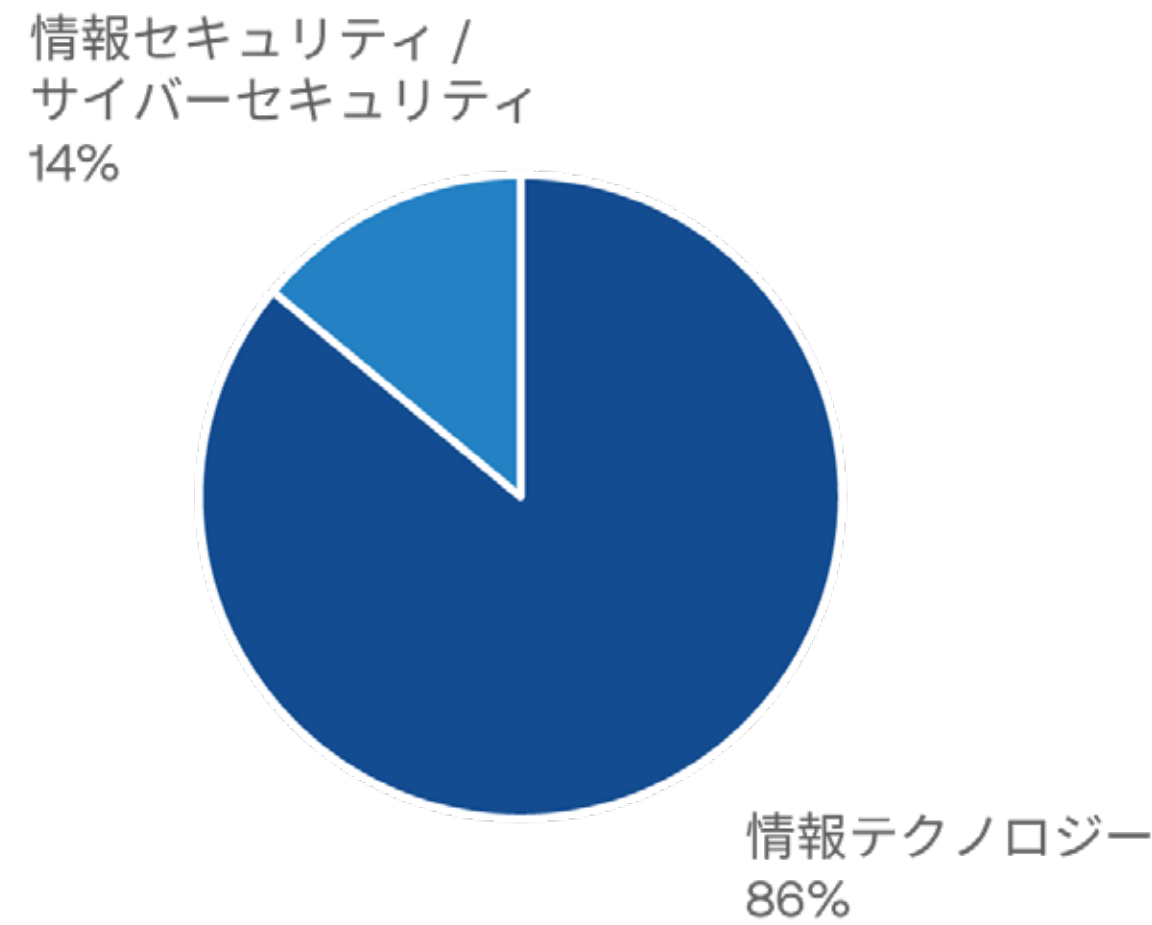
Enterprise Strategy Group は、本レポートのデータを収集するため、組織のアイデンティティ関連のテクノロジー投資 (IAM、MFA、SSO など) に責任 / 影響力を持つ IT / セキュリティ部門の担当者 / 意思決定者 600 人を対象に、包括的なオンライン調査を実施しました。

北米 (米国、カナダ：回答者の 50%)、西ヨーロッパ (英国、ドイツ：同 26%)、アジア (オーストラリア、ニュージーランド、シンガポール：同 25%) の官民全業種の組織が対象となりました。調査は、2023 年 11 月 13 日から 11 月 29 日の期間中に実施されました。

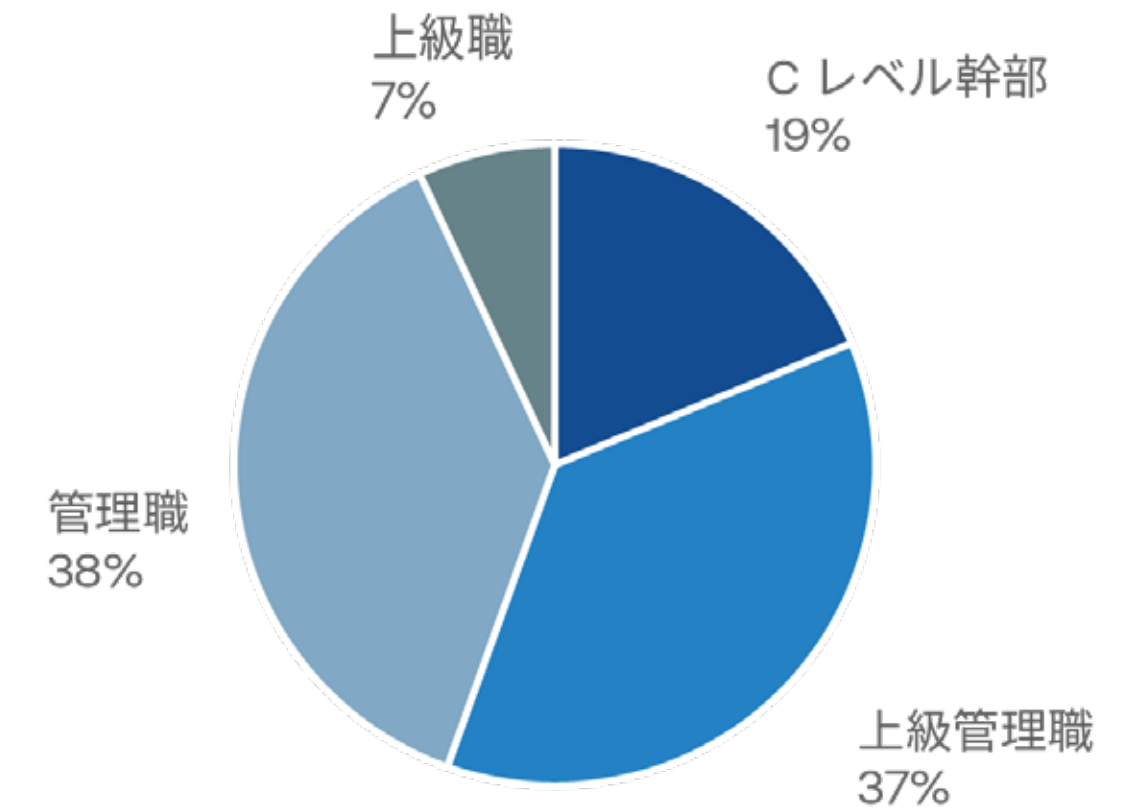
このサンプルサイズの 95% 信頼区間では、誤差が ± 4% ポイントとなります。

備考：本レポートでは、図表の数値を四捨五入しているため、合計値が 100% にならない場合があります。

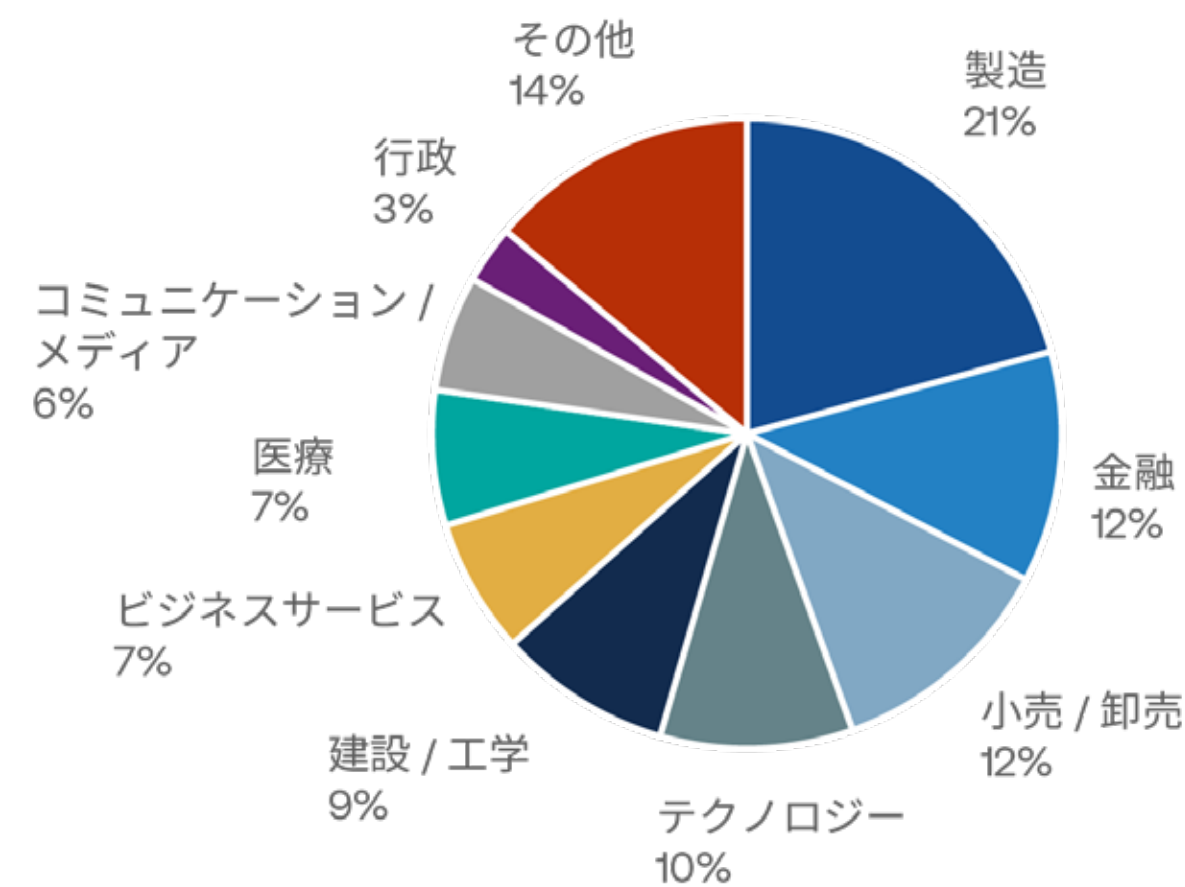
職種別の回答者数。  
(回答者の割合、n=600)



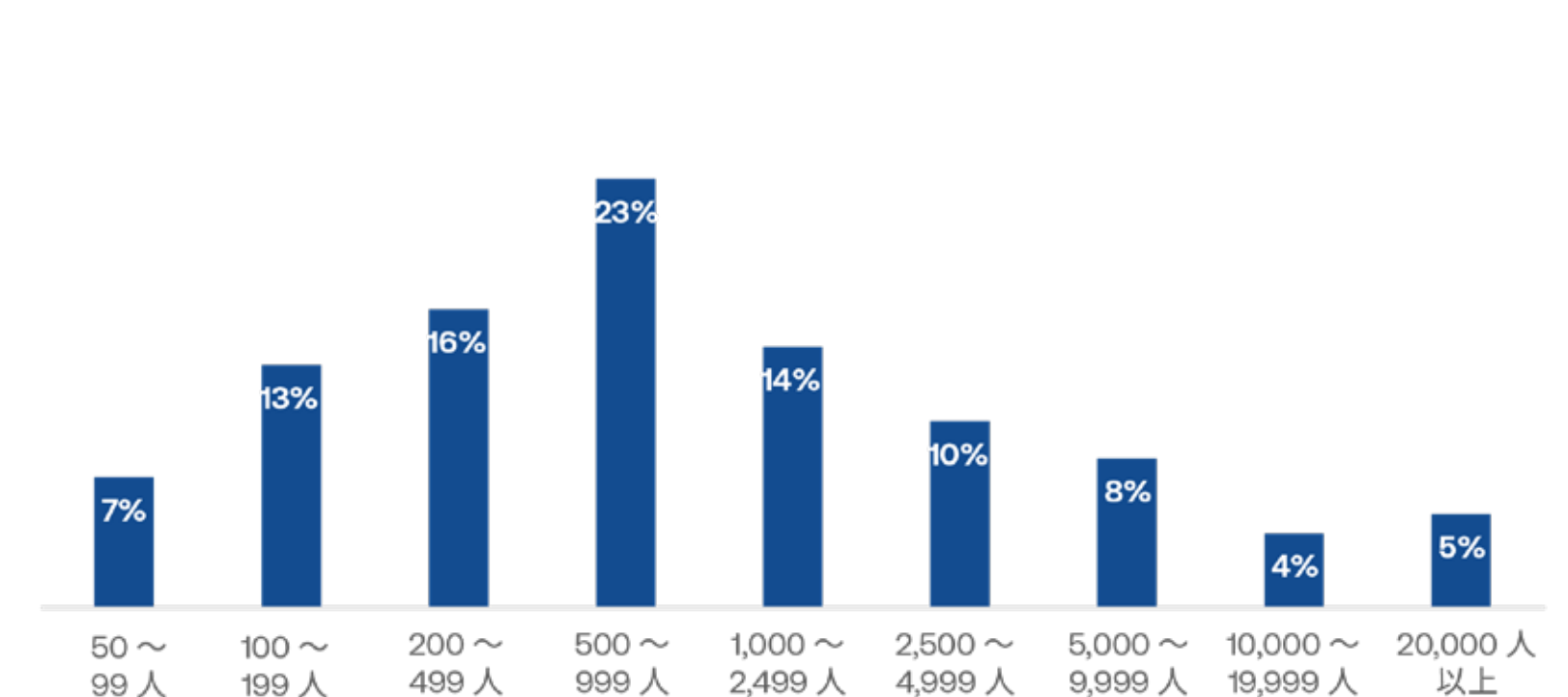
職位別の回答者数。  
(回答者の割合、n=600)



業種別の回答者数。  
(回答者の割合、n=600)



組織規模 (従業員数) 別の回答者数  
(回答者の割合、n=600)



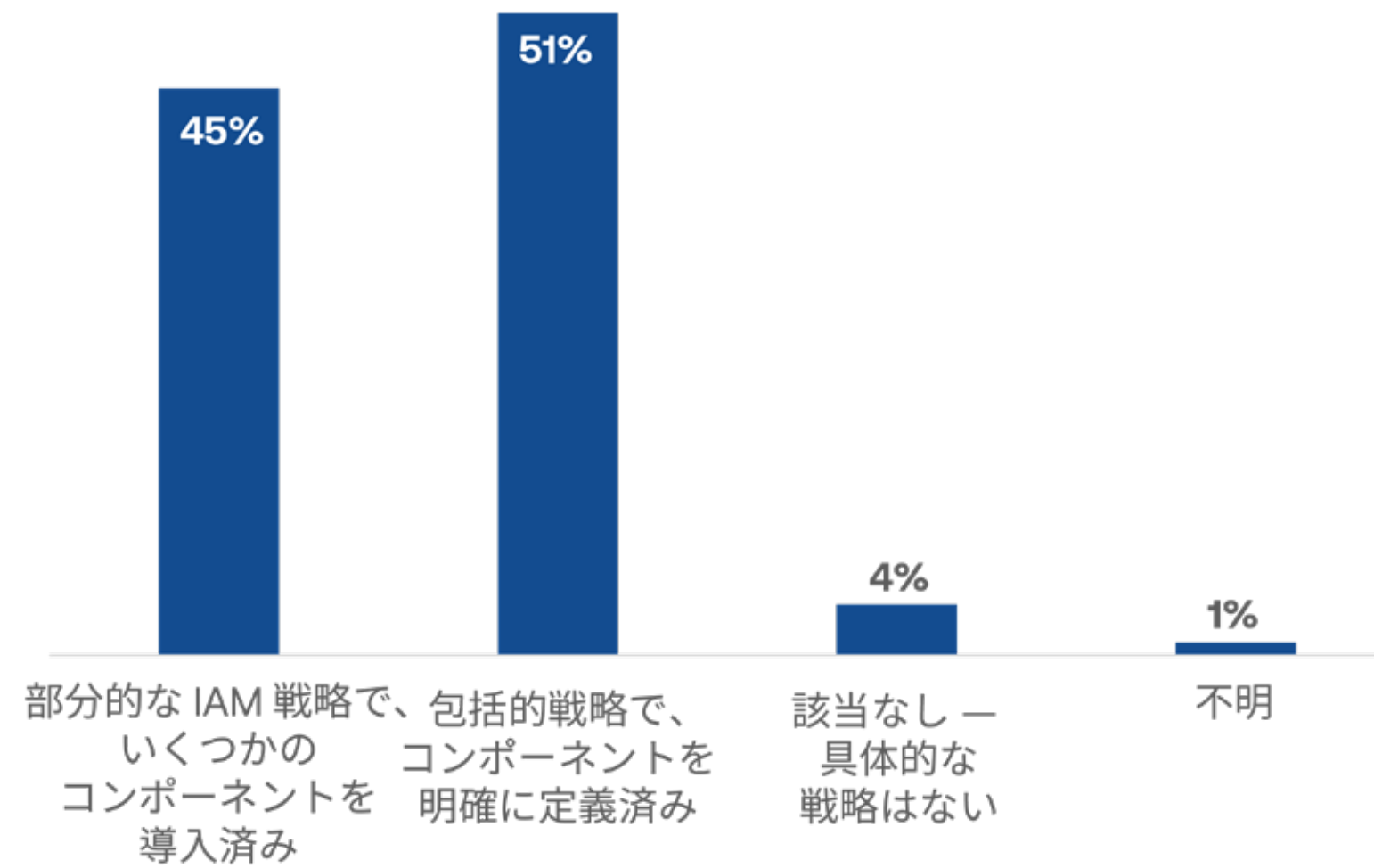
### 成熟度モデルの詳細

Enterprise Strategy Group は、アイデンティティに関連する組織のプラクティスの成熟度を評価するため、現行のテクノロジーとプロセスに関する 8 つの多面的な質問を評価する成熟度モデルを開発しました。

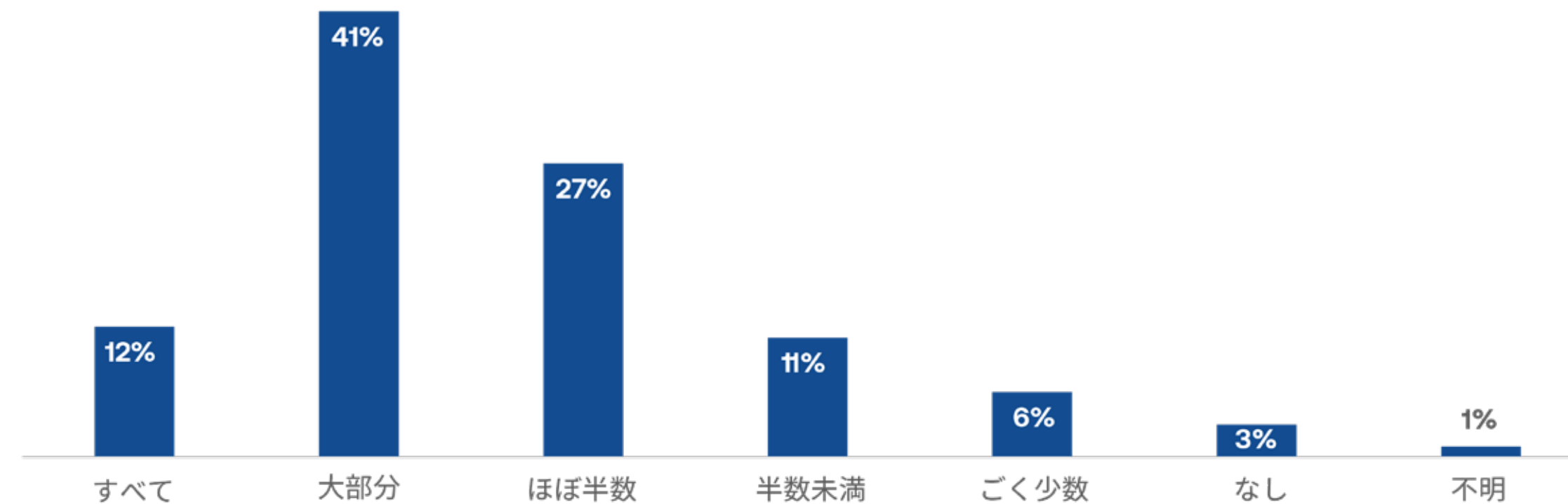
これらの質問に対する回答に基づき、アプローチの成熟度が高いと評価された組織はより多くのポイントを獲得し、アプローチの成熟度が低いと評価された組織は獲得ポイントが少なくなります。成熟度ポイントの範囲は 0 ～ 100 点となります。成熟度ポイントが 81 点以上の組織を「戦略的組織」、71 ～ 80 点の組織を「先進的組織」、61 ～ 70 点の組織を「拡張中の組織」、60 点以下の組織を「基礎レベルの組織」と定義します。

Enterprise Strategy Group が成熟度を評価するために使用した質問と、各回答に割り当てられた成熟度ポイントを、以下の図に示します。

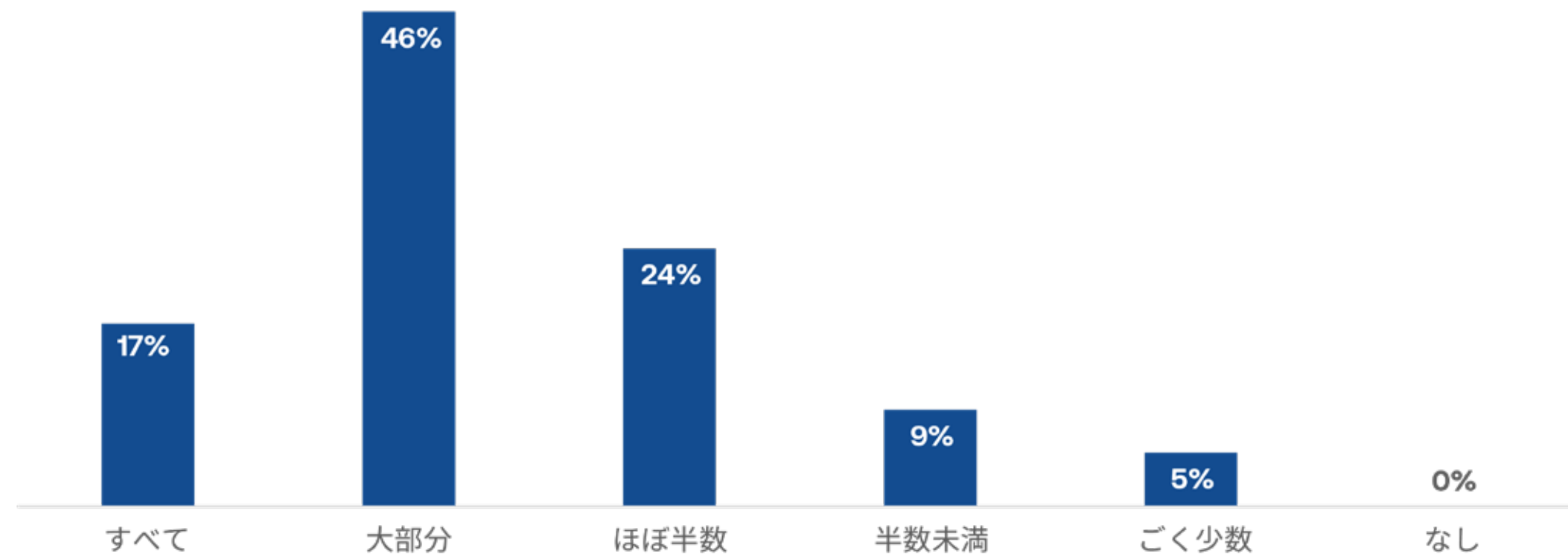
成熟度の質問：組織には包括的なアイデンティティ戦略がありますか？ (n=600)



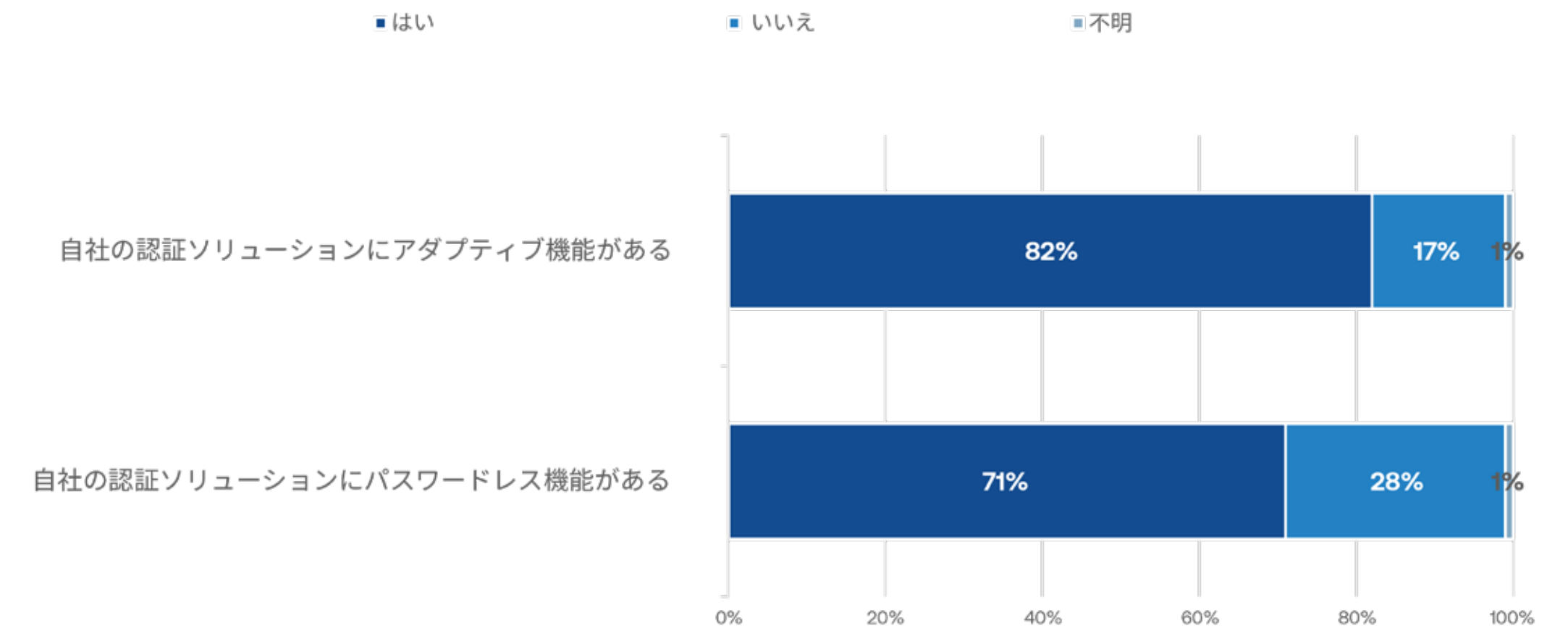
成熟度の質問：ビジネスクリティカルなアプリで、どの程度 SSO を導入していますか？ (n=600)



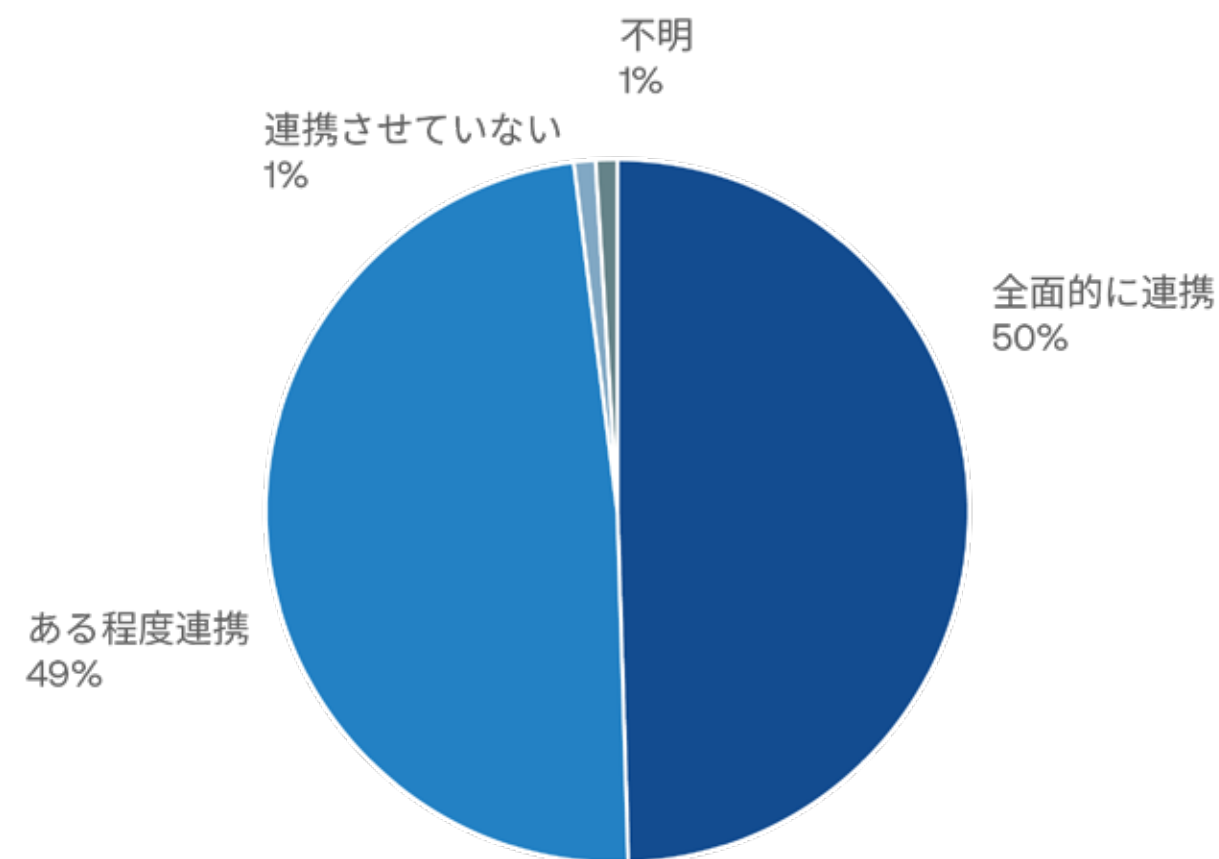
成熟度の質問：ビジネスクリティカルなアプリで、どの程度 MFA を導入していますか？ (n=600)



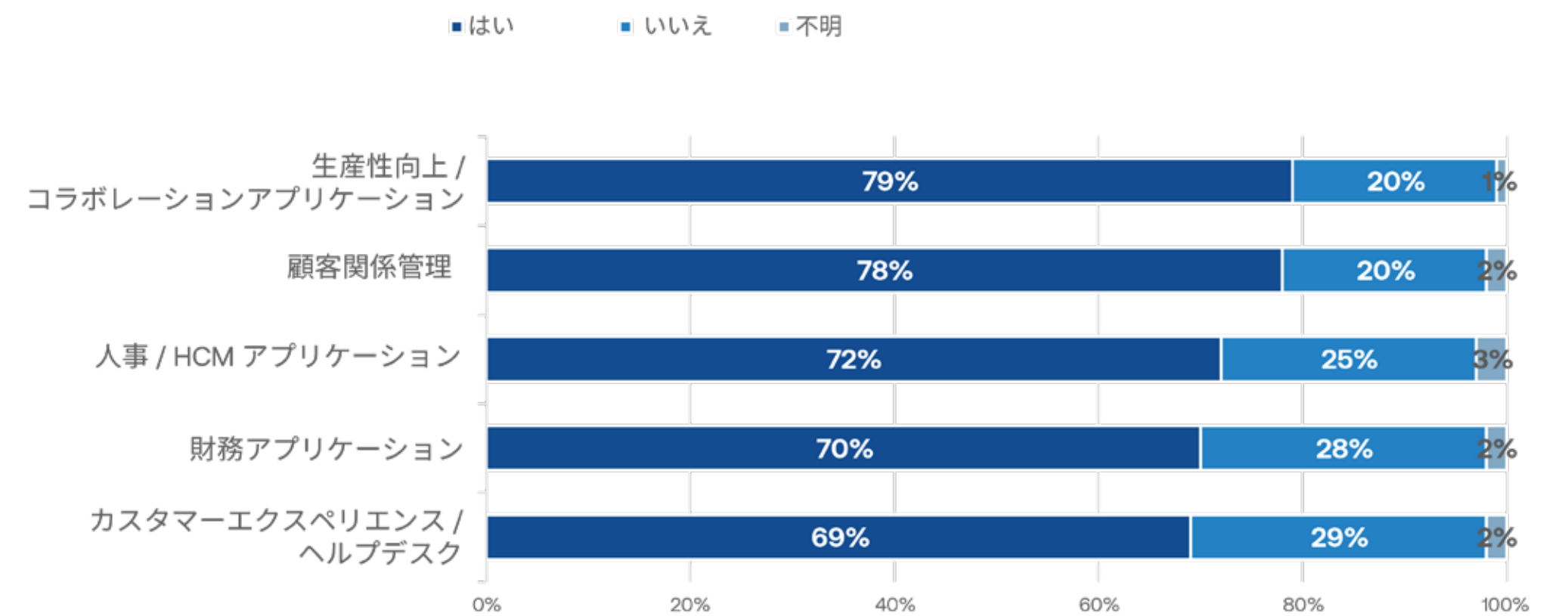
成熟度の質問：アダプティブ機能やパスワードレス機能を認証に組み込んでいますか？ (n=598)



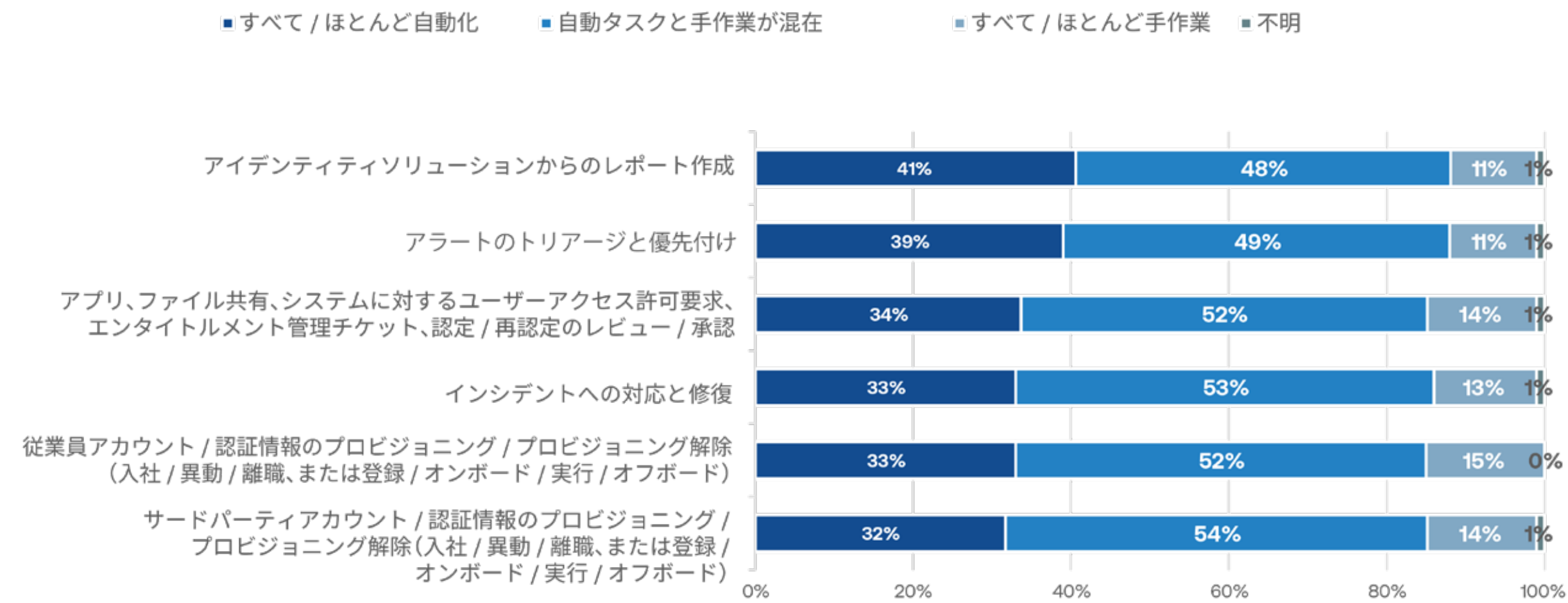
成熟度の質問：社内のディレクトリサービスを連携させていますか？ (n=547)



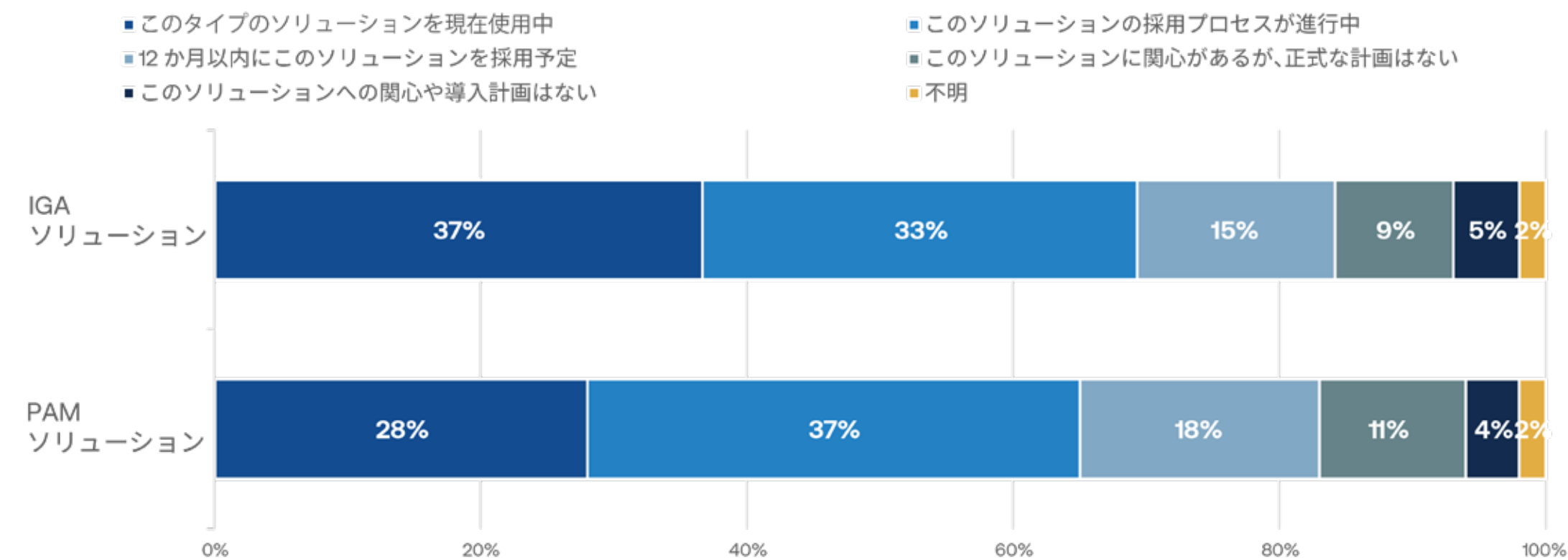
成熟度の質問：主要ビジネスアプリケーションとの統合が容易な IAM ソリューションを活用していますか？ (n=600)



成熟度の質問：手作業やカスタムスクリプトに伴うリスクを軽減するために、アイデンティティ関連タスクを自動化していますか？ (n=600)



成熟度の質問：IAM ソリューションセットを完備させるために、IGA や PAM ソリューションを採用していますか？ (n=600)



All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at [cr@esg-global.com](mailto:cr@esg-global.com).



Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

© 2024 TechTarget, Inc. All Rights Reserved.