SailPoint

Interactive Book

2024-2025

アイデンティティ セキュリティ 調査レポート

アイデンティティ セキュリティ機能を活用し、サイバー セキュリティを強化

読み始める →

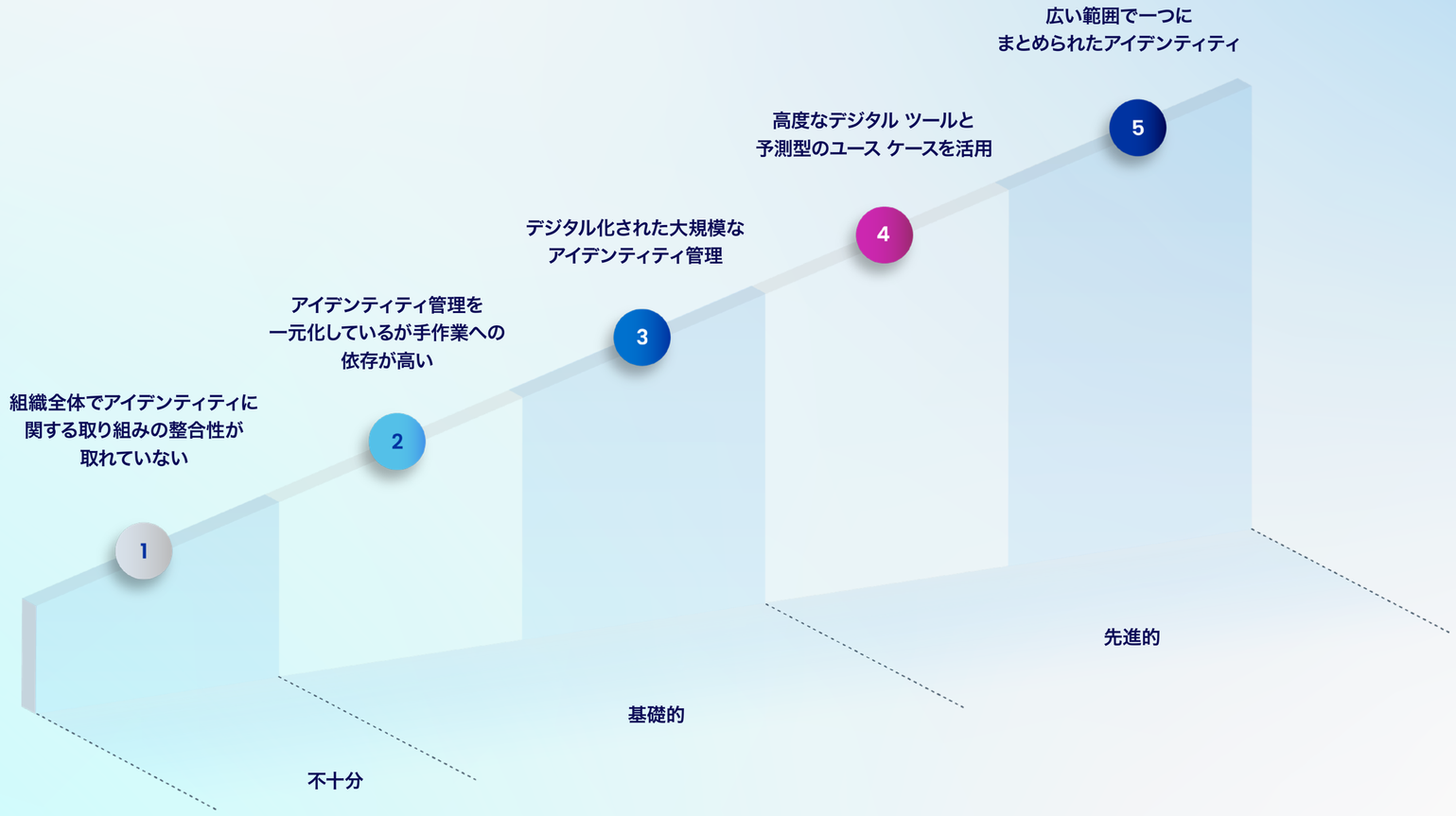
アイデンティティ セキュリティの成熟度の向上を目指して

業種に関係なく、世界中の企業が 2 つの課題に直面しています。1 つは、ますます高度化し増加を続けるサイバー脅威に対抗すること。もう 1 つは、限られた予算の中でコストを抑えながらこうした取り組みを進めなければならないことです。

特にアイデンティティ セキュリティの分野において、この傾向は非常に強くなっています。企業規模が大きくなるにつれ攻撃対象領域は拡大し、IT 予算が縮小されているにもかかわらず、内外のステークホルダーの「より適切なセキュリティとデジタル環境」を求める声は高まるばかりです。

SailPoint は、過去 3 年間にわたり、世界各地のアイデンティティ アクセス管理（IAM）の意思決定者を対象に調査を実施し、アイデンティティ セキュリティの成熟度を 5 段階に分けて評価しました。2024 年 7 月に行われた調査の対象は、情報技術、サイバー セキュリティ、リスク分野の上級管理職を含む 350 名の意思決定者です。半数以上が従業員 1 万人以上の企業に勤めており、半数以上が財務部門や技術部門に所属しています。

出典：本資料におけるすべての図表は、『アイデンティティ セキュリティ調査レポート（2024 年～ 2025 年）』が出典



第 1 章

技術の進歩がアイデンティティ セキュリティの未来を拓く

章の開始 →

アイデンティティの未来を支える 4 つの要素

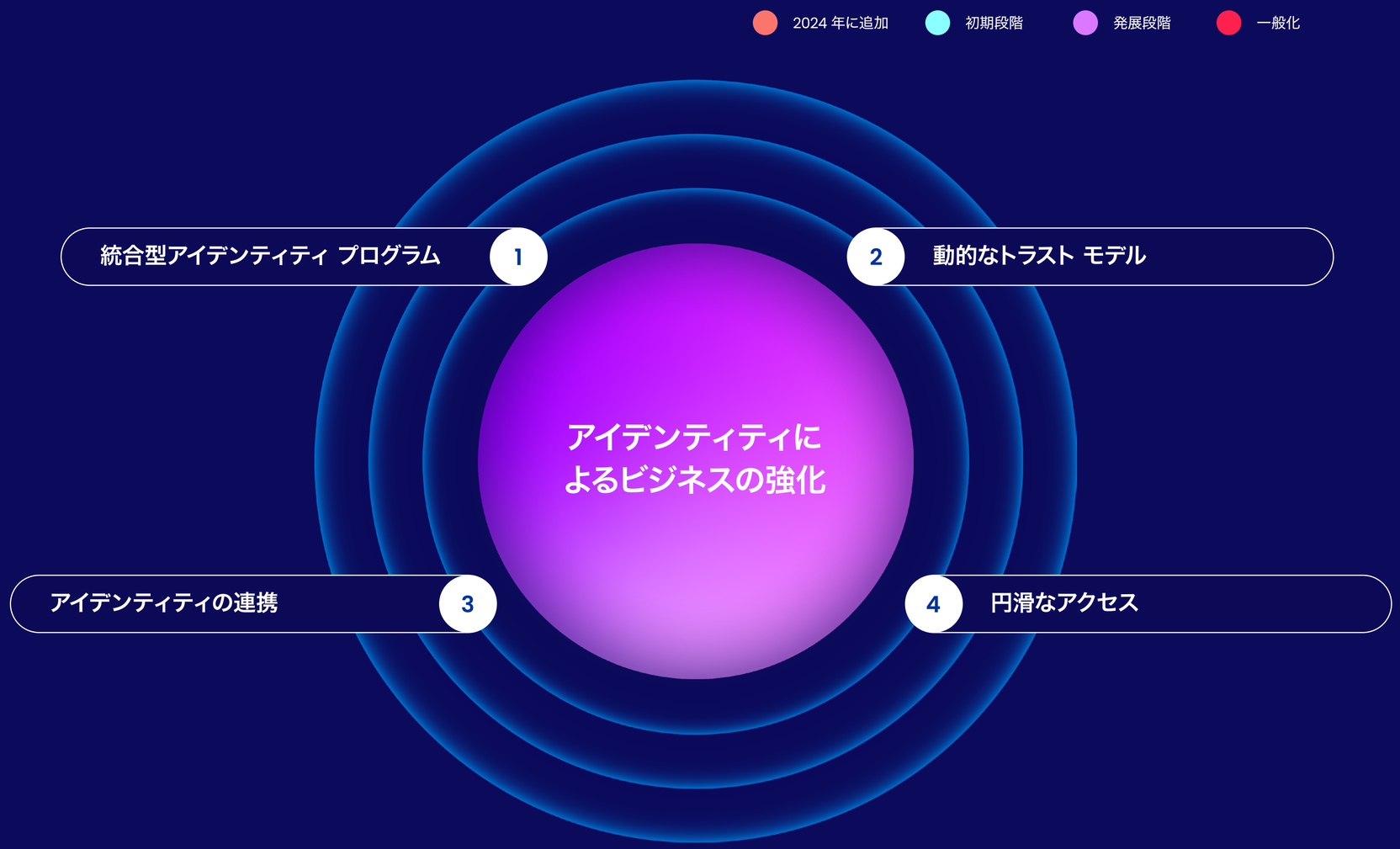
ここ数年間の SailPoint の調査と経験から、アイデンティティ セキュリティの未来は統合型アイデンティティ プログラムが鍵を握ると考えられます。

以下に、主要な要素とそれらを補完するトレンドをご紹介します。

規制やリスクの状況に合わせて、これらの要素も変化し続けます。

また、これらの構成要素は、今後のセキュリティ オペレーションにおける中核を担うものです。

アイデンティティ セキュリティに関連する規制や業界標準が世界各国で、さらには業界単位で増え続けることで、アイデンティティ セキュリティに対する期待はより一層高まるでしょう。



アイデンティティの未来を支える 4 つの要素

ここ数年間の SailPoint の調査と経験から、アイデンティティ セキュリティの未来は統合型アイデンティティ プログラムが鍵を握ると考えられます。

以下に、主要な要素とそれらを補完するトレンドをご紹介します。

規制やリスクの状況に合わせて、これらの要素も変化し続けます。

また、これらの構成要素は、今後のセキュリティ オペレーションにおける中核を担うものです。

アイデンティティ セキュリティに関連する規制や業界標準が世界各国で、さらには業界単位で増え続けることで、アイデンティティ セキュリティに対する期待はより一層高まるでしょう。

アイデンティティの未来を支える 4 つの要素

ここ数年間の SailPoint の調査と経験から、アイデンティティ セキュリティの未来は統合型アイデンティティ プログラムが鍵を握ると考えられます。

以下に、主要な要素とそれらを補完するトレンドをご紹介します。

規制やリスクの状況に合わせて、これらの要素も変化し続けます。

また、これらの構成要素は、今後のセキュリティ オペレーションにおける中核を担うものです。

アイデンティティ セキュリティに関連する規制や業界標準が世界各国で、さらには業界単位で増え続けることで、アイデンティティ セキュリティに対する期待はより一層高まるでしょう。

アイデンティティの未来を支える 4 つの要素

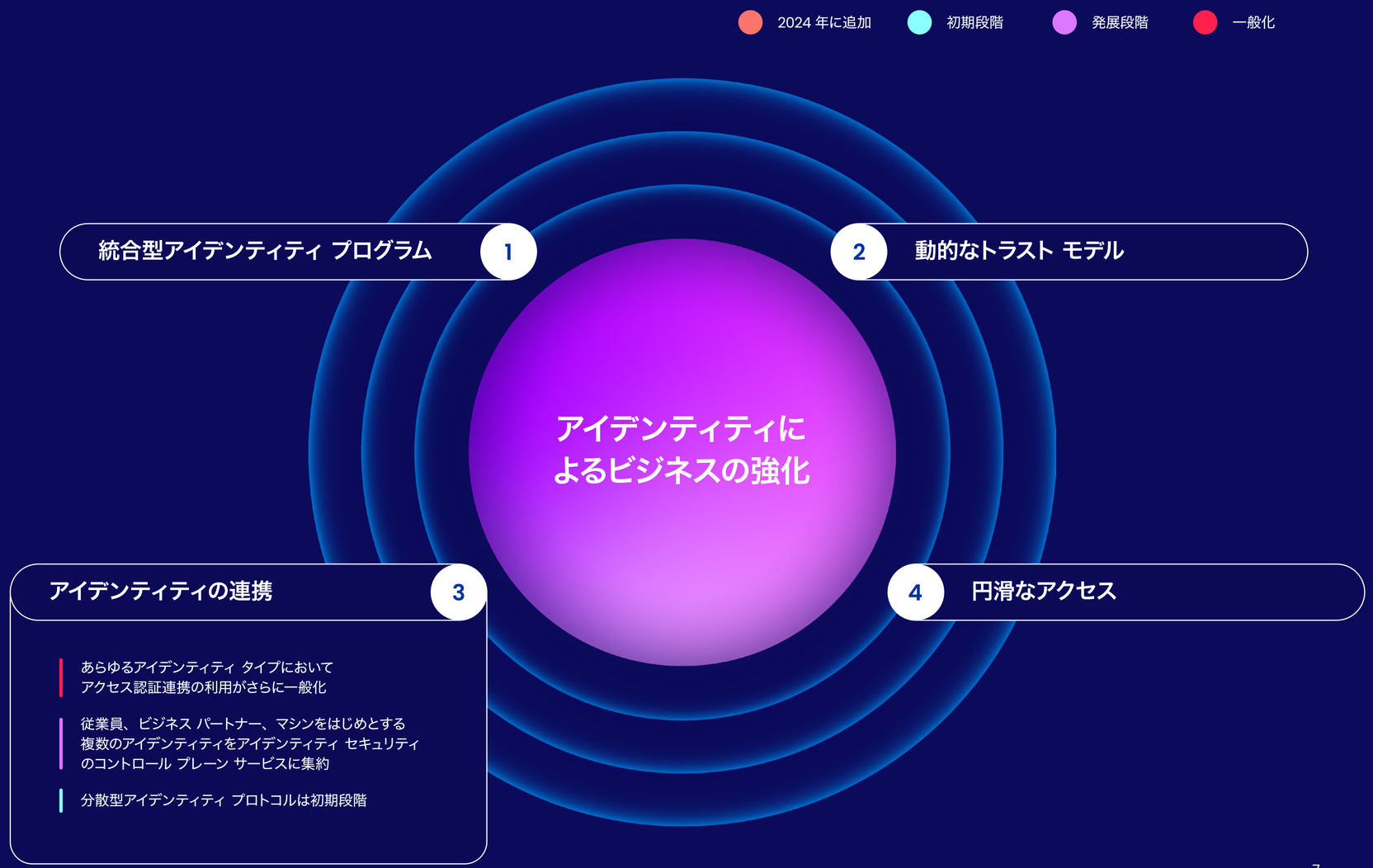
ここ数年間の SailPoint の調査と経験から、アイデンティティ セキュリティの未来は統合型アイデンティティ プログラムが鍵を握ると考えられます。

以下に、主要な要素とそれらを補完するトレンドをご紹介します。

規制やリスクの状況に合わせて、これらの要素も変化し続けます。

また、これらの構成要素は、今後のセキュリティ オペレーションにおける中核を担うものです。

アイデンティティ セキュリティに関連する規制や業界標準が世界各国で、さらには業界単位で増え続けることで、アイデンティティ セキュリティに対する期待はより一層高まるでしょう。



アイデンティティの未来を支える 4 つの要素

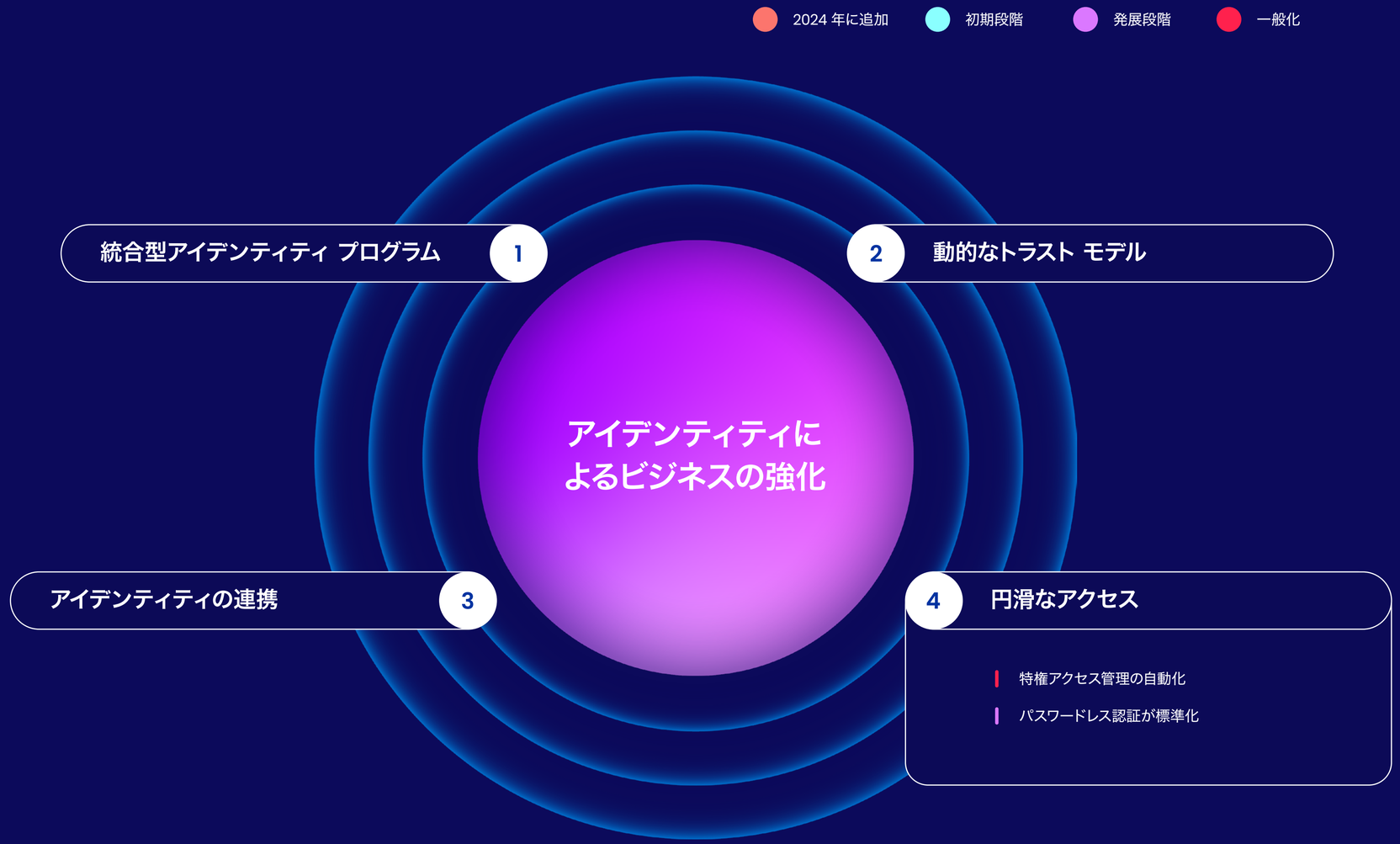
ここ数年間の SailPoint の調査と経験から、アイデンティティ セキュリティの未来は統合型アイデンティティ プログラムが鍵を握ると考えられます。

以下に、主要な要素とそれらを補完するトレンドをご紹介します。

規制やリスクの状況に合わせて、これらの要素も変化し続けます。

また、これらの構成要素は、今後のセキュリティ オペレーションにおける中核を担うものです。

アイデンティティ セキュリティに関連する規制や業界標準が世界各国で、さらには業界単位で増え続けることで、アイデンティティ セキュリティに対する期待はより一層高まるでしょう。



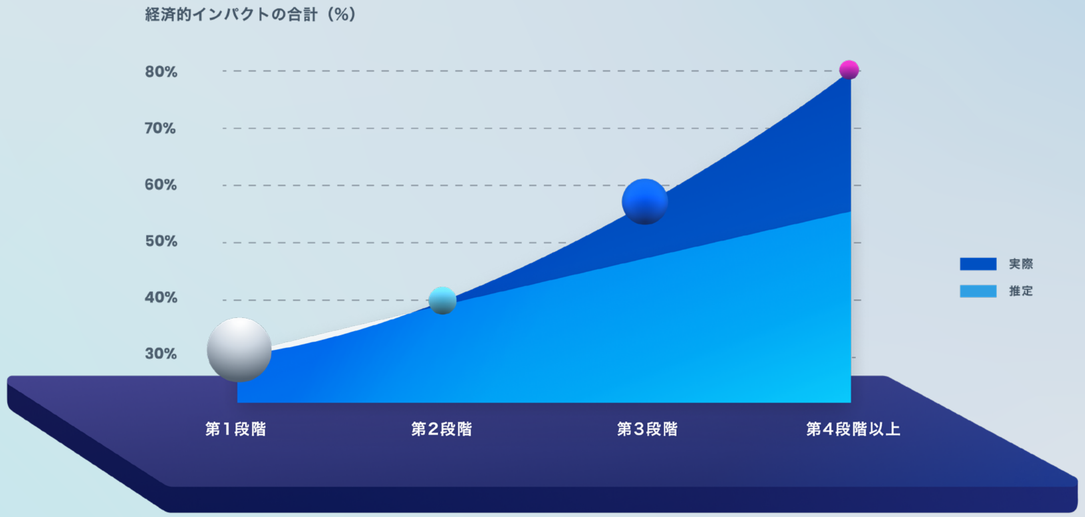
第 2 章

アイデンティティ セキュリティの底上げにつながる投資

章の開始 →

アイデンティティ セキュリティの成熟度が高い企業は投資した以上の高い費用対効果を実現

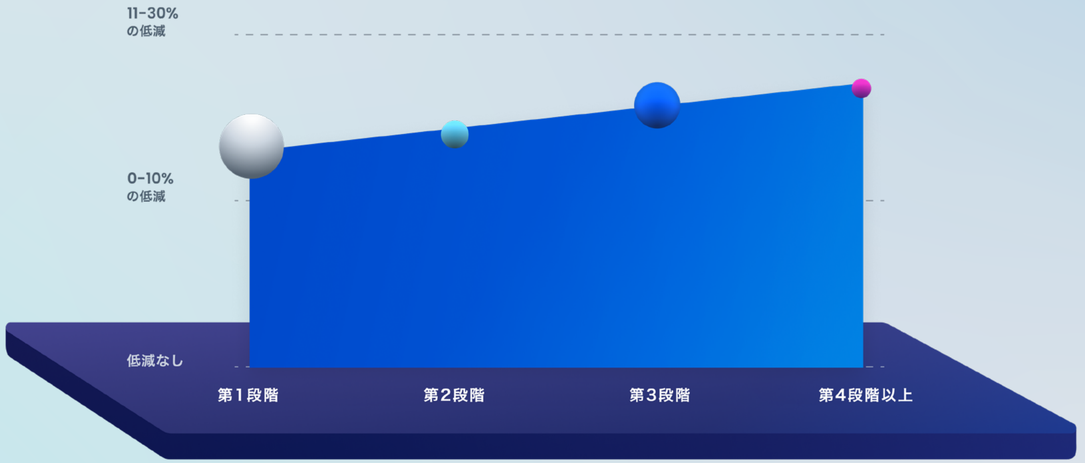
アイデンティティ セキュリティの成熟度が第 3 段階、第 4 段階にまで到達すると、ビジネスに顕著な影響が現れ、「価値曲線」が飛躍的な伸びを示すようになります。



*バブルの大きさは、各レベルの分布を示す

アイデンティティ セキュリティの成熟度が高まることで攻撃対象領域が縮小し潜在的リスクが低減

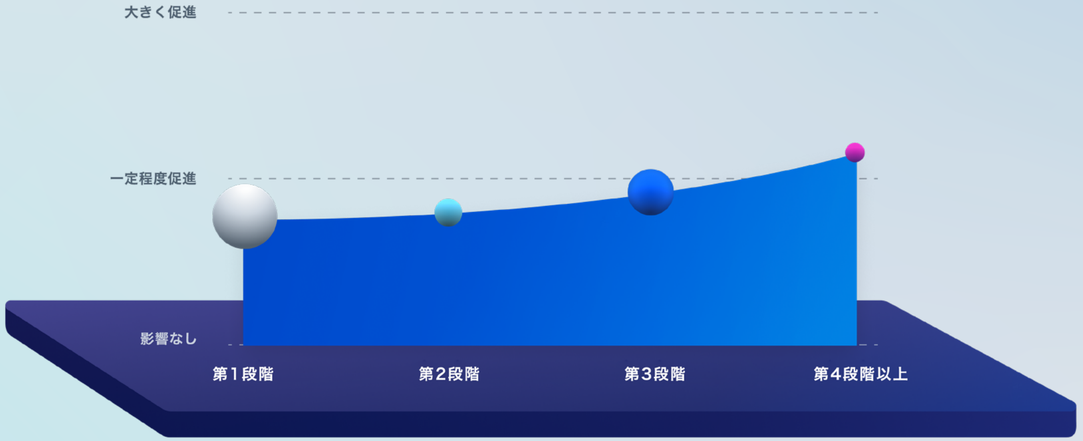
2023 年にアイデンティティ セキュリティに投資したことにより **83% の企業がアイデンティティに関連したセキュリティ問題が減少した**と報告しています。



*バブルの大きさは、各レベルの分布を示す

高度なアイデンティティ機能を備えた企業では市場投入までの時間が短縮され不具合も減少

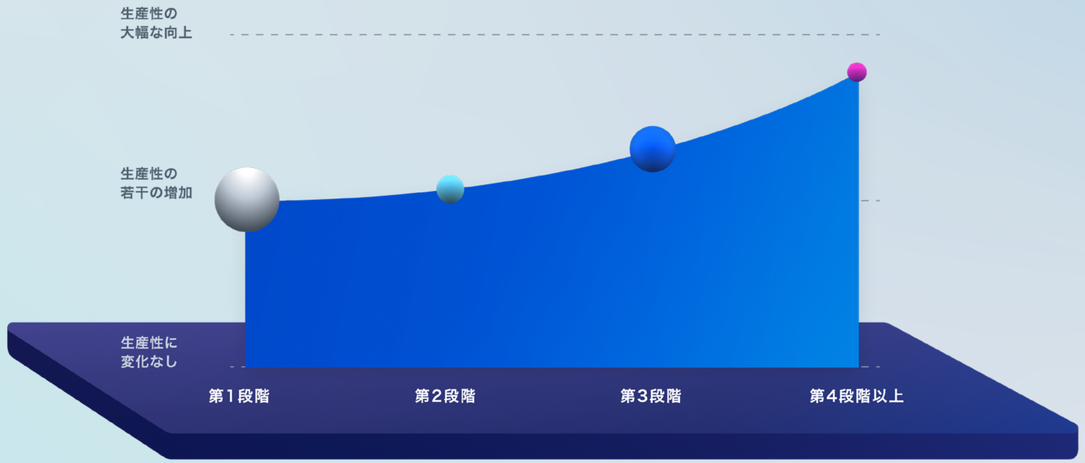
売上高が拡大：高度なアイデンティティ セキュリティ機能を備えることによりデジタル トランスフォーメーションが促進され、開発サイクルや市場投入までの時間が短縮し、収益の増加を実現できます。



*バブルの大きさは、各レベルの分布を示す

第 3 段階、第 4 段階以上の企業は生産性の大幅な向上が見込まれます

第 4 段階以上の企業は大幅な生産性の向上が見込まれます。これは、ガイダンスの操作支援、エンド ユーザー向けサービスの提供、ユーザー アクセス権の自動承認付与などの導入と、統合アイデンティティ セキュリティ アプローチによる効果です。



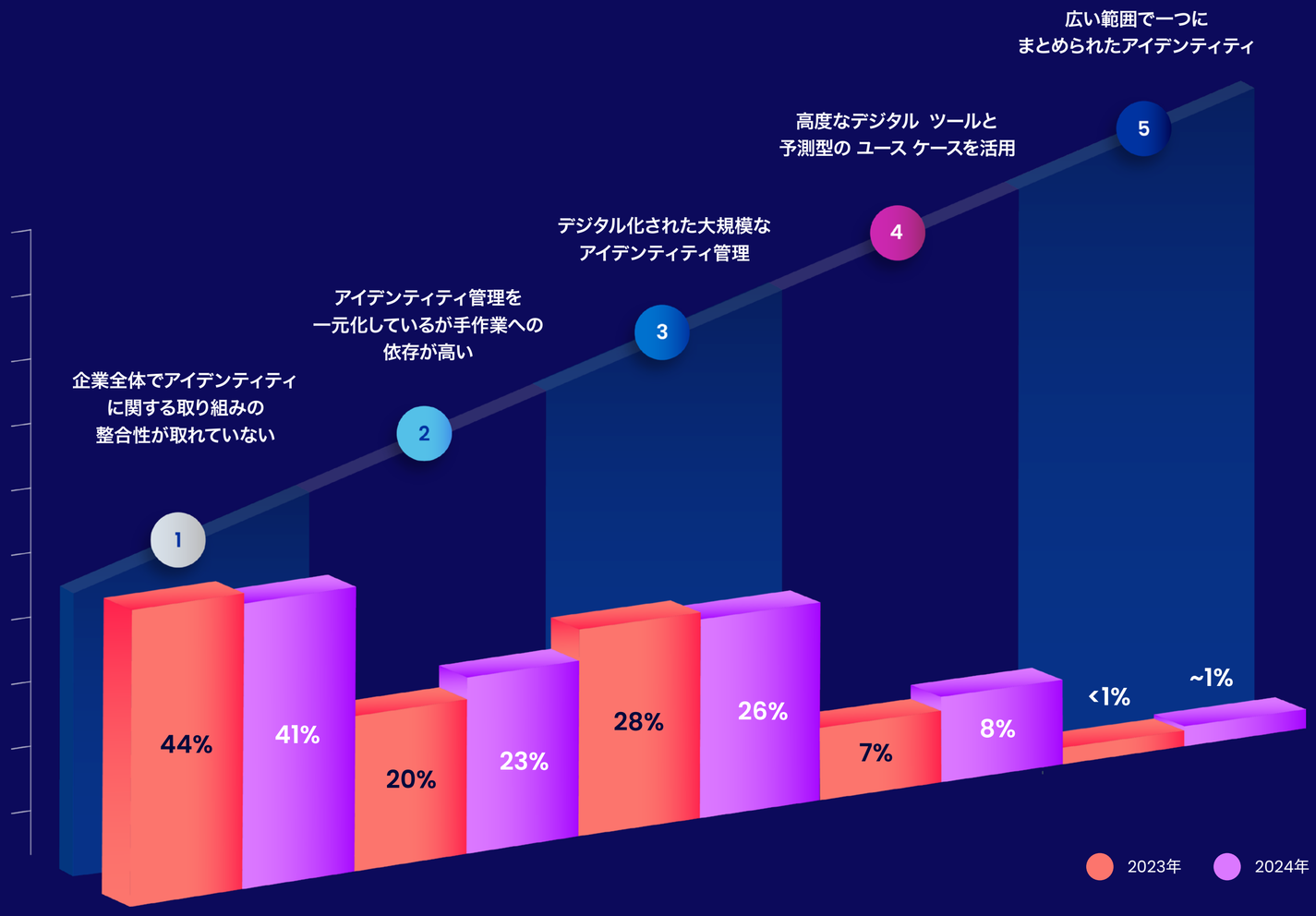
*バブルの大きさは、各レベルの分布を示す

第 3 章

企業の取り組み状況に見る「成熟度とリターンの関係」

章の開始 →

41% の企業が依然として第 1 段階に留まっており、アイデンティティ セキュリティ機能を十分に活用できていない



第 4 段階以上の企業では、どのアイデンティティ タイプでも 70% の機能がカバーされており リスクが低下、第 3 段階でも同様の結果を示す

第 1 段階、第 2 段階の企業は、第 3 段階以上の企業に比べて、対応しているアイデンティティ タイプに大きく隔たりがあります。
現在、以下のアイデンティティは管理対象に含まれていません。

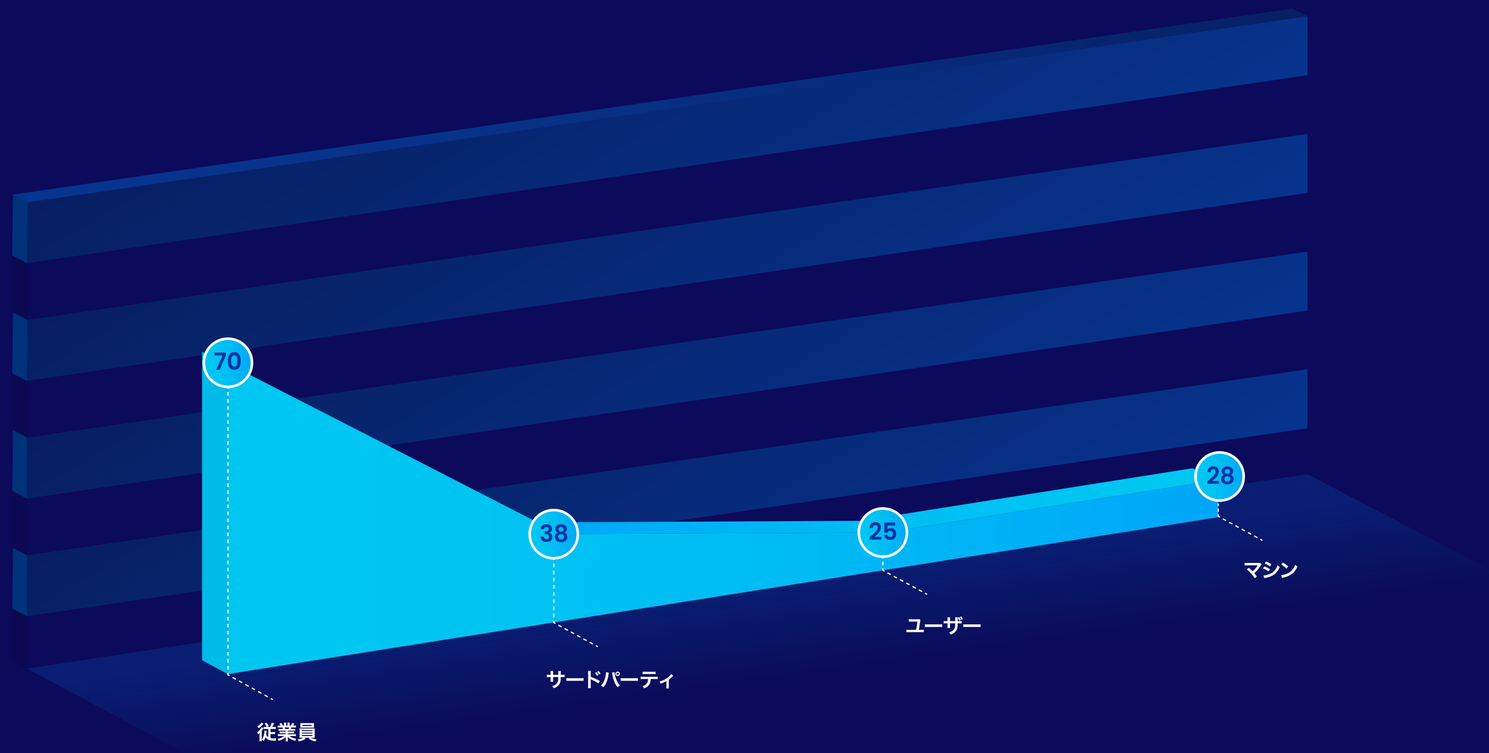
30%
従業員

62%
サードパーティ

72%
マシン アイデンティティ

一般的にマシン アイデンティティが組織全体のアイデンティティ数の 40% ～ 65% を占めるという事実を踏まえると、特にマシン アイデンティティのカバー率の低さが懸念されます。

第 1 ～第 2 段階 | 第 3 段階 | 第 4 段階以上 | 全体 | 全データ



第 4 段階以上の企業では、どのアイデンティティ タイプでも 70% の機能がカバーされており リスクが低下、第 3 段階でも同様の結果を示す

第 1 段階、第 2 段階の企業は、第 3 段階以上の企業に比べて、対応しているアイデンティティ タイプに大きく隔たりがあります。
現在、以下のアイデンティティは管理対象に含まれていません。

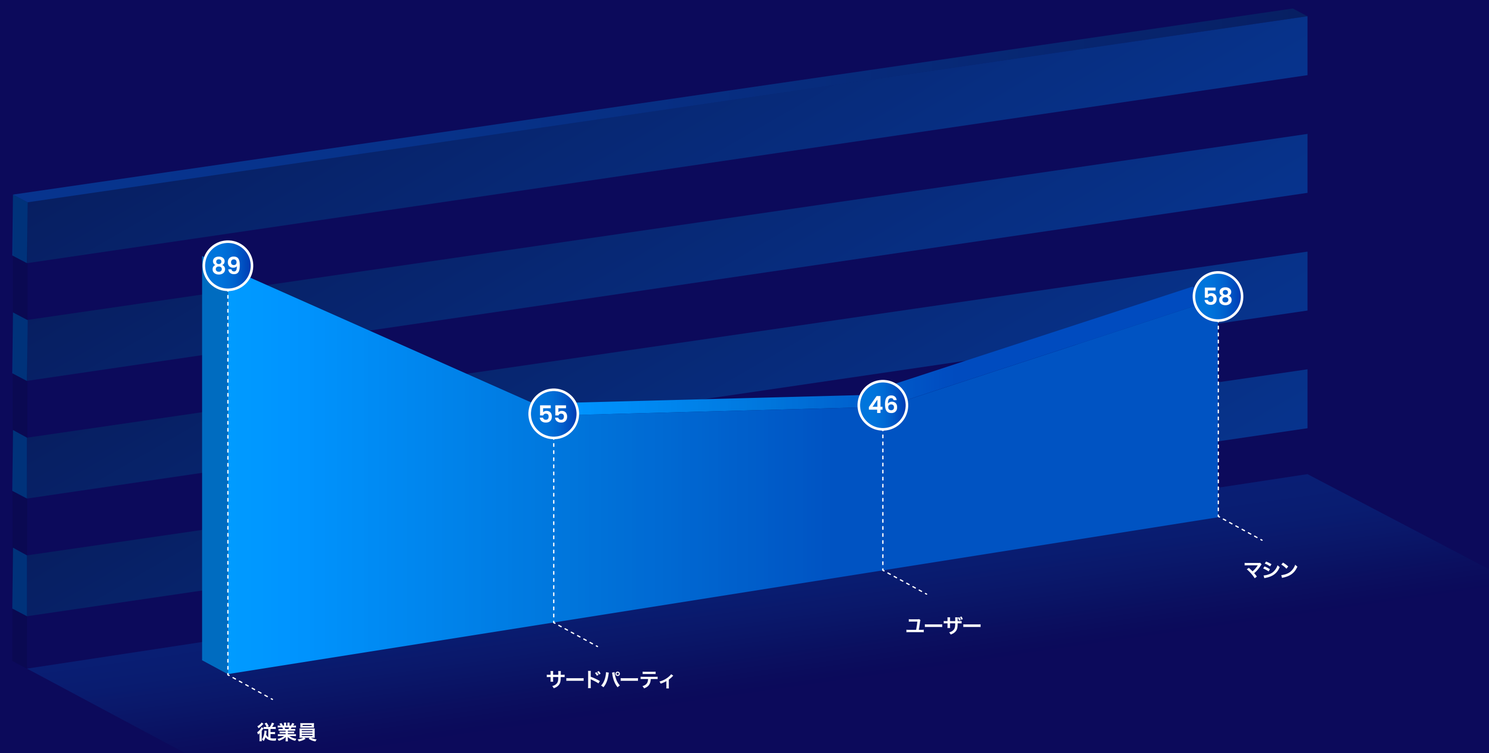
30%
従業員

62%
サードパーティ

72%
マシン アイデンティティ

一般的にマシン アイデンティティが組織全体のアイデンティティ数の 40% ～ 65% を占めるという事実を踏まえると、特にマシン アイデンティティのカバー率の低さが懸念されます。

第 1 ～第 2 段階 | 第 3 段階 | 第 4 段階以上 | 全体 | 全データ



第 4 段階以上の企業では、どのアイデンティティ タイプでも 70% の機能がカバーされておりリスクが低下、第 3 段階でも同様の結果を示す

第 1 段階、第 2 段階の企業は、第 3 段階以上の企業に比べて、対応しているアイデンティティ タイプに大きく隔たりがあります。
現在、以下のアイデンティティは管理対象に含まれていません。

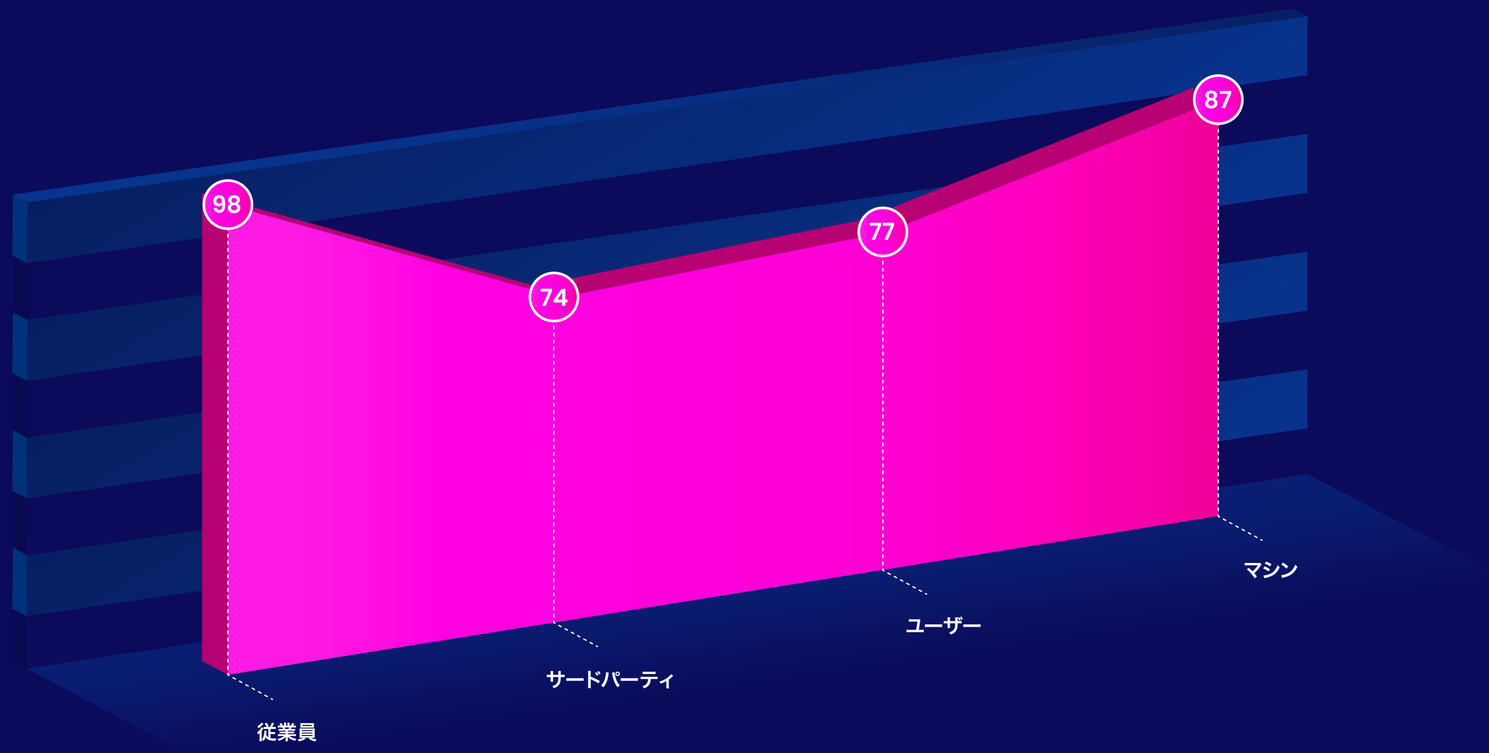
30%
従業員

62%
サードパーティ

72%
マシン アイデンティティ

一般的にマシン アイデンティティが組織全体のアイデンティティ数の 40% ～ 65% を占めるという事実を踏まえると、特にマシン アイデンティティのカバー率の低さが懸念されます。

第 1 ～第 2 段階 | 第 3 段階 | **第 4 段階以上** | 全体 | 全データ



第 4 段階以上の企業では、どのアイデンティティ タイプでも 70% の機能がカバーされており リスクが低下、第 3 段階でも同様の結果を示す

第 1 段階、第 2 段階の企業は、第 3 段階以上の企業に比べて、対応しているアイデンティティ タイプに大きく隔たりがあります。
現在、以下のアイデンティティは管理対象に含まれていません。

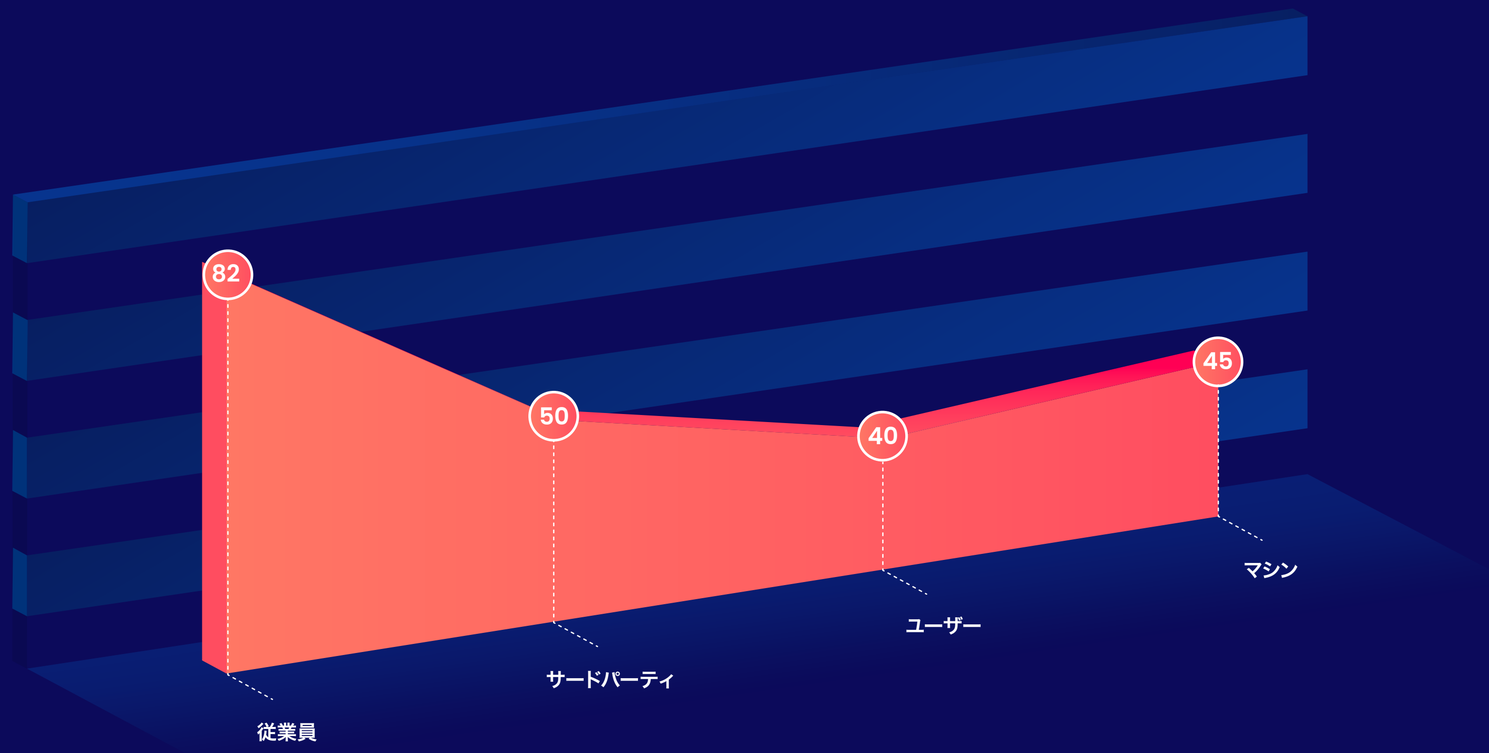
30%
従業員

62%
サードパーティ

72%
マシン アイデンティティ

一般的にマシン アイデンティティが組織全体のアイデンティティ数の 40% ～ 65% を占めるという事実を踏まえると、特にマシン アイデンティティのカバー率の低さが懸念されます。

第 1 ～第 2 段階 | 第 3 段階 | 第 4 段階以上 | 全体 | 全データ



第 4 段階以上の企業では、どのアイデンティティ タイプでも 70% の機能がカバーされており リスクが低下、第 3 段階でも同様の結果を示す

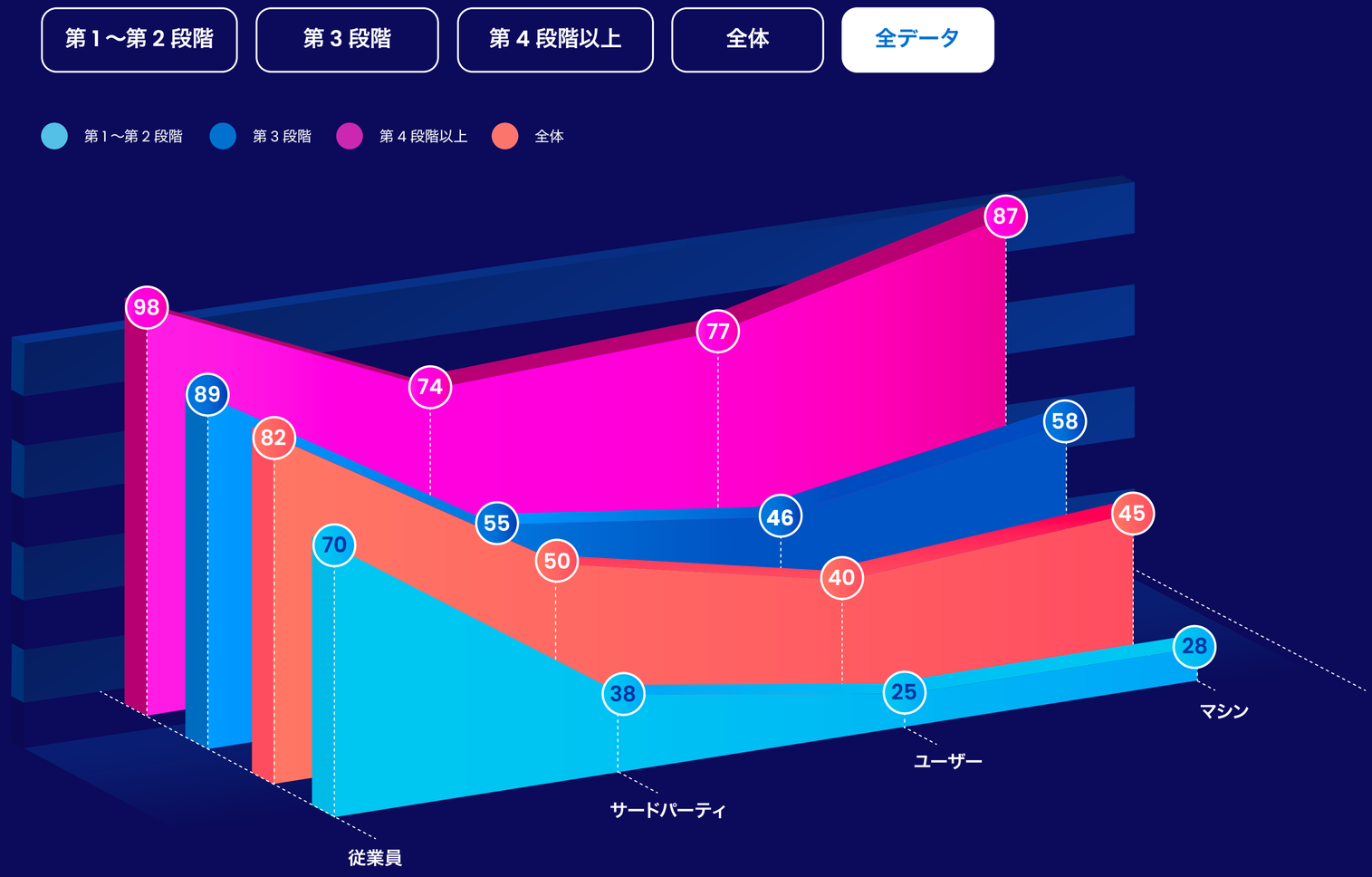
第 1 段階、第 2 段階の企業は、第 3 段階以上の企業に比べて、対応しているアイデンティティ タイプに大きく隔たりがあります。
現在、以下のアイデンティティは管理対象に含まれていません。

30%
従業員

62%
サードパーティ

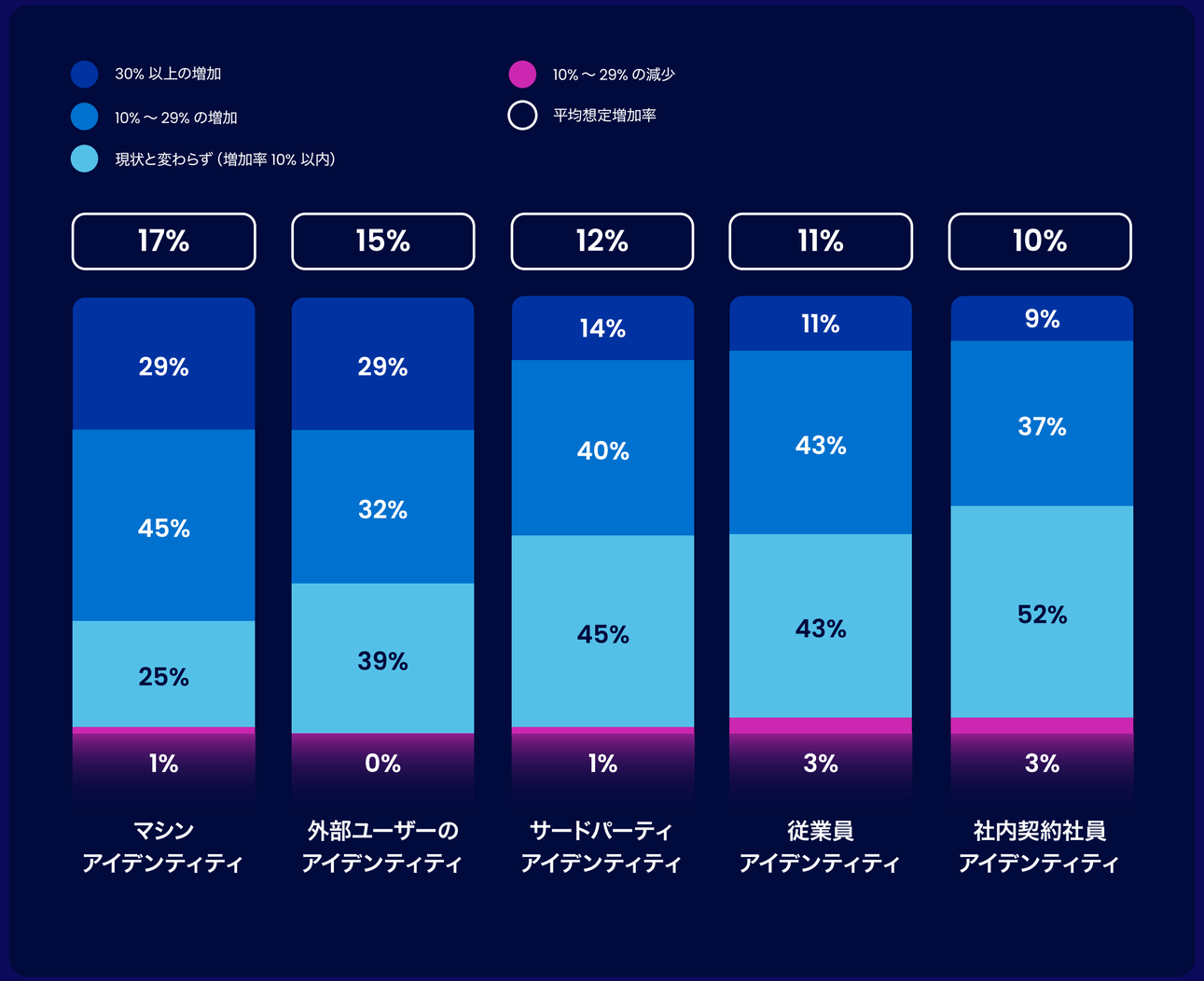
72%
マシン アイデンティティ

一般的にマシン アイデンティティが組織全体のアイデンティティ数の 40% ～ 65% を占めるという事実を踏まえると、特にマシン アイデンティティのカバー率の低さが懸念されます。

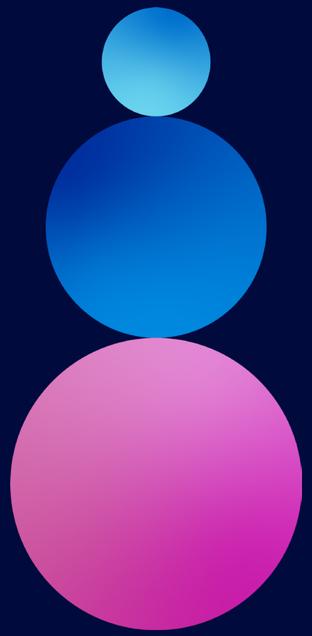


今後 3 年から 5 年のうちに、アイデンティティの数は全体で約 14% 増加し、中でもマシン アイデンティティの数は急増が見込まれる

マシン アイデンティティの増加ペースは、人間のアイデンティティのペースを上回る



第 4 段階以上の企業がアイデンティティ データをインテリジェンスや新規ユース ケースに活用する傾向は、第 1～第3段階の企業の 2 倍



<20%

アイデンティティ インテリジェンス データを大規模に活用している第 1 段階、第 2 段階の企業

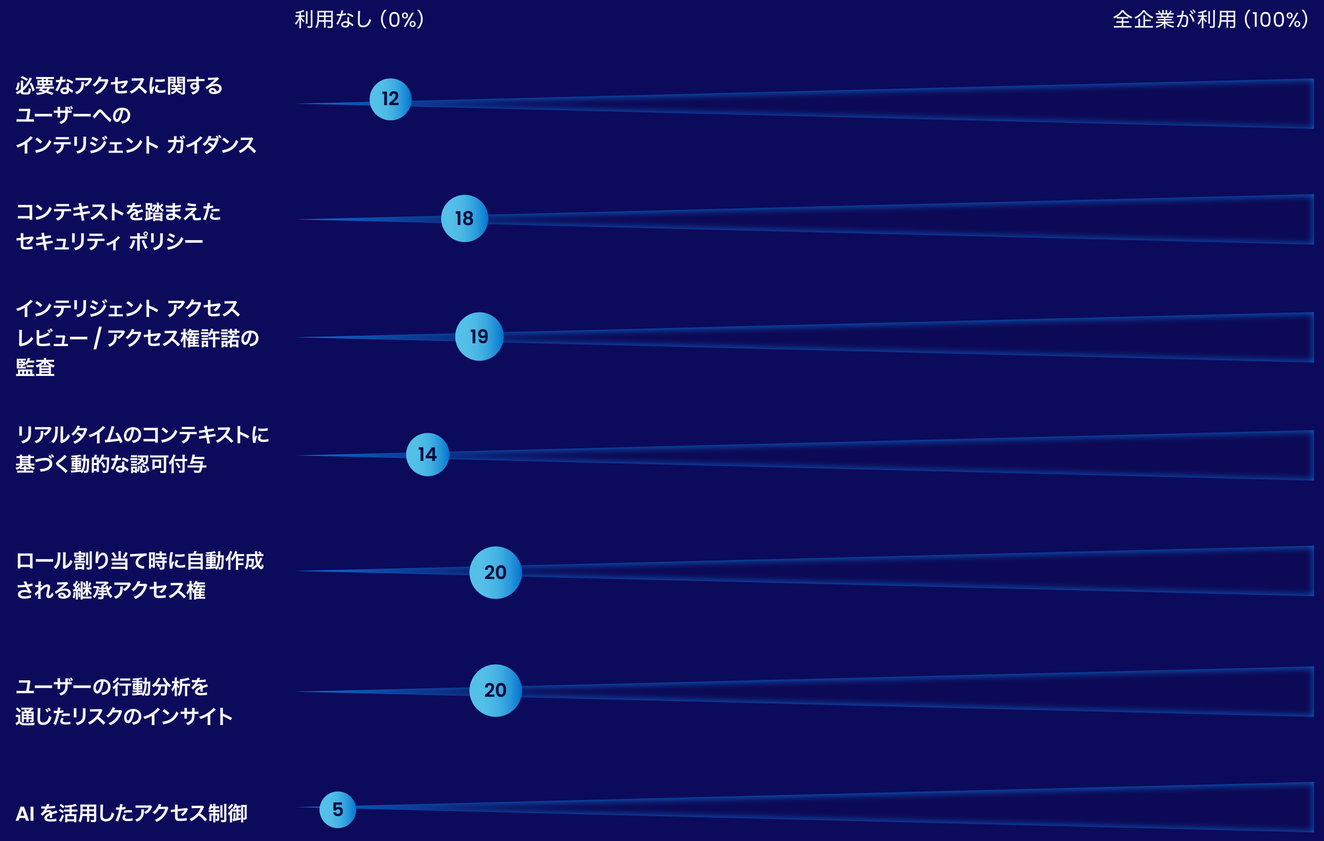
<40%

アイデンティティ インテリジェンス データを大規模に活用している第 3 段階の企業

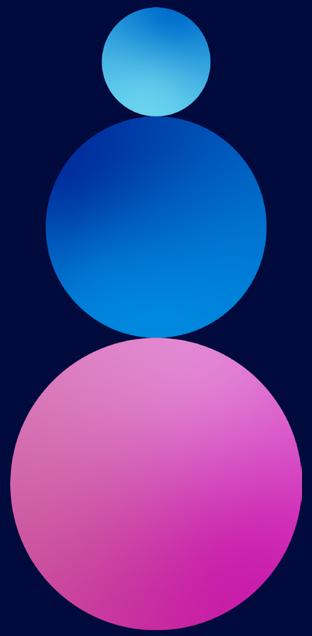
~50%

ユーザー アクセス、セキュリティ ポリシー、アクセス レビューの構造化データおよび非構造化データから得られたインテリジェンスを指針として活用している第 4 段階以上の企業

第 1～第 2 段階 | 第 3 段階 | 第 4 段階以上 | 全体 | 全データ



第 4 段階以上の企業がアイデンティティ データをインテリジェンスや新規ユース ケースに活用する傾向は、第 1～第 3 段階の企業の 2 倍



<20%

アイデンティティ インテリジェンス データを大規模に活用している第 1 段階、第 2 段階の企業

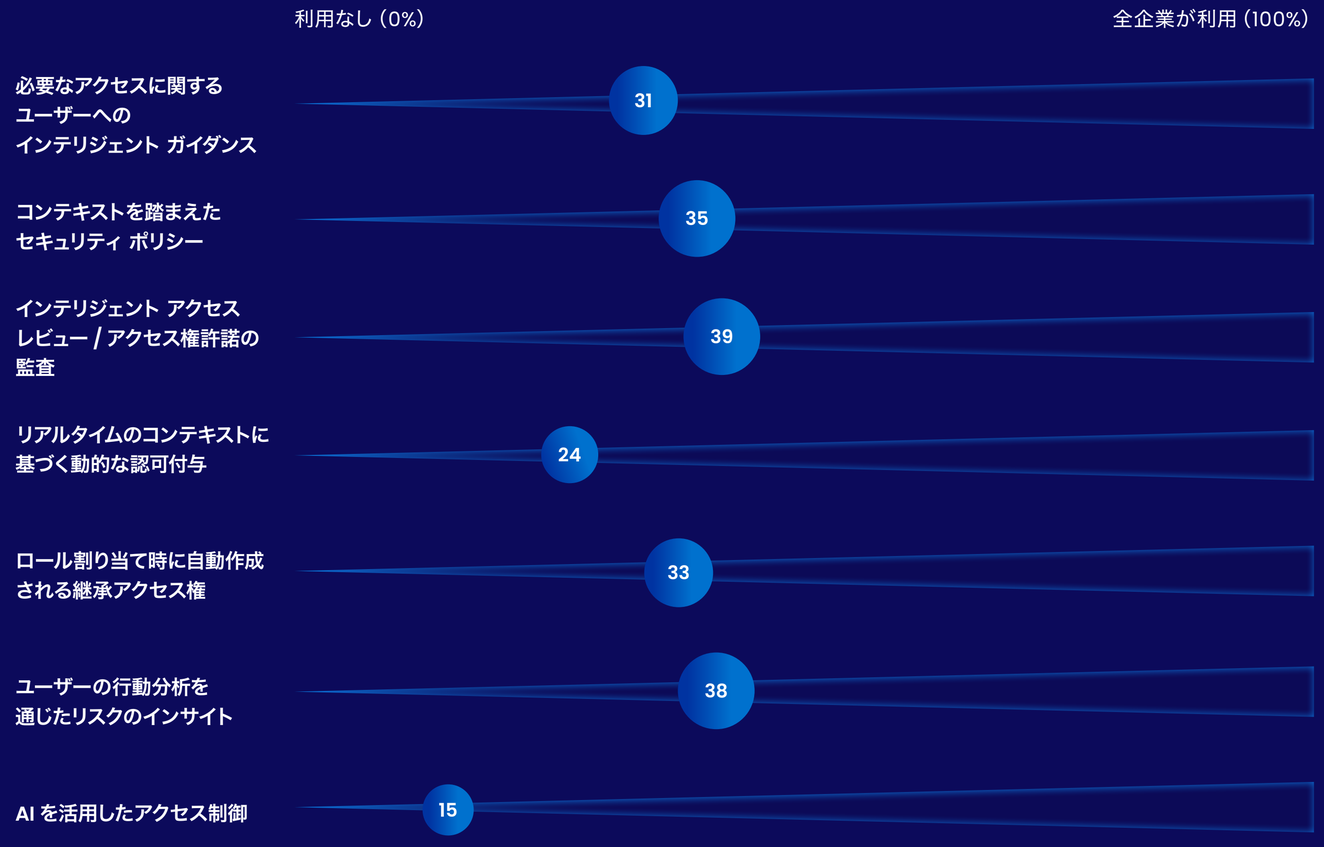
<40%

アイデンティティ インテリジェンス データを大規模に活用している第 3 段階の企業

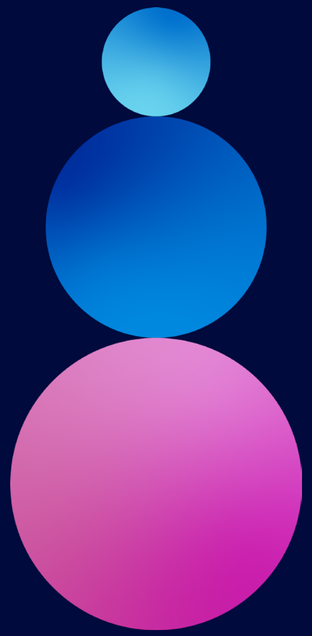
~50%

ユーザー アクセス、セキュリティ ポリシー、アクセス レビューの構造化データおよび非構造化データから得られたインテリジェンスを指針として活用している第 4 段階以上の企業

第 1～第 2 段階 | 第 3 段階 | 第 4 段階以上 | 全体 | 全データ



第 4 段階以上の企業がアイデンティティ データをインテリジェンスや新規ユース ケースに活用する傾向は、第 1～第3段階の企業の 2 倍



<20%

アイデンティティ インテリジェンス データを大規模に活用している第 1 段階、第 2 段階の企業

<40%

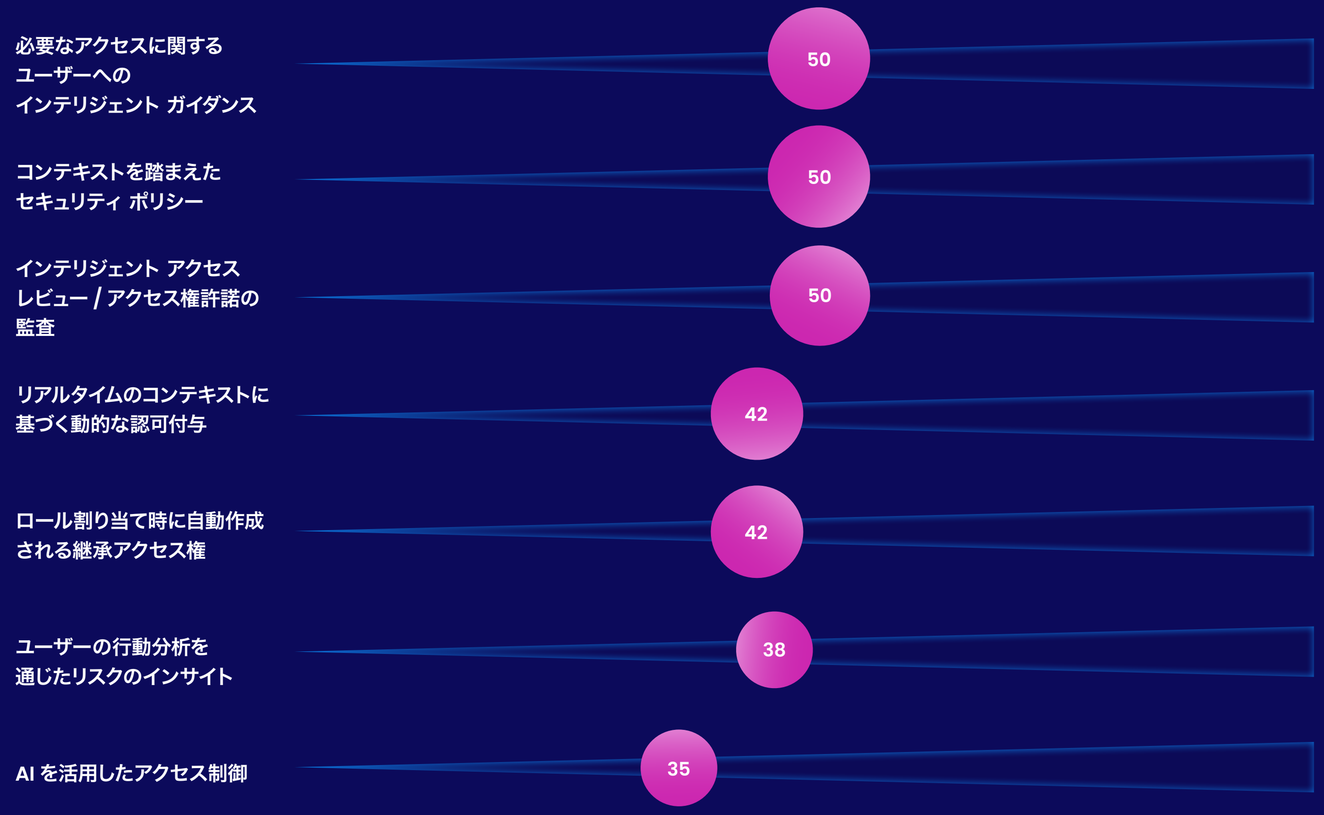
アイデンティティ インテリジェンス データを大規模に活用している第 3 段階の企業

~50%

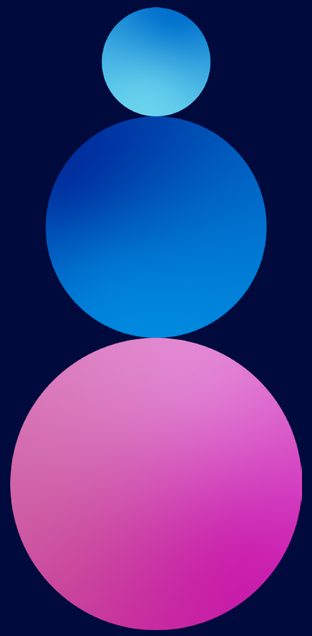
ユーザー アクセス、セキュリティ ポリシー、アクセス レビューの構造化データおよび非構造化データから得られたインテリジェンスを指針として活用している第 4 段階以上の企業

第 1～第 2 段階 | 第 3 段階 | 第 4 段階以上 | 全体 | 全データ

利用なし (0%) 全企業が利用 (100%)



第 4 段階以上の企業がアイデンティティ データをインテリジェンスや新規ユース ケースに活用する傾向は、第 1～第 3 段階の企業の 2 倍



<20%

アイデンティティ インテリジェンス データを大規模に活用している第 1 段階、第 2 段階の企業

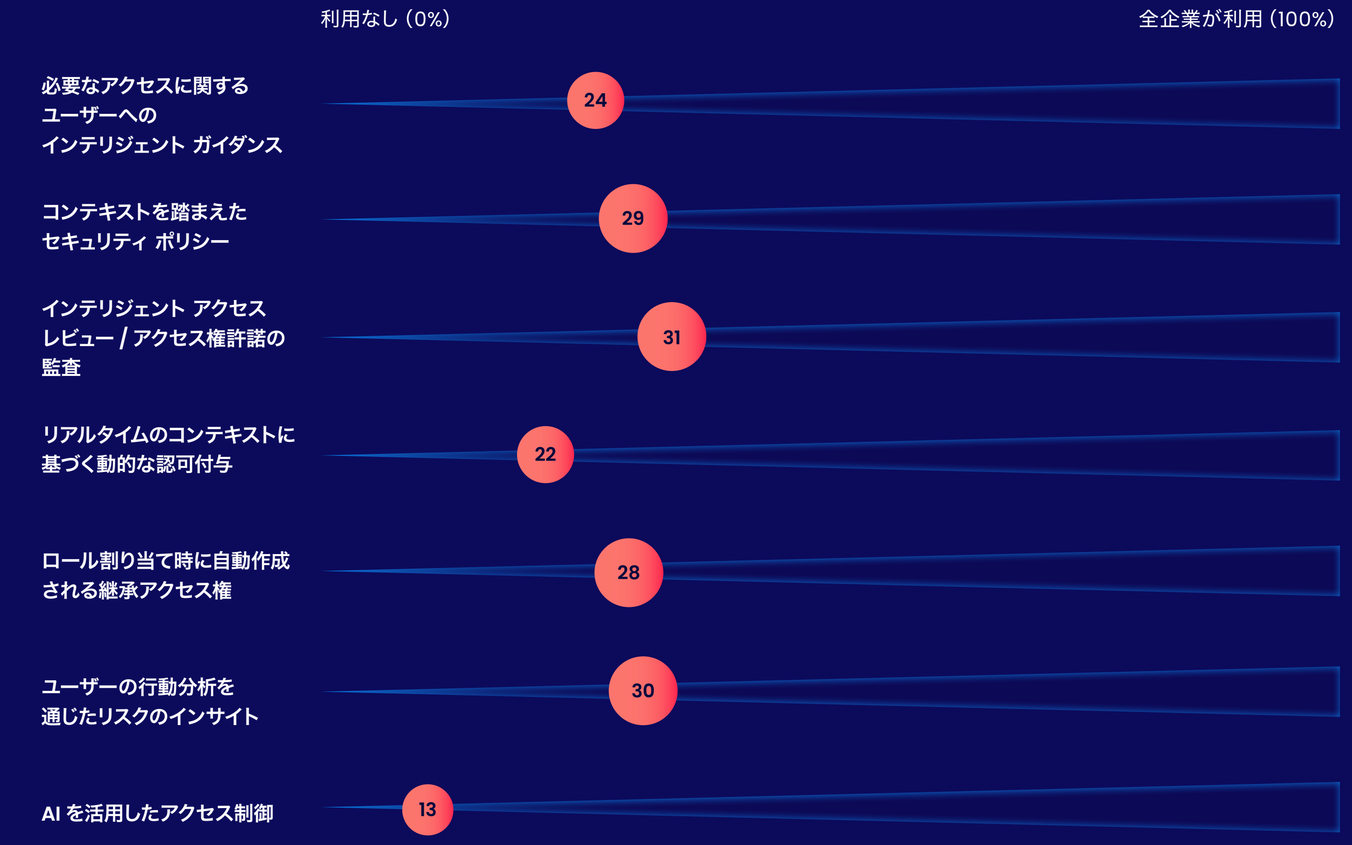
<40%

アイデンティティ インテリジェンス データを大規模に活用している第 3 段階の企業

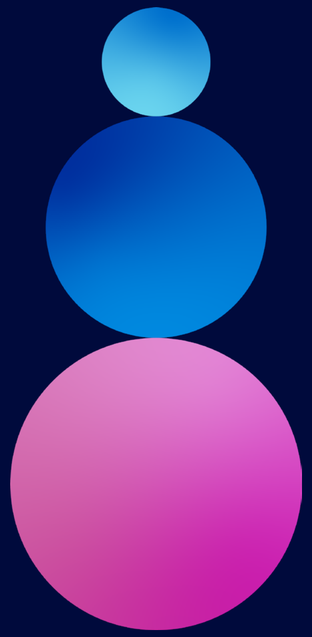
~50%

ユーザー アクセス、セキュリティ ポリシー、アクセス レビューの構造化データおよび非構造化データから得られたインテリジェンスを指針として活用している第 4 段階以上の企業

第 1～第 2 段階 | 第 3 段階 | 第 4 段階以上 | 全体 | 全データ



第 4 段階以上の企業がアイデンティティ データをインテリジェンスや新規ユース ケースに活用する傾向は、第 1～第3段階の企業の 2 倍



<20%

アイデンティティ インテリジェンス データを大規模に活用している第 1 段階、第 2 段階の企業

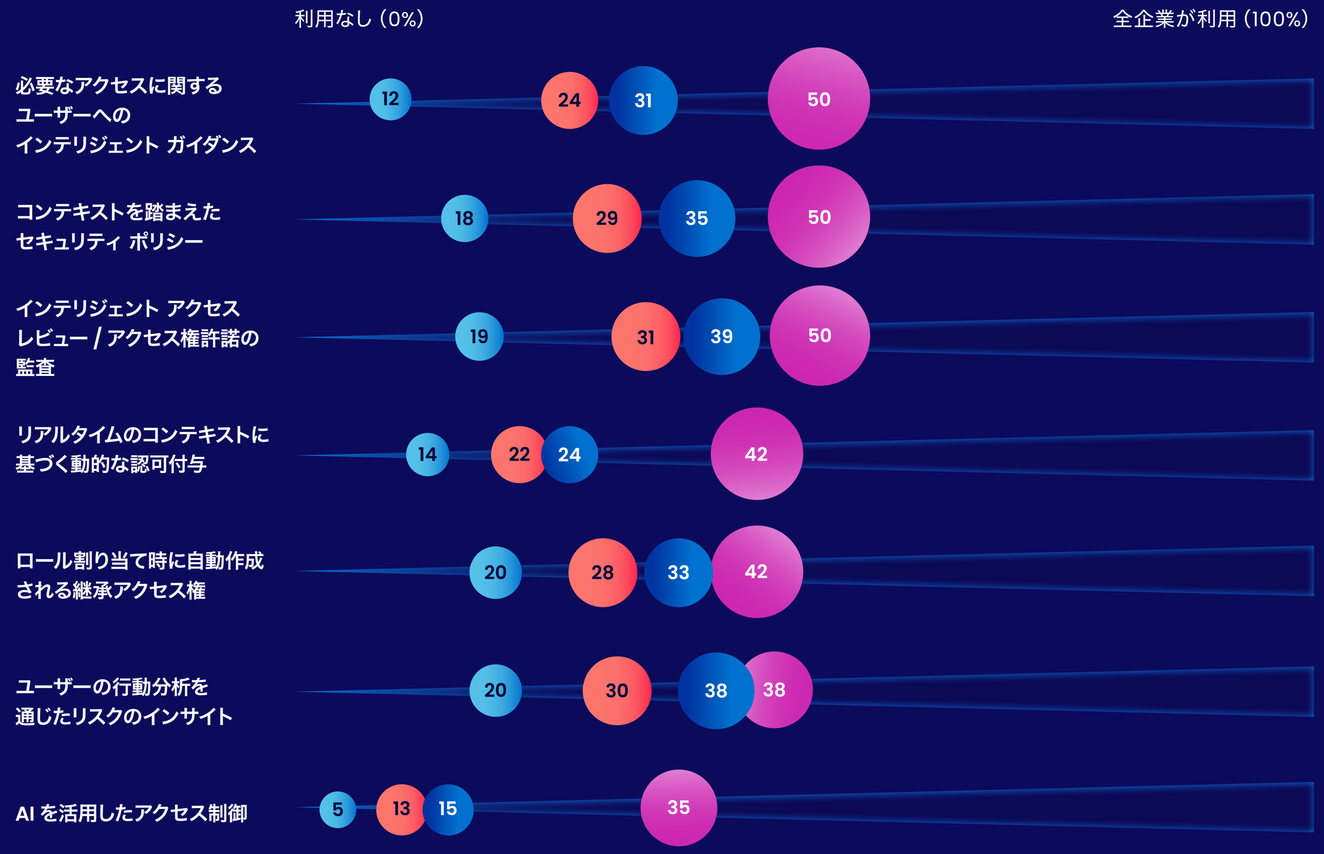
<40%

アイデンティティ インテリジェンス データを大規模に活用している第 3 段階の企業

~50%

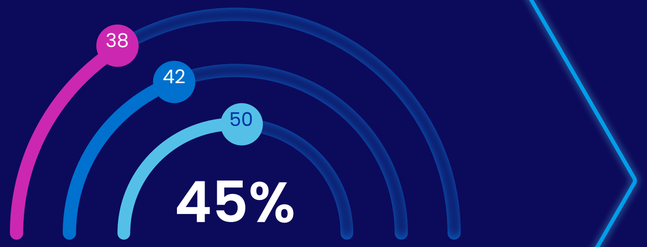
ユーザー アクセス、セキュリティ ポリシー、アクセス レビューの構造化データおよび非構造化データから得られたインテリジェンスを指針として活用している第 4 段階以上の企業

第 1～第 2 段階 | 第 3 段階 | 第 4 段階以上 | 全体 | 全データ

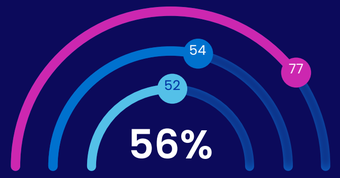


成熟したアイデンティティ セキュリティを備えた企業は、拡張性のある生成 AI を組み合わせた活用に投資する余裕がある

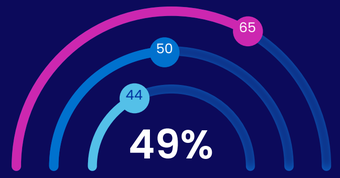
第 3 段階以上の企業は、自社のアイデンティティ セキュリティの強化と拡大を目的とした拡張性の高いソリューションの開発に注力しています。一方、第 1 ～第 2 段階の企業は、同じプロセスを繰り返すようなアクティビティの自動化に注力しています。



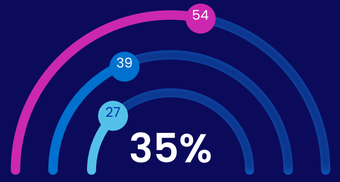
IAM の即時対応とタスク処理を目的とした AI チャットボット



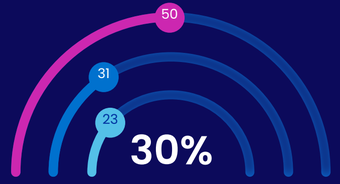
AI を活用したワークフローの作成（ユーザー プロビジョニング、アクセス レビュー、ロール管理など）



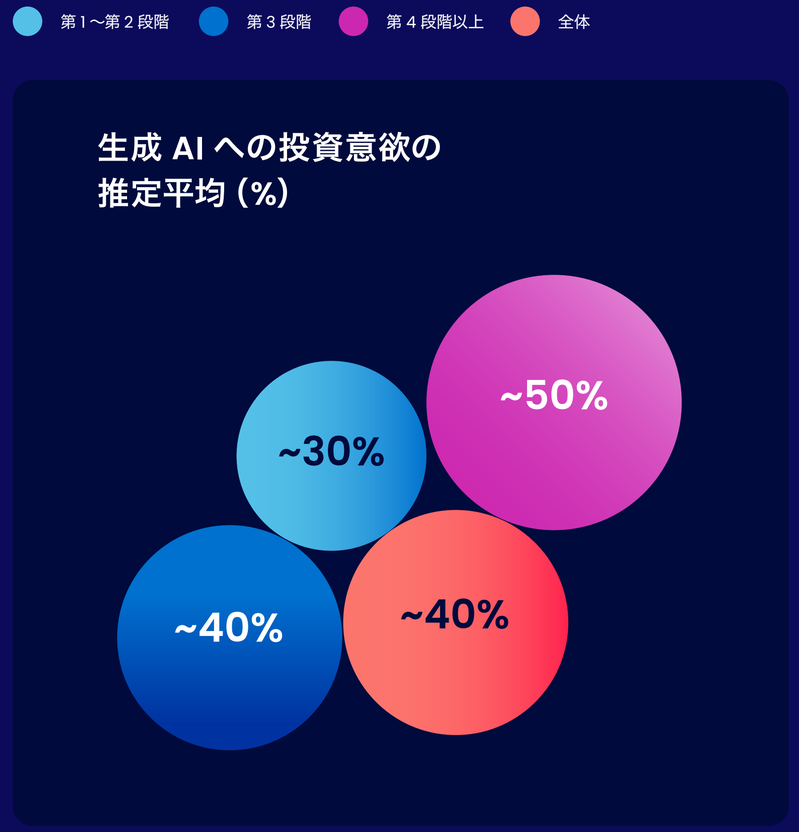
ユーザー エンタイトルメントとロールの説明（権利、特権、アクセス レベルなど）の AI による生成



自然言語での検索による簡便な IAM データの取得



自動化コネクタ開発のための操作支援



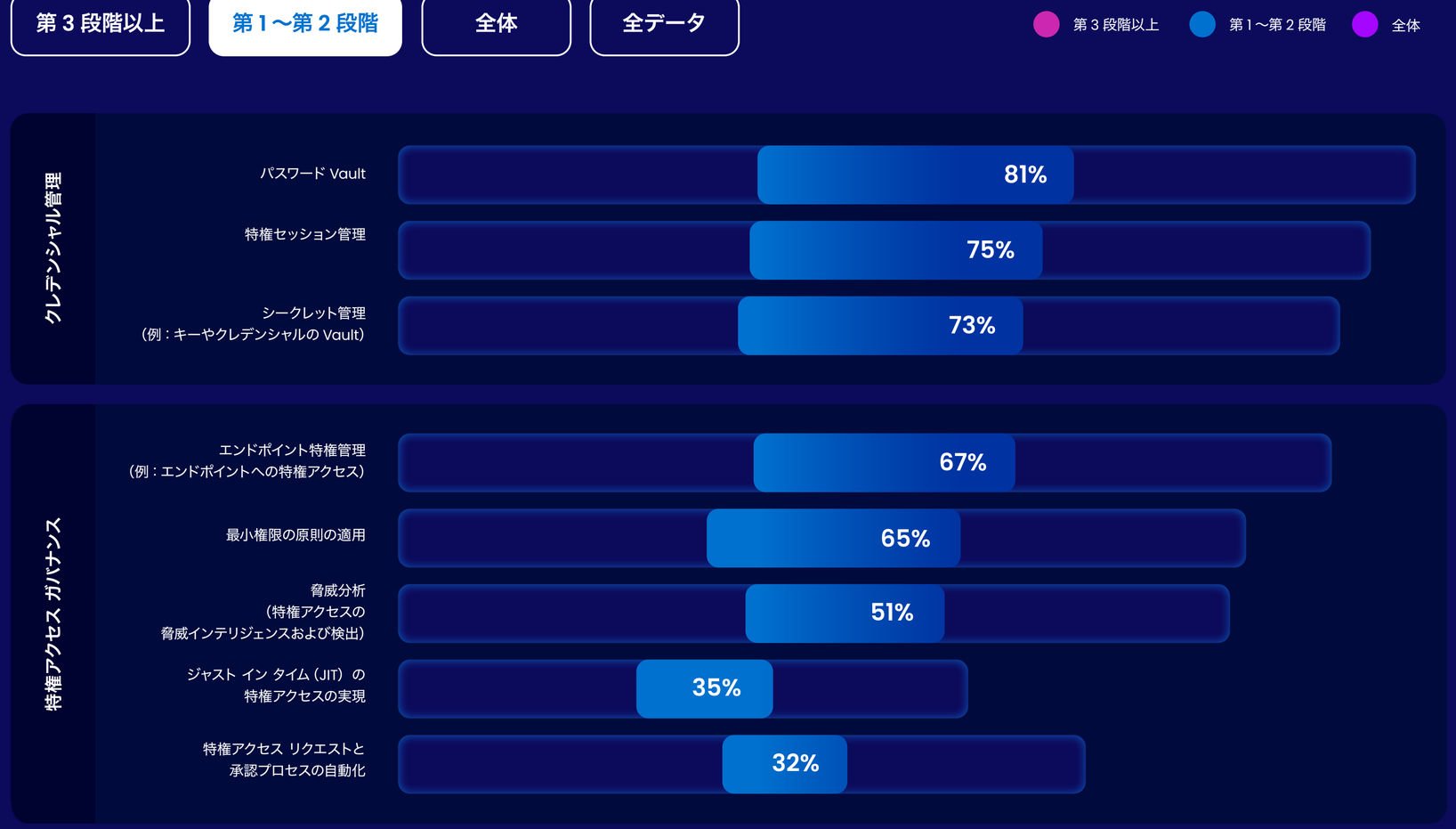
第 3 段階以上の企業は特権アクセス ガバナンス機能の導入率が第 1 ～ 2 段階の企業に比べて 50% 以上高い

クレデンシャル Vault やセッション管理よりもさらに高度なソリューションに投資することで、企業はアクセスの承認やリクエストのプロセスを簡素化しながら、特権アカウントの脅威分析を強化できます。

第 3 段階以上の企業は特権アクセス ガバナンス機能の導入率が第 1 ～ 2 段階の企業に比べて 50% 以上高い

クレデンシャル Vault やセッション管理よりもさらに高度なソリューションに投資することで、企業はアクセスの承認やリクエストのプロセスを簡素化しながら、特権アカウントの脅威分析を強化できます。

第 3 段階以上 | 第 1 ～第 2 段階 | 全体 | 全データ



第 3 段階以上の企業は特権アクセス ガバナンス機能の導入率が第 1 ～ 2 段階の企業に比べて 50% 以上高い

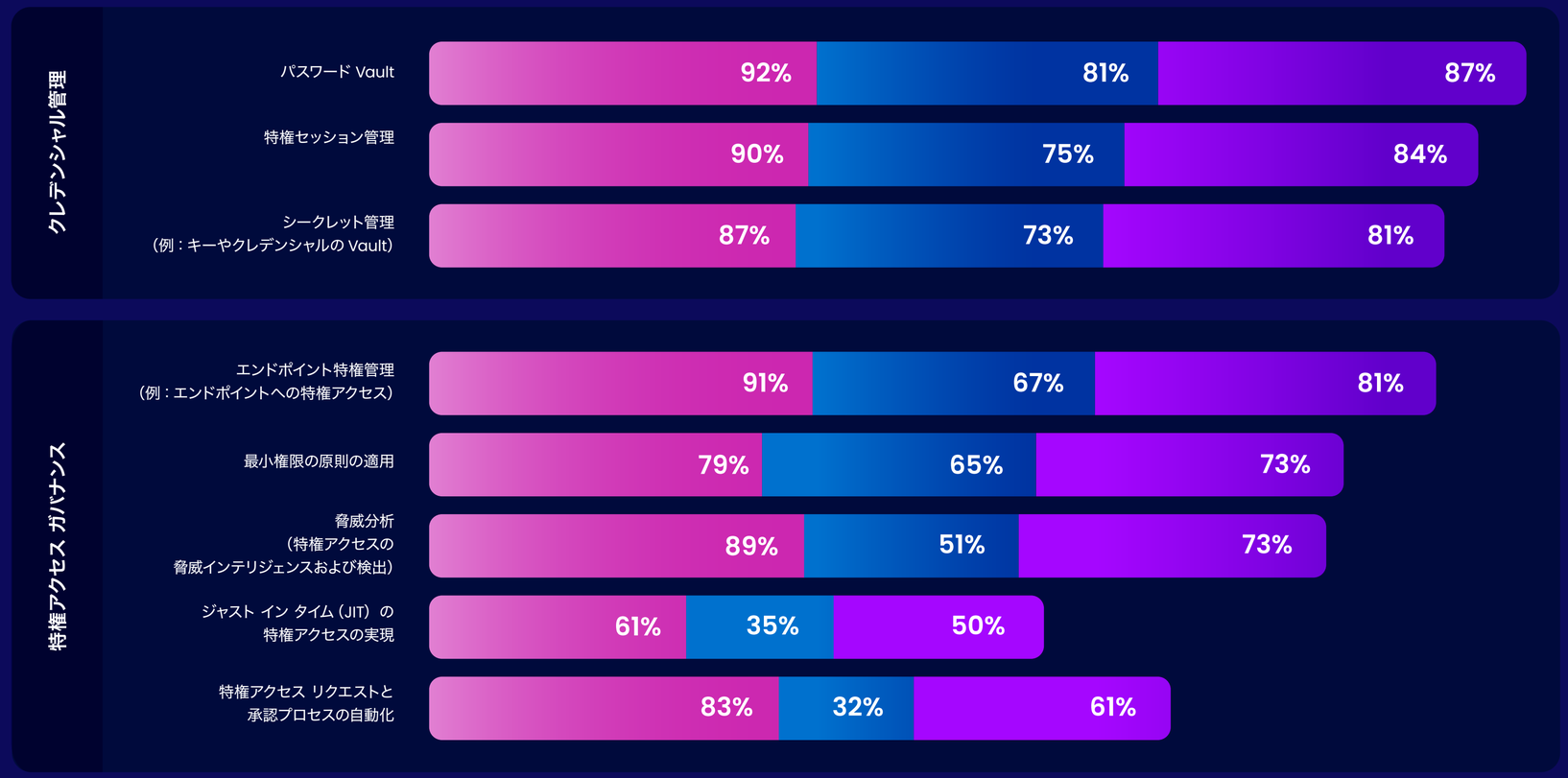
クレデンシャル Vault やセッション管理よりもさらに高度なソリューションに投資することで、企業はアクセスの承認やリクエストのプロセスを簡素化しながら、特権アカウントの脅威分析を強化できます。

第 3 段階以上 | 第 1 ～第 2 段階 | 全体 | 全データ

第 3 段階以上の企業は特権アクセス ガバナンス機能の導入率が第 1 ～ 2 段階の企業に比べて 50% 以上高い

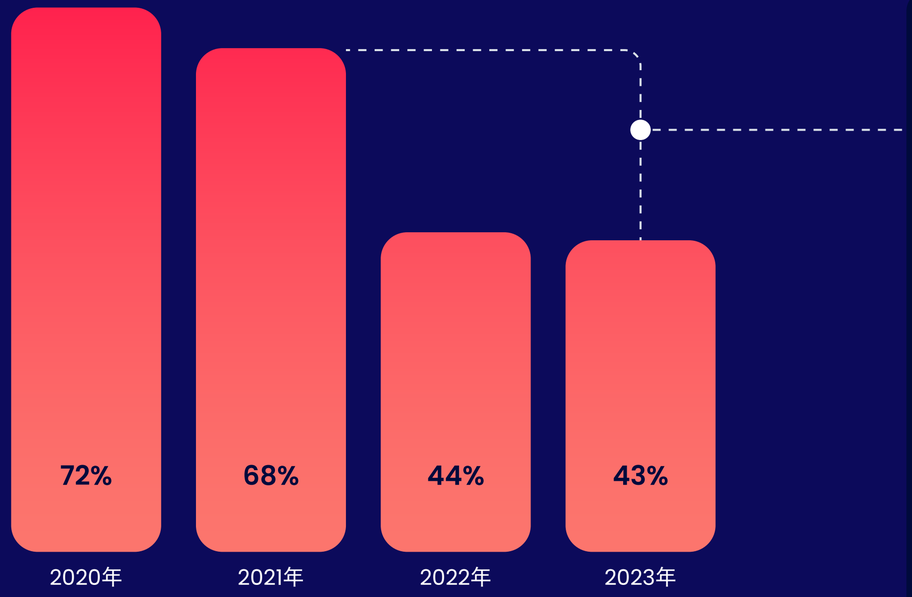
クレデンシャル Vault やセッション管理よりもさらに高度なソリューションに投資することで、企業はアクセスの承認やリクエストのプロセスを簡素化しながら、特権アカウントの脅威分析を強化できます。

第 3 段階以上 | 第 1 ～第 2 段階 | 全体 | 全データ

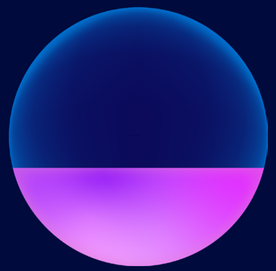


サイバー保険事業者がより成熟した方法でサイバー リスク管理を評価するようになるにつれ、サイバー保険の保険料が高くなる

サイバー保険事業者は損害率を下げ、より成熟した方法でリスク評価と管理を行っています。



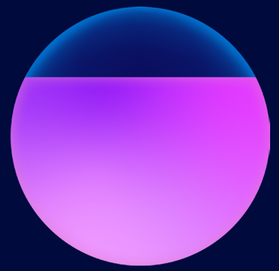
単独でのサイバー保証の損害率、請求に応じて支払われる保険料の負担割合



40%

サイバー保険事業者が支払う損害額の減少は、サイバー リスク管理がより高度化していることを示しています

. . . また、増大するリスク特性に見合うように保険料を見直しています



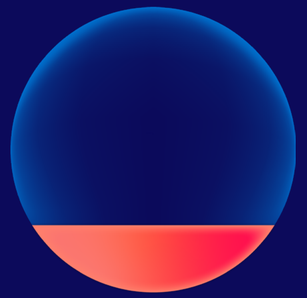
77%

各企業から、直近3年間で保険料が増額したことが報告されています

保険会社は企業によるセキュリティ制御状況をより精査するようになっています。今後、企業が保険料を抑えるためには、新しいセキュリティ制御の実装を働きかけてくる可能性もあります。

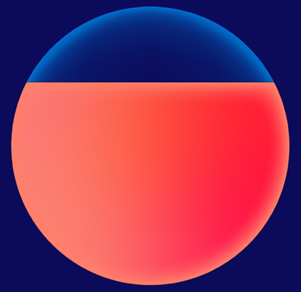
大手証券会社のサイバー保険専門家

サイバー保険の契約企業は、保険の査定時にアイデンティティ セキュリティ機能が最も大きく影響したと報告



25%

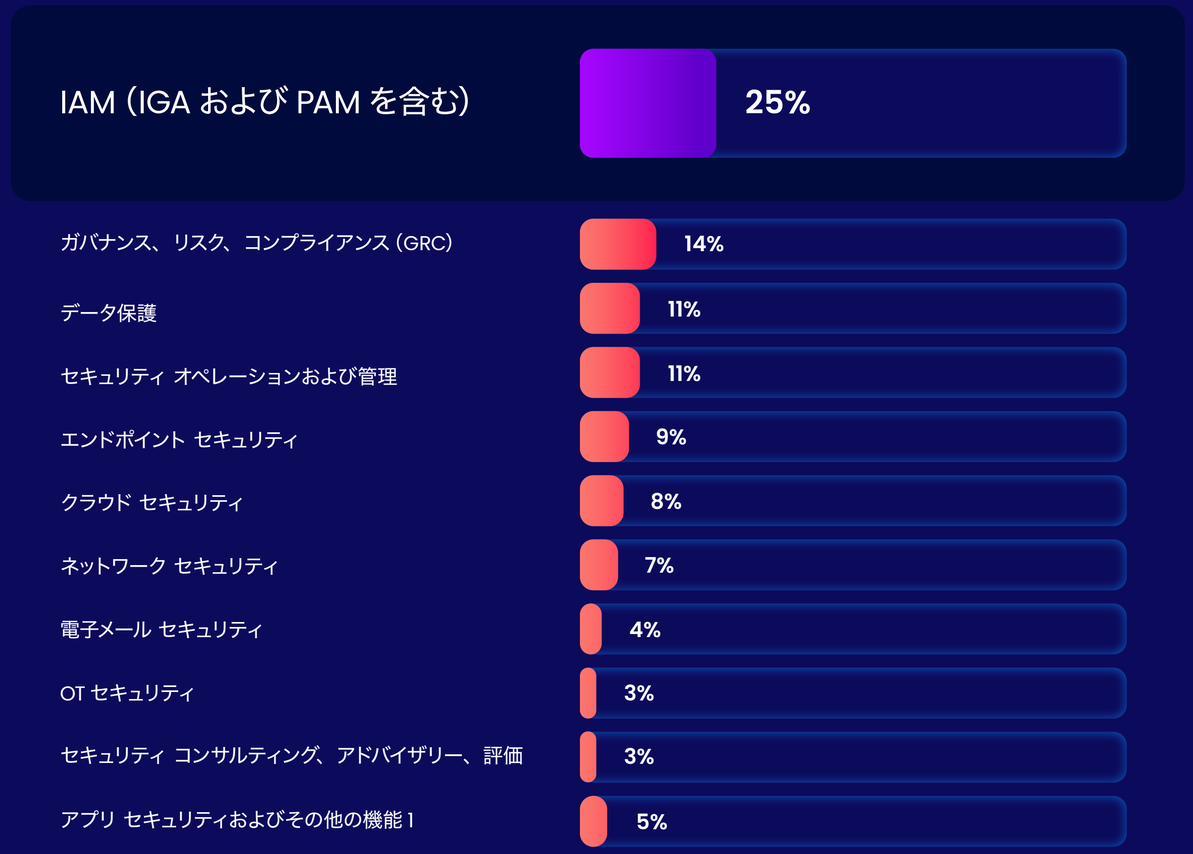
25%の回答者が、IAMはサイバー保険の評価において最重要の要素であり、最も大きな割合を占めると考えています。



73%

73%が、保険の査定に影響する上位3つの機能の1つにIAM機能を挙げています。

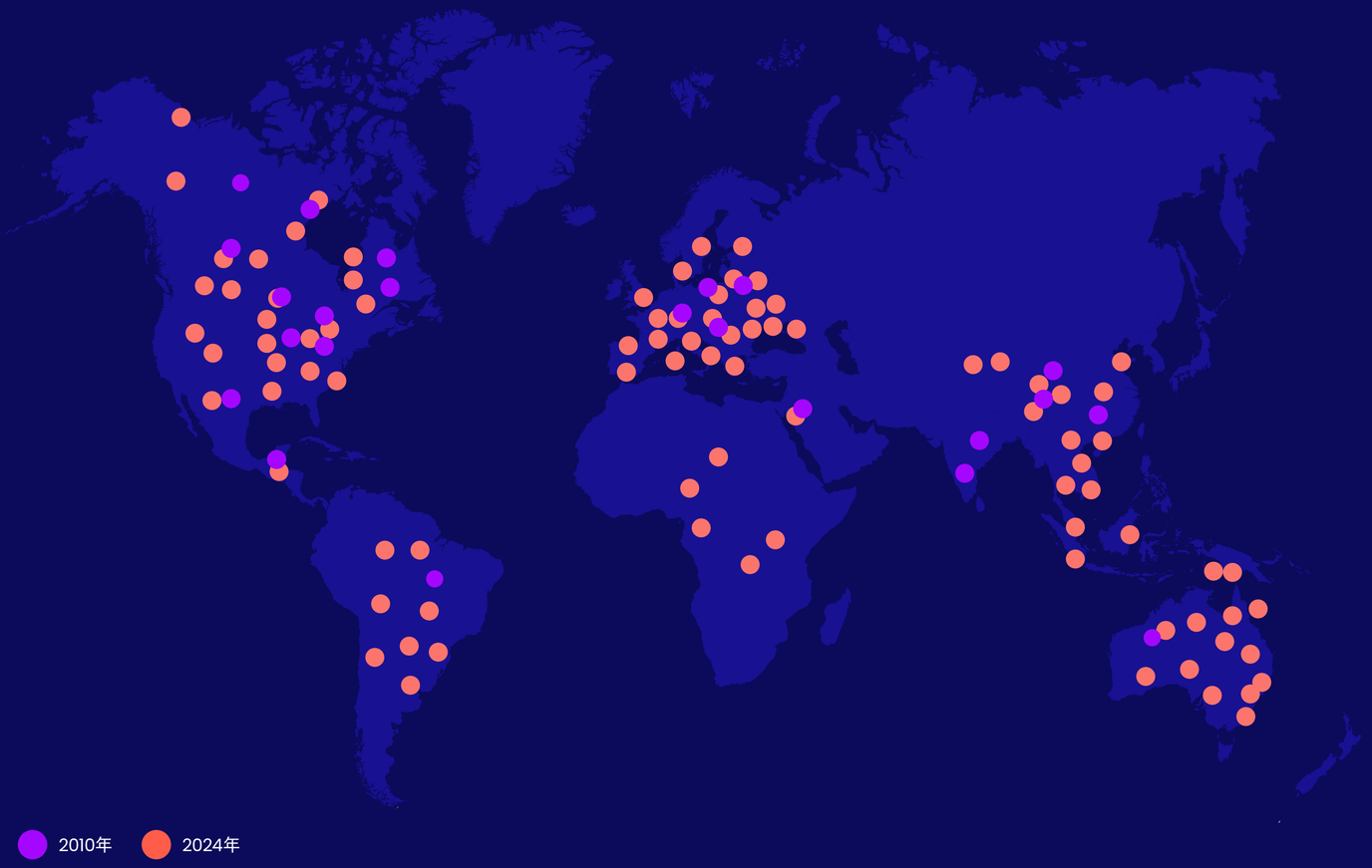
サイバー保険の査定に影響するサイバー セキュリティ機能のランキング（最も影響が大きい機能として選択した回答者の割合）



ウェブ セキュリティおよび MSSP/ アウトソーシングを含む

2010 年以降、アイデンティティ関連の規制は各地域および業界全体で 7 倍にまで増加

すべて | 2010年 | 2024年



5 倍以上の増加

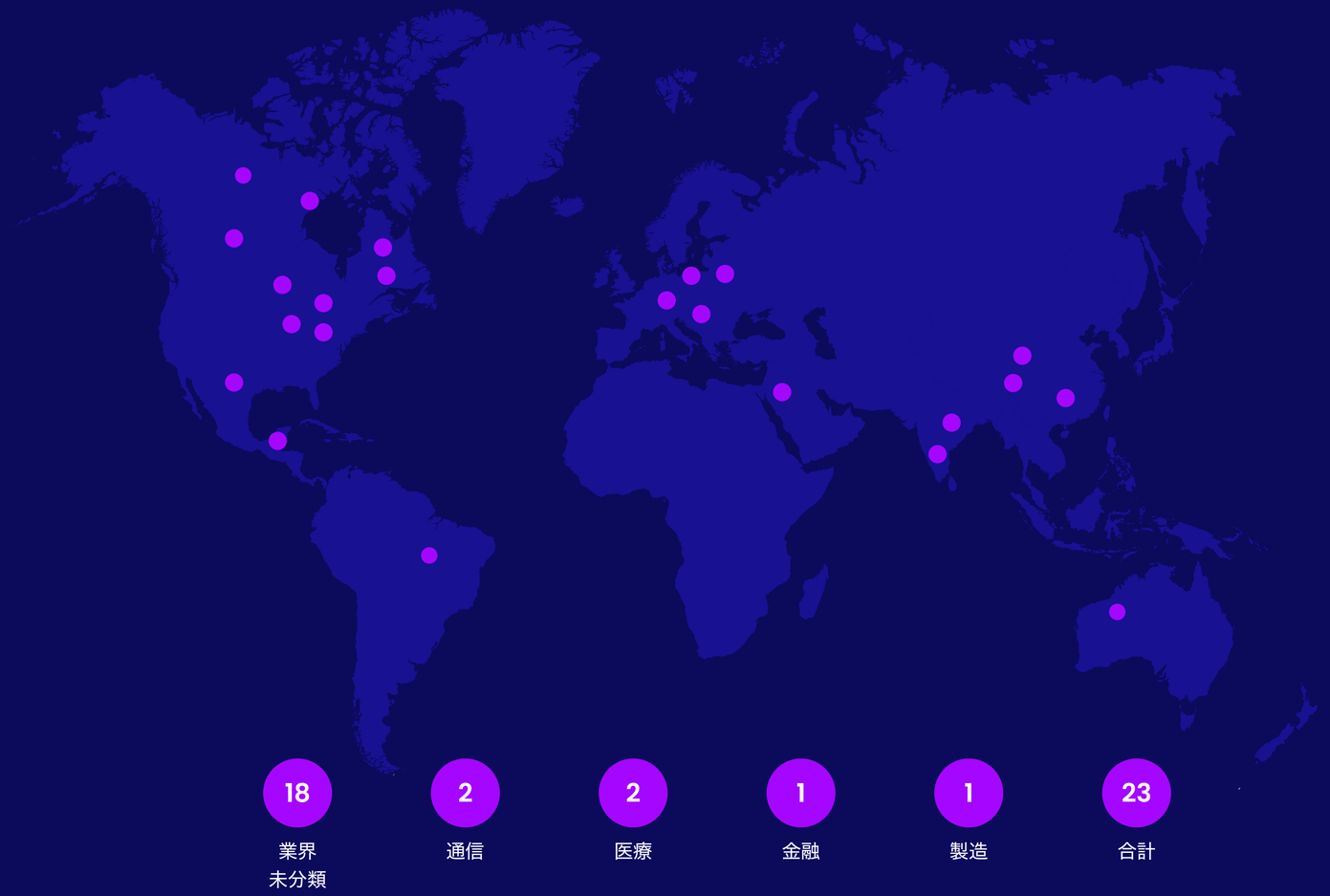
金融および医療以外の業界での規制

13 倍以上の増加

北米、APAC、欧州以外での規制

2010 年以降、アイデンティティ関連の規制は各地域および業界全体で 7 倍にまで増加

All 2010年 2024年



~25

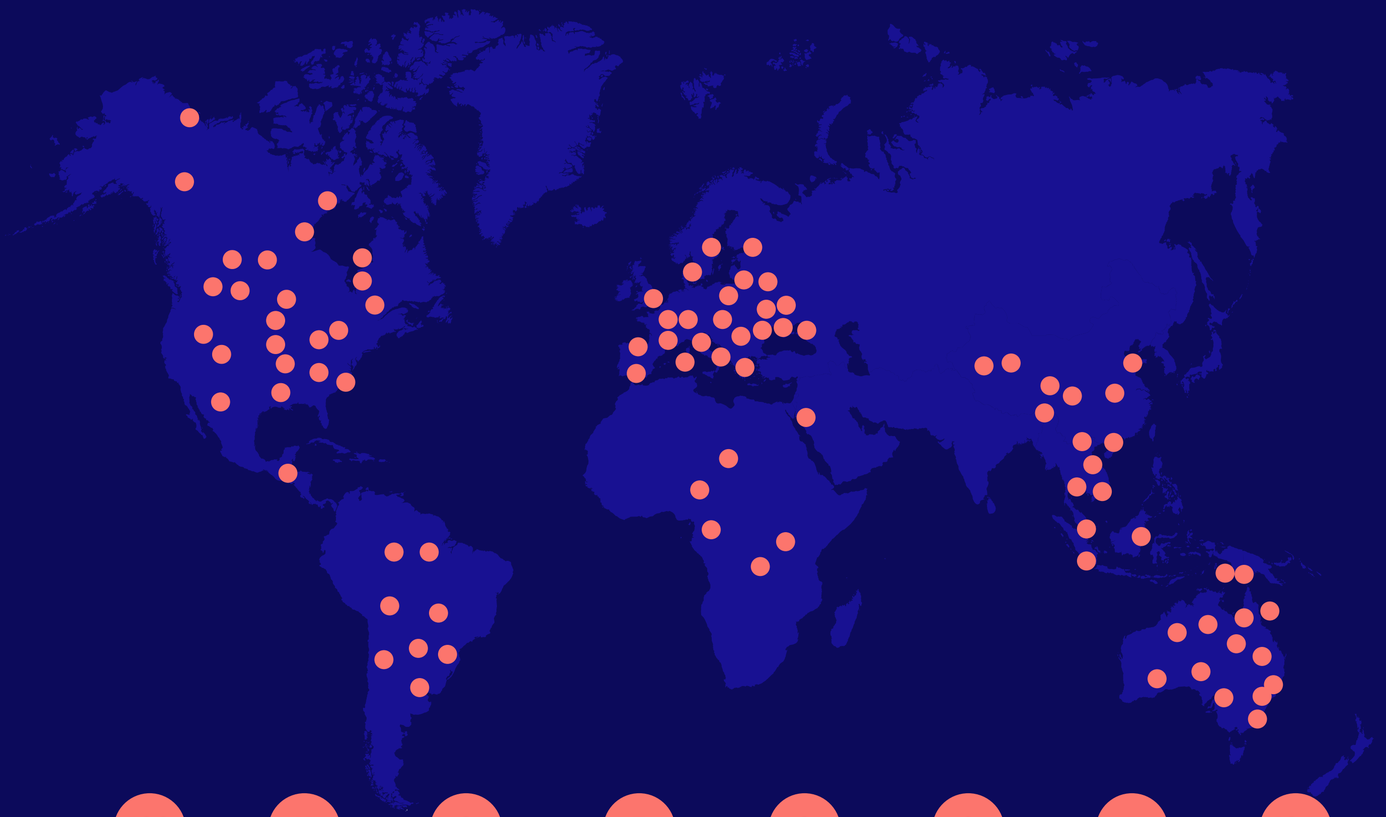
2010 年における成熟度の高い地域と一部の業界に焦点を絞った規制およびフレームワークの合計

2010 年以降、アイデンティティ関連の規制は各地域および業界全体で 7 倍にまで増加

~135

2024 年にすべての地域および業界で大幅な増加を見せた規制およびフレームワーク

All 2010年 2024年



業界未分類	通信	金融	医療	製造	その他	官公庁	合計
103 ~6倍	11 ~5倍	9 9倍	5 ~3倍	3 3倍	2	1	134

第 4 章

大手企業における価値向上の事例

章の開始 →

ケース スタディ
BNP パリバ銀行
製薬会社
Absa
Currys

企業の ケース スタディ

世界中の多様な業界で、大手企業がアイデンティティ セキュリティに投資しています。その結果として、サイバー セキュリティの価値を高め、コンプライアンス、オペレーション効率、ユーザーの生産性、セキュリティにおいて非常に大きなリターンを実現しています。

BNP PARIBAS

目標：

サイバー リスクを軽減し生産性を向上

BNP パリバ銀行のポーランド支店は、手作業による IAM タスクを大規模に自動化することで生産性を大きく向上させました。

合併が相次いでいた同銀行では、IAM プログラムが連携されていない状態で、1 万人のユーザーと 1,000 近いアプリケーションを管理していました。IT チームが大量のユーザー リクエストや IAM タスクに対応するには自動化が不可欠でした。自動化することで、わずか 2 名の従業員がそれぞれの勤務時間の 15% 程度を割り当てるだけで、権限審査や棚卸まですべてを管理できるようになりました。

ケース スタディを見る →

40,000
毎月実行される
自動アイデンティティ
タスク数

90%
のアクセス権限の
申請・付与を自動化

40,000
毎月自動で行われる
リセット数および
パスワード変更数

目標：

生産性

7 万 2 千名の従業員を抱える大手製薬会社は、自動 IAM タスクによって生産性と効率性を高めています。

同社では、既存のオンプレミス アイデンティティ ソリューションの保守に多大な手作業を要しており、それに代わる拡張性に優れたクラウドベースのシステムを検討していました。新しいクラウドベースのシステムを導入したことで、簡潔な手順で法規制を遵守できるようになり、アクセス レビューにかかる時間やアクセスまでの待機時間が顕著に短縮されました。

40%
アクセス レビューに要する時間を短縮

20%
アクセスまでの待機時間を短縮

30%
IT オペレーションにおける手作業によるタスクを削減

目標：

ビジネス価値の増加

3 万 5 千人以上の従業員を有するアフリカの金融サービス会社である Absa 社は、オンボーディングおよびサードパーティ アイデンティティ管理を効率化することで、コスト削減に成功しています。

同社では、AI ベースのリスク管理ツールを導入し、GDPR（EU 一般データ保護規則）と POPIA（個人情報保護法）の規制に対応可能なプロビジョニング機能とサードパーティ アイデンティティの権限審査（棚卸）機能を手にしました。このツールの導入により、オペレーションの負荷を軽減するとともに、契約社員や非正規社員のアイデンティティ ガバナンスを簡素化することに成功しています。

ケース スタディを見る →

300 ドル
アイデンティティ オンボーディング 1 回あたりの削減額

15 日
サードパーティ アイデンティティのオンボーディング日数を短縮

1.2 万
アイデンティティの保護対象となった非正規社員数

currys

目標：
サイバー リスクの軽減

英国を拠点に 800 以上の店舗を展開する大手量販店の Currys 社は、アイデンティティ ガバナンスを強化し、アイデンティティ セキュリティを自動化することで、リスクを軽減しました。

以前は Excel をベースとした手作業のプロセスに依存しており、常に一定数の従業員を確保して交代で対応していました。そのため、オーバー プロビジョニングとコンプライアンス上のリスクが生じていましたが、自動化により完全な監査証跡が作成されるようになりました。また、コンプライアンス上の課題が解消されるとともに、アクセス権が割り当てられながら実行されないようなケースを最小限に抑え、セキュリティ体制全体を底上げできました。

ケース スタディを見る →

3 倍
約 6,000 個のアカウントに適切な権限を設定することでリスクを軽減

210
手作業の削減時間（年間）

24,000
管理しているアイデンティティ数

世界規模のテクノロジー グループである Aboitiz は、「Great Transformation」イニシアチブにより、24 か月でアイデンティティ セキュリティの成熟度が第 1 段階から第 3 段階以上へと一気に移行しました。

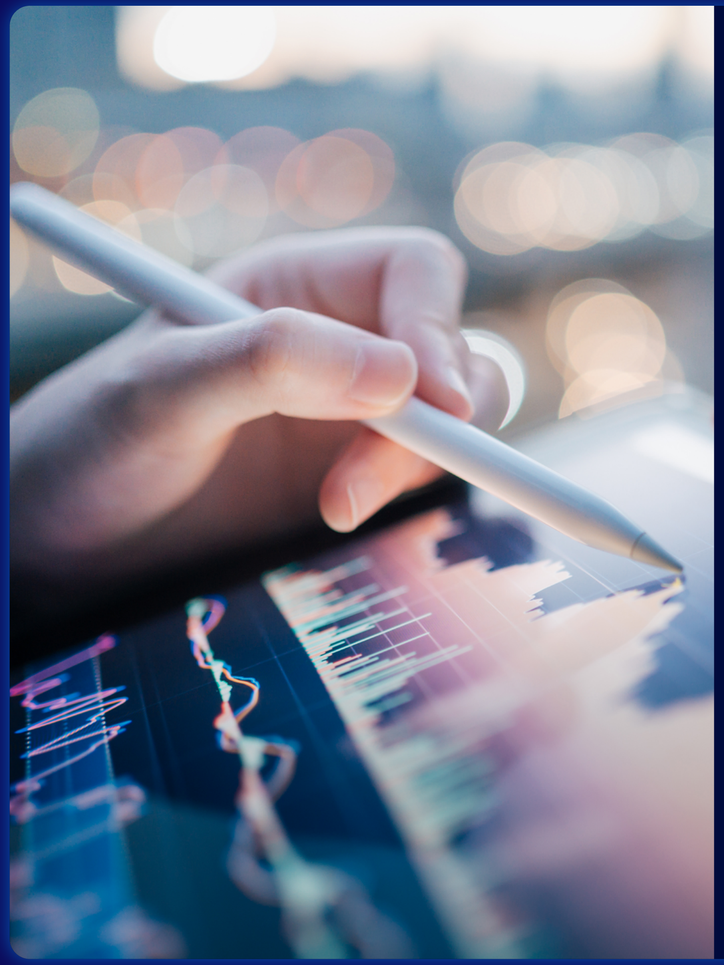
各項目にマウスポインタを合わせると、実施されたアクションを確認できます

0 従来の手順に沿った アイデンティティ アクセス管理 プロセス	21 非アクティブ化までの日数 ユーザー アカウントの アクティブ化には 5 日間	<5 一元化されたアイデンティティ ガバナンスを使用する ビジネス ユニット数	<1,000 自動化プロセスを通じて管理される アカウント数
1 統合アイデンティティ アクセス 管理プログラムにより、すべての スタッフ アカウントを管理	0 即時プロビジョニングおよび デプロビジョニングによる 待機時間	47 約 23,000 のアプリケーション アカウントに対し一元化された ガバナンスを使用する ビジネス ユニット数	144,000 アカウント変更および 検証の自動化

第 1 段階 (2020 年)

第 3 段階以上 (2022 年)

ケース スタディを見る →



何もないところから始めたのですが、テクノロジーを使用して一気に変革を実現することができました。組織の最も重要な資産であるアイデンティティに時間と労力を投資するという重大な決断が功を奏しました。

CISO, Aboitiz Equity Ventures

aboitiz

第 5 章

成熟度を高めるためにできること

章の開始 →

次の段階への道のり

1. ビジョンを設定する
2. 適切なソリューション、特に AI の活用によって初期段階を省略し、より高いリターンが得られるソリューションに投資する
3. すべてのアイデンティティタイプを保護する
4. セキュリティオペレーションと IAM をより広範に統合し、継続的な監視と保険料の制御を行う
5. アイデンティティ データからインサイトと適用可能なセキュリティポリシーを導き出す
6. 今後新たに生じる規制や標準にあらかじめ対応し、コンプライアンスを遵守

SailPoint

アイデンティティ セキュリティの成熟度について自社の段階のご確認にお役立てください

成熟度を診断

すべてのレポートをダウンロードする

IB2571-2502