プライバシーの利点：デジタル世界における信頼の構築

シスコ 2025 データ プライバシー ベンチマーク調査

目次

はじめに

過去 10 年間、組織はプライバシーに関するリソースと投資を着実に増加させてきました。当初はコンプライアンスの必要性が原動力となっていましたが、これまでの取り組みにより、顧客の信頼を獲得し、構築し、維持するための基盤として、プライバシーがより広範な価値を持っていることが明らかになりました。生成人工知能（生成 AI）の台頭により、組織はプライバシーへの取り組みの次の段階に直面しています。2025 データ プライバシー ベンチマーク調査では、業界の現状を示す重要なテーマを取り上げています。それは、データローカリゼーションの重視とグローバルプロバイダーの優先、信頼を構築する力となるプライバシー規制、プライバシーと AI ガバナンスの共通の基盤です。

評価方法

本レポートは、2024 年秋に実施された、セキュリティおよびプライバシーの専門家を対象とした匿名の調査で収集されたデータに基づくものであり、回答者は誰が調査を実施しているのか知らされておらず、調査者も誰が回答しているのか知らされていません。調査には、12 か国（ヨーロッパ 5 か国、アジア 4 か国、南北アメリカ 3 か国）の 2,600 人以上が参加しています。[1] 回答者は、自分の組織におけるプライバシーへの取り組みと支出、プライバシー保護法への対応、AI、データローカリゼーション要件について尋ねられました。今回の調査結果は、企業にとって、また企業が顧客にサービスを提供するうえで、プライバシーが引き続き重要であることを示しています。

[1] オーストラリア、ブラジル、中国、フランス、ドイツ、インド、イタリア、日本、メキシコ、スペイン、英国、米国。

主な調査結果

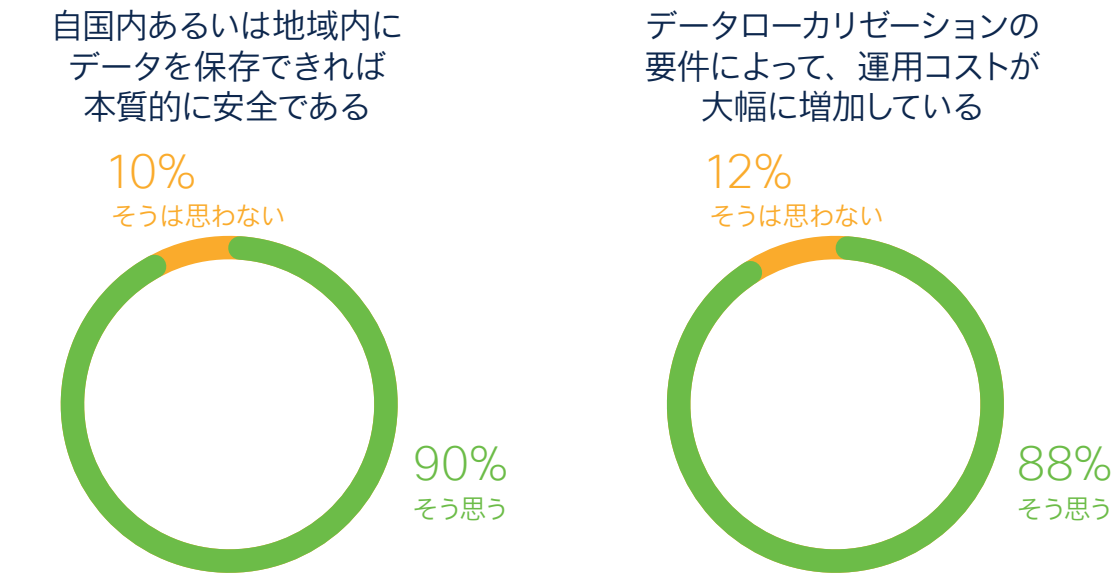
1. データと AI に世界的な注目が集まる中、回答者の 90% が、国内あるいは域内にデータを保存した方が本質的に安全であると考えています。その一方で 91% は、ローカルプロバイダーよりもグローバルプロバイダーの方がデータを適切に保護できると考えています。
2. プライバシー保護法に対する支持は高まり続けており、86%（前年比 6% 増）の組織が、法律がプラスの影響を与えていると回答しています。
3. 組織は引き続き、プライバシーへの投資から得られた価値を実感しています。予算は前年比で安定しており、回答者の 96% がコストを上回るメリットがあると回答しています。
4. AI への理解度が高まり、その価値が実感されるようになった一方で、潜在的なリスクに関する懸念は依然として残っています。興味深いことに、回答者が新しいテクノロジーに慣れ、AI ガバナンスフレームワークを導入するにつれて、法的リスクへの懸念は減少しています。
5. AI のポテンシャルを認識した組織は、AI への注力と予算の拡大を見込んでいます。こうした成長は、堅牢なデータプライバシーとサイバーセキュリティ プログラムを維持するという継続的なニーズと結び付いています。

調査結果

1. データの安全性とセキュリティに関する認識がローカリゼーションを推進

何十年もの間、デジタル経済は経済成長を促進するうえで重要な役割を果たし、規模や業界を問わず、さまざまな企業が世界中のデータの動きに依存してきました。しかし近年、多くの地域でデータローカリゼーションへの関心が高まっています。シスコ 2024 データ プライバシー ベンチマーク調査と同様に、回答者の大多数（90%）が、ローカル、つまり自国内にデータを保存した方がより安全だと考えています。プロバイダーに関係なく、データをローカルに保存するには多額のコストがかかるかどうかを尋ねたところ、88% が「そう思う」と回答しました（2023 年は 85%）。この 2 つの回答を組み合わせると、追加コストがかかってもデータをローカルに保持したいという意向が強まっていることが分かります。図 1 を参照してください。

図 1. データローカリゼーション



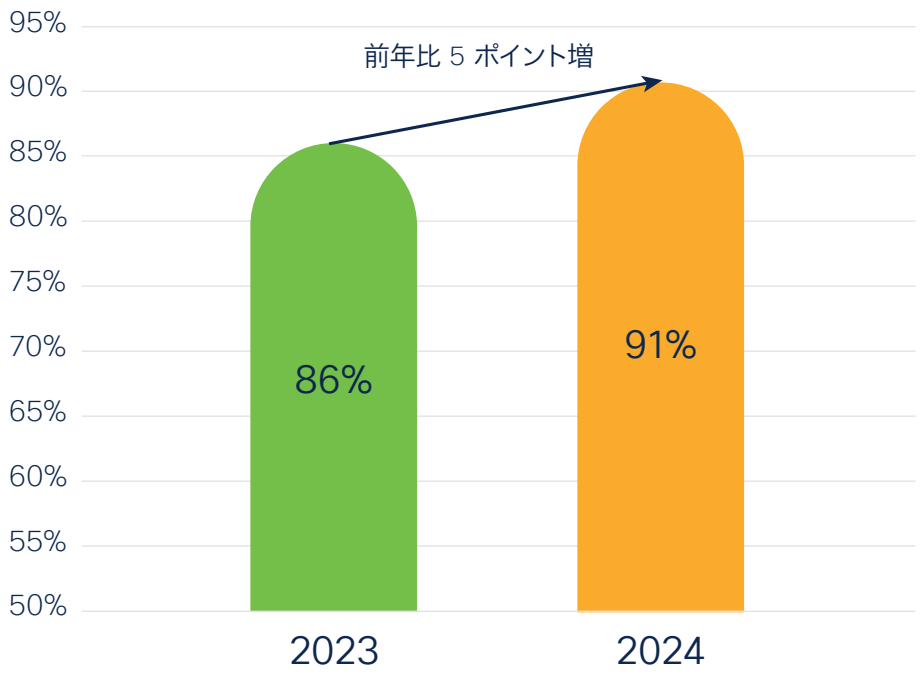
出典：シスコ 2025 データ プライバシー ベンチマーク調査

「プライバシーは今日のデジタル経済における信頼の核心であり、競争的差別化要因です」

Harvey Jang、シスコ バイスプレジデント、副法務顧問、最高プライバシー責任者

また、回答者の 91%（他の設問よりわずかに高い割合）が、特定の国や地域にサービスを提供するローカルプロバイダーよりも、グローバルプロバイダーの方がデータを適切に保護できると考えています。注目すべきなのは、この割合が昨年から 5 ポイント上昇していることです。この上昇幅は、多国籍プロバイダーが地域内データストレージ機能を導入する傾向が高まっていることを反映していると考えられます。これにより、回答者は特定のデータレジデンシーに関する要望や要件を満たしつつ、グローバルな規模と専門性の両方のメリットを享受できるようになりました。データローカリゼーションとグローバルプロバイダーの両方が同じように強く支持されているのは一見矛盾しているように思えるかもしれませんが、現在の状況ではこれは理にかなった結果だと言えます。データの価値がますます高まる中、企業も消費者も、堅牢な保護対策を期待し、要求しているのです。図 2 を参照してください。

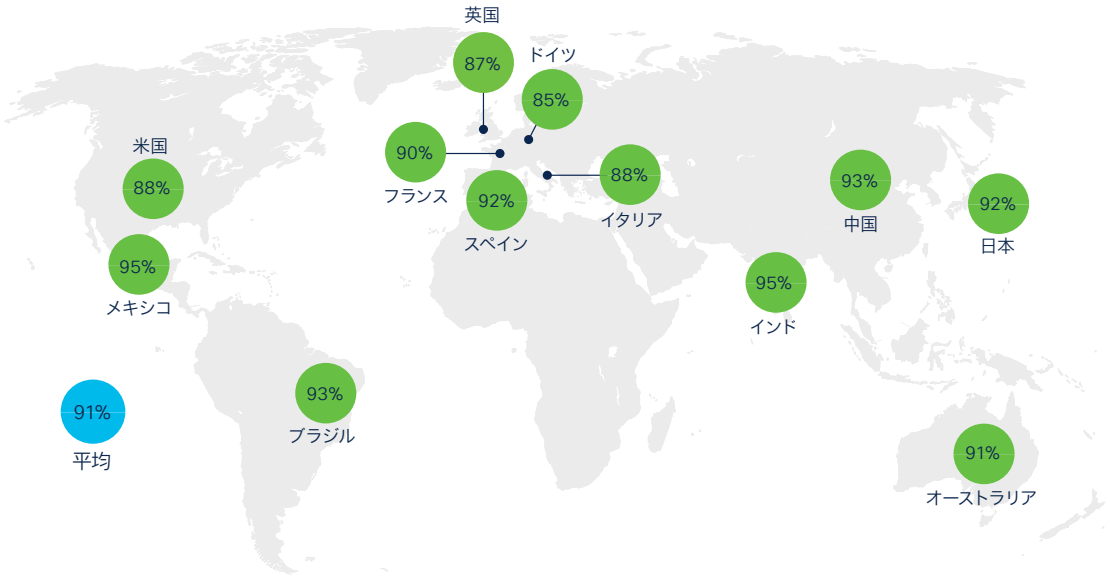
図 2. ローカルプロバイダーよりもグローバルプロバイダーの方がデータを適切に保護できる



出典：シスコ 2025 データ プライバシー ベンチマーク調査

また、データローカリゼーションへの対応が国によって異なることを踏まえると、現地の規制に応じてグローバル データ プロバイダーの優先度が変わってくると予想されます。しかし、ローカルプロバイダーよりグローバルプロバイダーを支持する傾向は、調査対象となった地域全体でほぼ一貫しています。図 3 を参照してください。

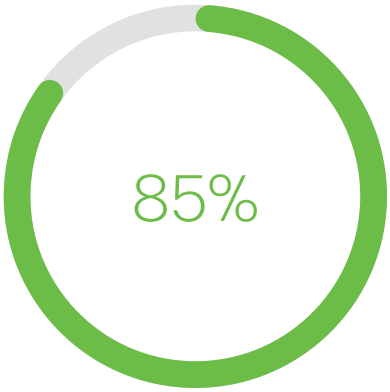
図 3. ローカルプロバイダーよりもグローバルプロバイダーの方がデータを適切に保護できると答えた回答者（国別）



出典：シスコ 2025 データ プライバシー ベンチマーク調査

回答者は、ローカルにデータを保存した方がより安全だと強く確信していますが、規制が国ごとに異なるため、グローバル企業にとっては複雑さが増しています。経済協力開発機構（OECD）によると、データローカリゼーション要件は 40 か国で 100 件を超えています。[2] このようにローカリゼーションが進む中、一部の政府は、一貫性のあるデータ保護の基盤に基づく貿易協定やデジタル契約を結び、相互運用可能なデータ流通の実現に取り組んでいます。具体的には、信頼に基づく自由なデータ流通（DFFT）という G20 のイニシアチブ（OECD が支援）、グローバル越境プライバシー ルール フォーラム、EU と英国間の貿易・協力協定などです。これらは、各国のデータガバナンスシステムを相互運用できるようにし、過度に厳格なデータおよびインフラストラクチャのローカリゼーションを禁止することを目的としています。信頼に基づく自由なデータ流通が経済成長を促進できるかどうか尋ねたところ、85% の回答者が「そう思う」と回答しました。これは、今日のグローバルなデジタル経済に不可欠な国境を越えたデータの流通を今後も安全な形で実現していく方法を見つけることに対する組織の関心とニーズを示しています。図 4 を参照してください。

図 4.「信頼に基づく自由なデータ流通」で経済成長を促進できる



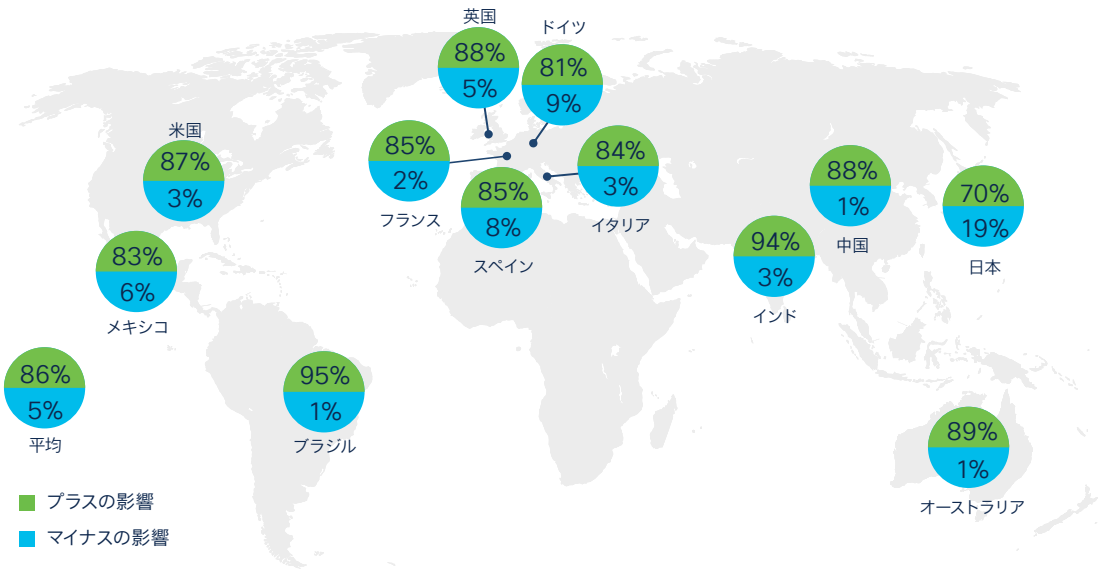
出典：シスコ 2025 データ プライバシー ベンチマーク調査

[2] Del Giovane, C., J. Ferencz and J. López González (2023)、『The Nature, Evolution and Potential Implications of Data Localisation Measures』、OECD Trade Policy Papers、No. 278、OECD Publishing、Paris、https://doi.org/10.1787/179f718a-en

2. 規制は信頼の源泉であり続ける

プライバシー保護法を遵守するには投資が必要です。本レポートの後半で取り上げますが、これらの規制は有益であると広く見なされており、顧客からの信頼と信用を高める構造的なフレームワークを提供しているという点が特に評価されています。この肯定的な考えはデータによって裏付けられており、回答者の 86% が、プライバシー保護法は自社にプラスの影響を与えていると答えています（シスコ 2024 データ プライバシー ベンチマーク調査の 80% から増加）。図 5 を参照してください。

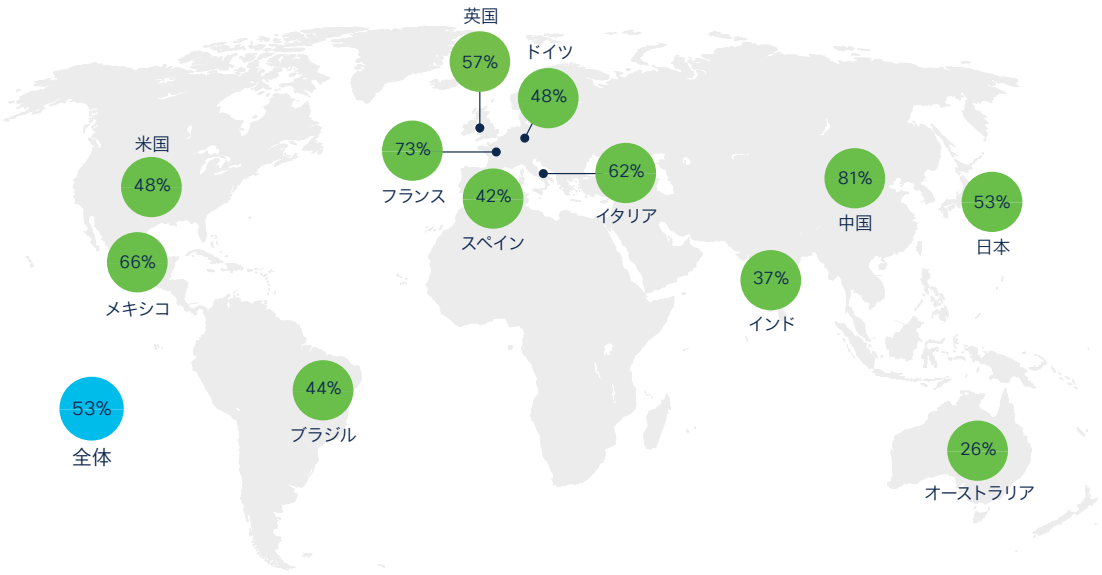
図 5. プライバシー保護法が組織に与える影響



出典：シスコ 2025 データ プライバシー ベンチマーク調査

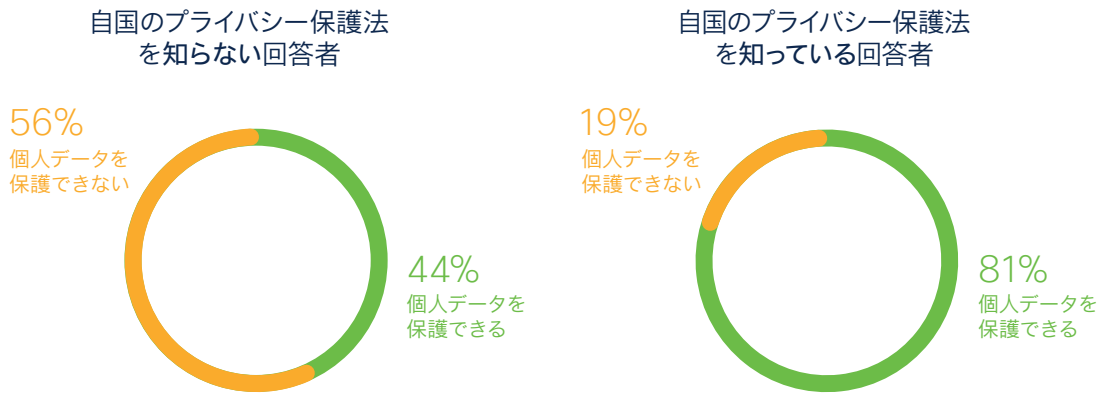
シスコ 2024 コンシューマプライバシー調査からインサイトを導き出すことで、このデータに興味深い背景情報が追加されます。2019 年にこの調査を開始して以来初めて、世界の消費者の過半数 (53%) が自国のプライバシー保護法を知っていると回答しました。プライバシー保護法に対する認知度は、消費者の信頼と密接に関連しています。自国のプライバシー保護法を知らなかった回答者のうち、個人データを保護できると回答したのは 44% のみでした。一方、プライバシー保護法を知っている回答者の 81% が個人データを保護できると回答しており、規制が消費者の信頼を高める要因として重要な役割を果たしていることが明らかになっています。図 6 と図 7 を参照してください。

図 6. プライバシー保護法の認知度 (国別)



出典 : シスコ 2024 コンシューマプライバシー調査 (6 ページ、図 3)

図 7. プライバシー保護法の認知度とデータ保護能力



出典 : シスコ 2024 コンシューマプライバシー調査 (6 ページ、図 2)

3. プライバシーへの投資が組織にもたらすメリット

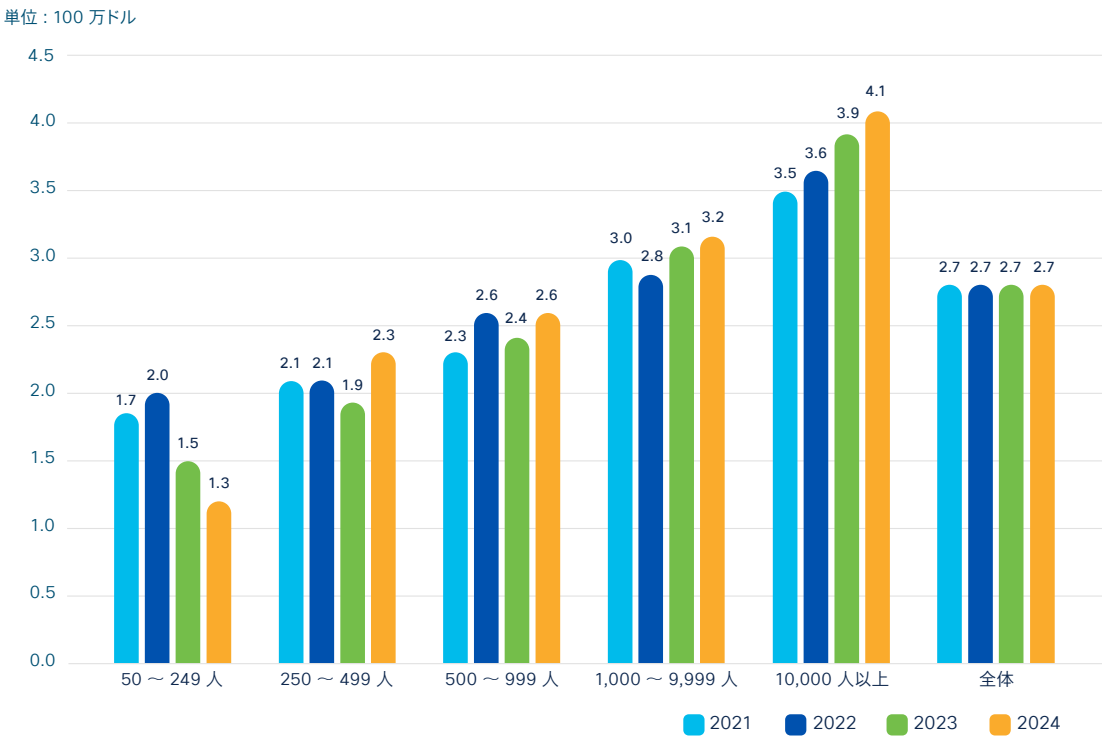
データプライバシー規制を遵守するには、多くのリソースが必要です。データのカタログ化、制御機能の導入、影響評価と利益のバランス調整、顧客や関係者とのコミュニケーション手段の強化などです。しかし、ほとんどの回答者は、こうした規制がビジネス価値を生み出すうえで重要な役割を果たすことを理解しています。今年は、調査対象となった組織の 96% が、プライバシーへの投資から得られるメリットはコストを上回ると回答しています。図 8 を参照してください。

図 8. プライバシーへの投資から得られるメリットはコストを上回る

出典 : シスコ 2025 データ プライバシー ベンチマーク調査

コンプライアンスに関連するメリットに対する組織の評価の高さは、過去 4 年間でデータプライバシーへの支出が一貫していることに表れており、組織全体での平均支出額は 270 万ドルでした。中規模組織（従業員数 250 ～ 499 人）、大規模組織（従業員 500 ～ 999 人）、大企業（従業員数 1,000 ～ 9,999 人）、超大企業（従業員数 10,000 人以上）のいずれも、前年比で支出が増加しています。これに対し、小規模組織（従業員数 50 ～ 249 人）では支出が減少しています。図 9 を参照してください。

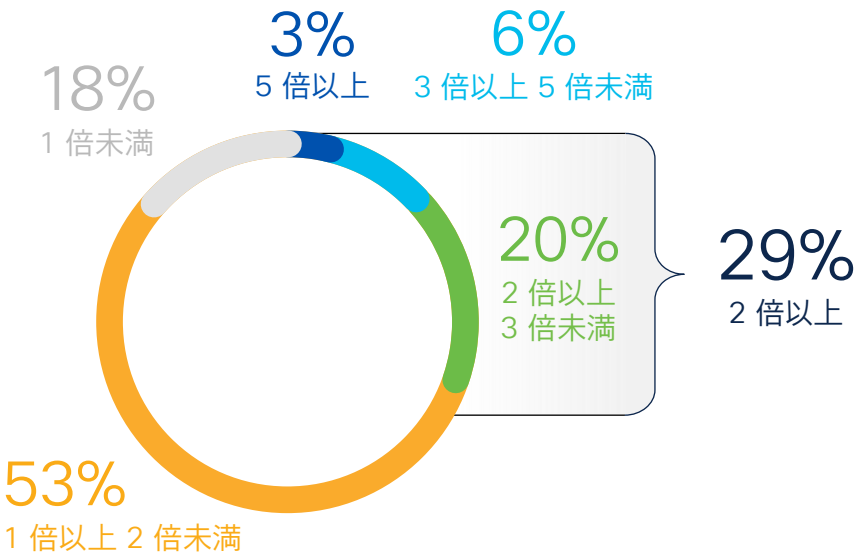
図 9. プライバシーへの支出額



注:一貫性を保つために、2023 年の全体的な支出（270 万ドル）は、過去の企業規模の構成に基づいています。
出典 : シスコ 2025 データ プライバシー ベンチマーク調査

投資の価値については、調査対象の組織の大半（53%）が、プライバシーへの支出に対する ROI（投資利益率）が 1 ～ 2 倍（中央値は 1.6 倍）だったと回答しています。図 10 を参照してください。

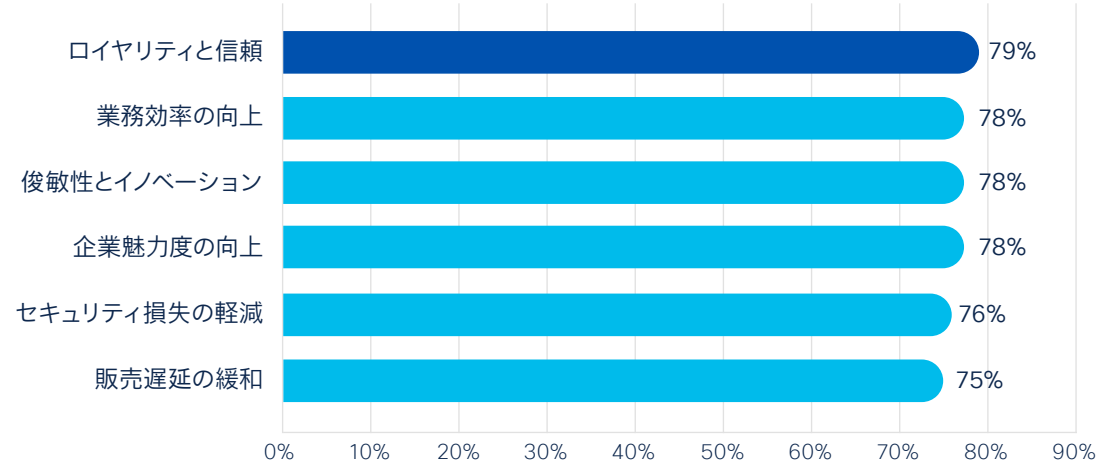
図 10. 回答者の ROI の範囲（2024 年の推定）



出典：シスコ 2025 データ プライバシー ベンチマーク調査

プライバシーへの投資に対するリターンの性質をより深く理解するために、回答者に具体的なメリットについて尋ねました。回答者の少なくとも 75% が、販売遅延の緩和、セキュリティ損失の軽減、企業魅力の向上、俊敏性とイノベーションの促進、業務効率の向上、顧客のロイヤリティと信頼の強化などのメリットを挙げています。注目すべきは、プライバシーへの投資により組織の魅力が高まったという回答の割合が、前年比で 75% から 78% に増加していることです。2024 コンシューマプライバシー調査で、データ保護に関して信用できないプロバイダーからは購入しないという回答が 75% に上っていることを踏まえると、納得がいきます。図 11 を参照してください。

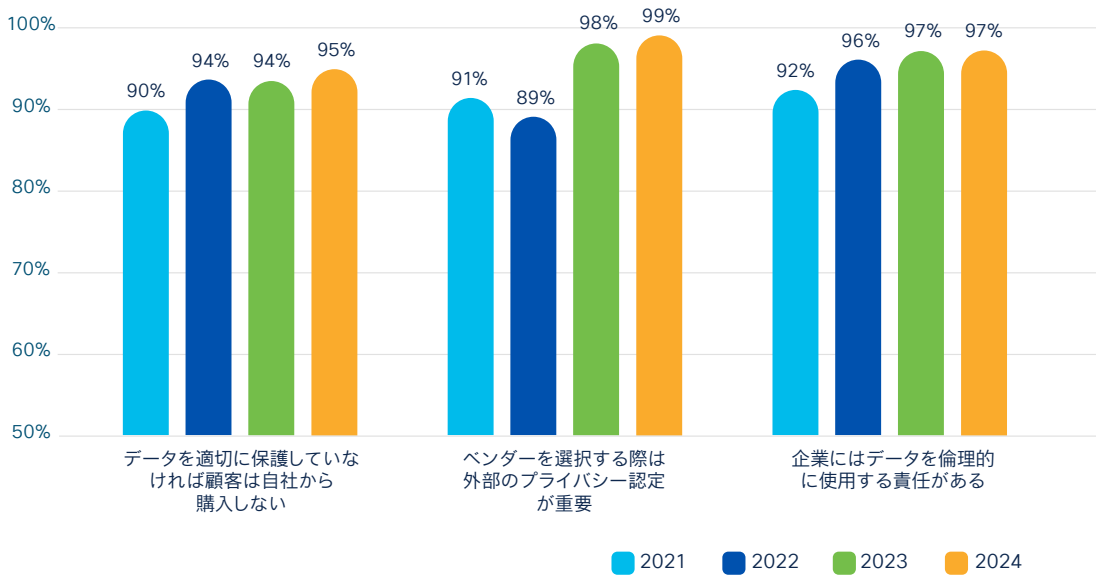
図 11 プライバシーへの投資から大きなメリットを得ている割合 (2024 年)



出典 : シスコ 2025 データ プライバシー ベンチマーク調査

多くの組織が、顧客の信頼を構築するにはプライバシーポリシーと透明性が不可欠であることを広く認識しています。ほとんどの回答者が、堅牢なデータ保護対策が講じられていない場合、顧客が商品やサービスを購入しない傾向が強まっていると考えています。さらに、ほぼすべての組織が、顧客データを責任を持って扱う義務があると認識しています。ベンダーを選定する際は、外部のプライバシー認定が重要な考慮事項であることに変わりはありません。今年の調査でも、回答者の 99% がその重要性を強調しており、この認識が安定していることが示されています。組織は、信頼を高める要因としてプライバシーを優先するだけでなく、自社と取引先が実施している堅牢なデータ保護対策を証明するために、独立した第三者機関による検証を受けています。図 12 を参照してください。

図 12. 顧客の信頼に対するプライバシーの重要性

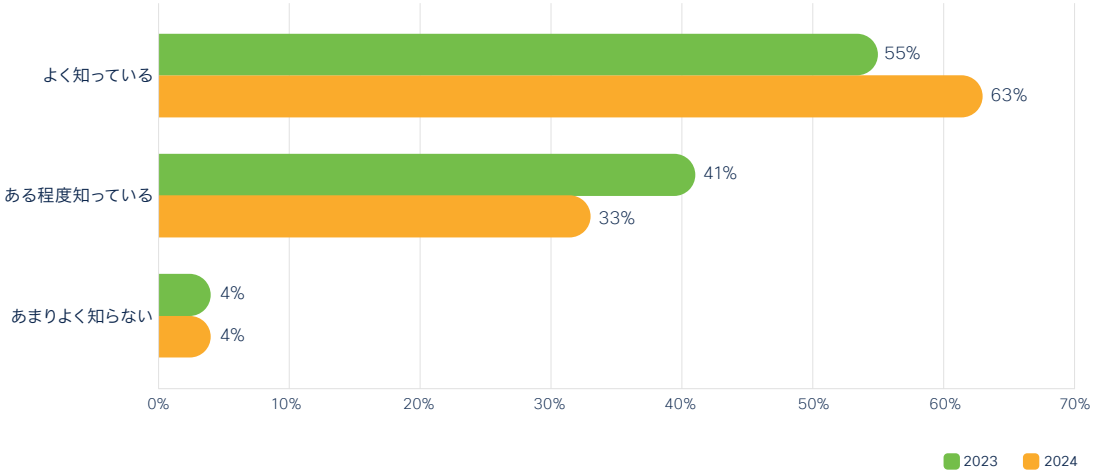


出典 : シスコ 2025 データ プライバシー ベンチマーク調査

4. 生成 AI の利用が増加する一方で残る不確実性

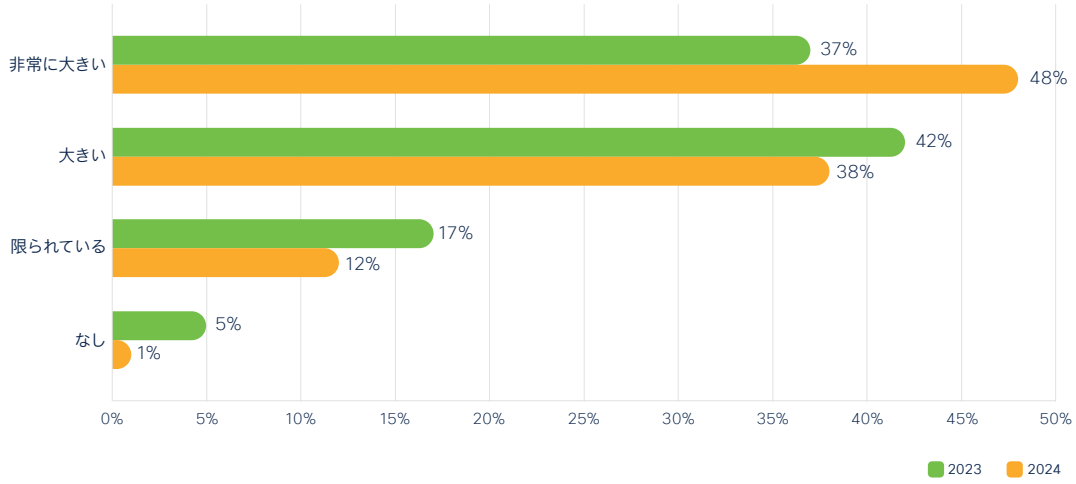
生成 AI の利用が増加するにつれて、プライバシーリスクの管理が最優先事項となっています。2022 年後半に生成 AI が登場して以来、組織も個人も生成 AI の導入を急速に進めています。人々は生成 AI に慣れ、使いこなすようになってきています。2024 年の調査対象者のうち、63% が生成 AI をよく知っていると回答し、2023 年の 55% から増加しました。ある程度知っていると回答した割合は、2023 年の 41% から 2024 年には 33% に減少しています。このテクノロジーについてよく知らないと回答したのは 4% のみでした。認知度が向上するにつれて、価値も高まりました。回答者の 48% が、生成 AI から非常に大きな価値を得ていると回答しており、これは 2023 年の 37% から増加しています。図 13 と図 14 を参照してください。

図 13. 生成 AI についての知識



出典：シスコ 2025 データ プライバシー ベンチマーク調査

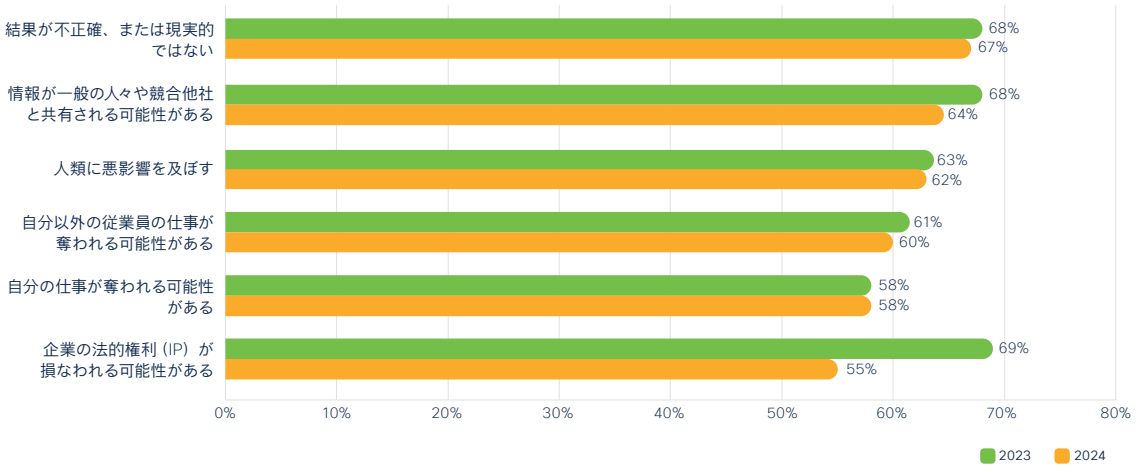
図 14. 生成 AI から得ている価値



出典：シスコ 2025 データ プライバシー ベンチマーク調査

生成 AI を使用する組織が世界中で増えている一方で、初期段階のテクノロジーに対する懸念は前年比であまり変化していません。例外が 1 つあり、生成 AI が著作権や知的財産の形で企業の法的権利を侵害する可能性があるという懸念については、2023 年の 69% から 2024 年には 55% に減少しました。この減少は、責任ある AI に対する認識が高まっていることと、生成 AI ツールへの機密データの入力についてのガバナンスや管理が改善されていることを示しています。同様に、組織が生成 AI の活用スキルを向上させるにつれて、機密情報が漏洩するリスクについての懸念も、回答者の 68% から 64% に若干減少しました。興味深いことに、懸念は低下したものの、回答者のほぼ半数が、依然として生成 AI ツールに従業員の個人情報や非公開情報を入力していると答えています。図 15 と図 16 を参照してください。

図 15. 生成 AI に関するユーザーの懸念

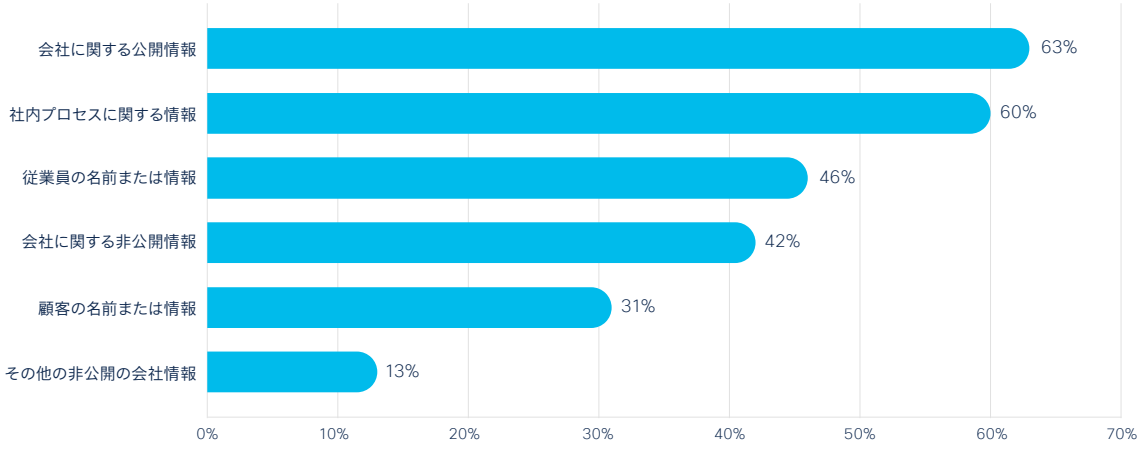


出典 : シスコ 2025 データ プライバシー ベンチマーク調査

「AI の活用に取り組む組織にとって、プライバシーへの投資は重要な基盤を確立するものであり、効果的な AI ガバナンスを促進する助けとなります」

Dev Stahlkopf
シスコ エグゼクティブ バイスプレジデント兼最高法務責任者

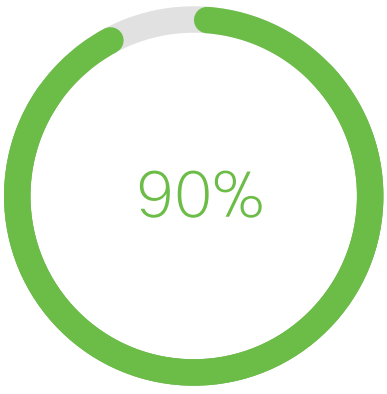
図 16. 生成 AI アプリケーションに入力された情報の種類



出典 : シスコ 2025 データ プライバシー ベンチマーク調査

先の調査結果を踏まえると、圧倒的多数の回答者（90%）が、強力なプライバシー保護法により、顧客が生成 AI ツールでデータを共有する際の安心感が高まると答えています。プライバシー保護法は、透明性、公平性、説明責任を義務付けており、自分のデータがどのように使用されているかをユーザーが理解できるようにし、適切かつ責任を持ってデータが使用されるよう徹底しています。この透明性により、個人データを保護するための法的保護対策が講じられていると理解したうえで、さらに安心して生成 AI テクノロジーを利用できるようになります。図 17 を参照してください。

図 17. 強力なプライバシー保護法により、顧客が AI アプリケーションでデータを共有する際の安心感が高まる



出典 : シスコ 2025 データ プライバシー ベンチマーク調査

5. 組織は AI により多くのリソースを割り当てる見込み

シスコ 2024 年 AI 成熟度指標によると、世界中で AI への投資が急務になっています。調査対象者の 98% が、前年よりも AI 投資の緊急性が高まっていると感じていました。その一方で、このテクノロジーのポテンシャルを最大限に活用する準備ができていると答えたのは、わずか 13% です。[3] また、同指標によると、今後数年間で IT 予算の割り当て額がほぼ 2 倍になると見込まれています。

こうした背景を踏まえると、今年のデータ プライバシー ベンチマーク調査で、回答者のほぼ全員 (99%) が、来年はプライバシー予算が AI 予算として再配分されると答えたのも当然のことでしょう。図 18 を参照してください。

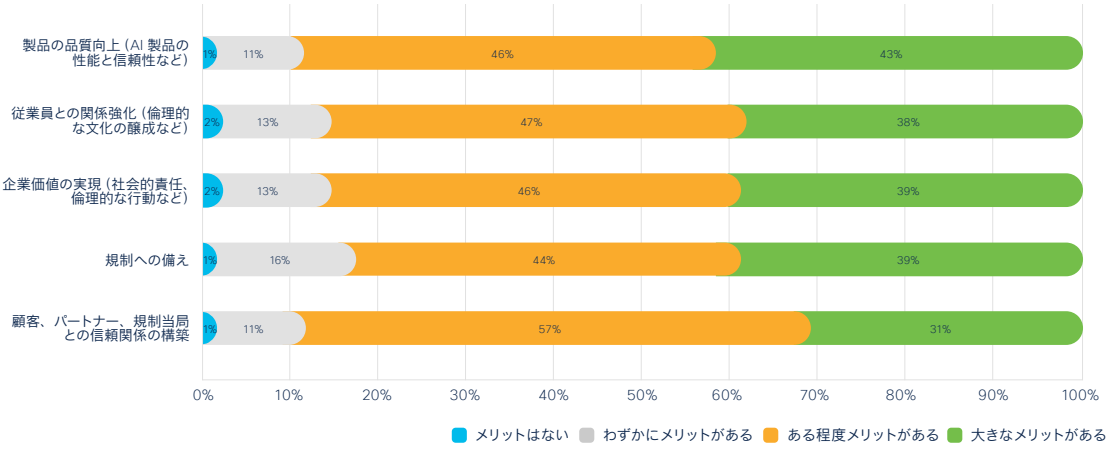
図 18. プライバシー関連のリソースと支出は、来年は AI にシフトする可能性が高い

出典 : シスコ 2025 データ プライバシー ベンチマーク調査

[3] シスコ 2024 年 AI 成熟度指標

AI の導入を急いでいる組織は、強力な AI ガバナンスに投資することのメリットを認識しています。具体的には、リスクを管理し、関係者を保護し、信頼を構築し、罰金を回避するための倫理的・法的・運用上のフレームワークの整備などです。調査対象者の 4 分の 3 以上が、製品の品質、従業員との関係の強化、企業価値の実現、規制への備え、関係者からの信頼の面で、堅牢な AI ガバナンスから中程度以上のメリットが得られていると感じていました。組織がこうしたメリットを享受するために AI ガバナンスプログラムの拡大を図る際は、既存のプライバシー投資をプログラムでどのように活用または補完するのかを決め、顧客の信頼に与える影響を考慮しながら、今後の意思決定を慎重に行う必要があります。図 19 を参照してください。

図 19. AI ガバナンスプログラムの利点



出典：シスコ 2025 データ プライバシー ベンチマーク調査

まとめと組織への推奨事項

本調査は、2024 年のデータプライバシーに関するプライバシーおよびセキュリティ専門家のグローバルな視点をまとめたものであり、さまざまな規模や地域の組織にとって、顧客の信頼を獲得、構築、維持するうえでデータプライバシーがいかに重要な役割を果たすかを明らかにしています。生成 AI がますます普及する中、組織は安全で信頼性の高い生成 AI 活用のための基盤として、既存のプライバシーへの取り組みを活用するようになっています。一方で、新たなリスクに対処するには追加の投資が必要になるとの認識も高まっています。このような状況を踏まえ、次の推奨事項を検討することをお勧めします。

1. 複数の地域で事業を展開する際は、データローカリゼーションに関する規制や移転メカニズムという複雑な状況を効果的に乗り切るためのコンプライアンス戦略を策定するようにします。
2. プライバシー規制を受け入れ、プライバシー保護法に対する社会全体の関心の高まりを重視します。コンプライアンスには相応の投資が必要ですが、それによって得られる顧客の信頼は、買い控えリスクの軽減に不可欠であり、そのコストを上回る価値をもたらすはずです。
3. プライバシーへの投資がもたらすビジネス上のメリットを広い視野で捉えるようにします。確かに、社会的信用も重要ですが、俊敏性、イノベーション、市場投入までの時間短縮、業務効率も大きな価値をもたらします。
4. プライバシーを尊重し、意図しない外部影響を管理するために、ガバナンスと制御機能を備えた AI を展開します。AI から得られるビジネス価値には疑いの余地がありませんが、機会とリスクのバランスを取る必要があります。
5. 予算や重点が AI に移行していくことが見込まれる中、AI への投資が、すでに整備されているプライバシーとセキュリティの基盤を支え続けるようにします。これには、継続的なリソースが必要です。

顧客の信頼基準に応える

組織は、資産を保護し、リスクの管理に役立て、顧客の信頼とロイヤリティを構築するために、常にセキュリティを必要としてきました。プライバシーは、今日の複雑なビジネス環境において、顧客の信頼を高めるための重要な要素です。シスコは、お客様が設定した信頼基準に耳を傾け、学び、それらの基準を満たすように進化を続けています。シスコの包括的なアプローチでは、信用性、透明性、説明責任が優先されます。

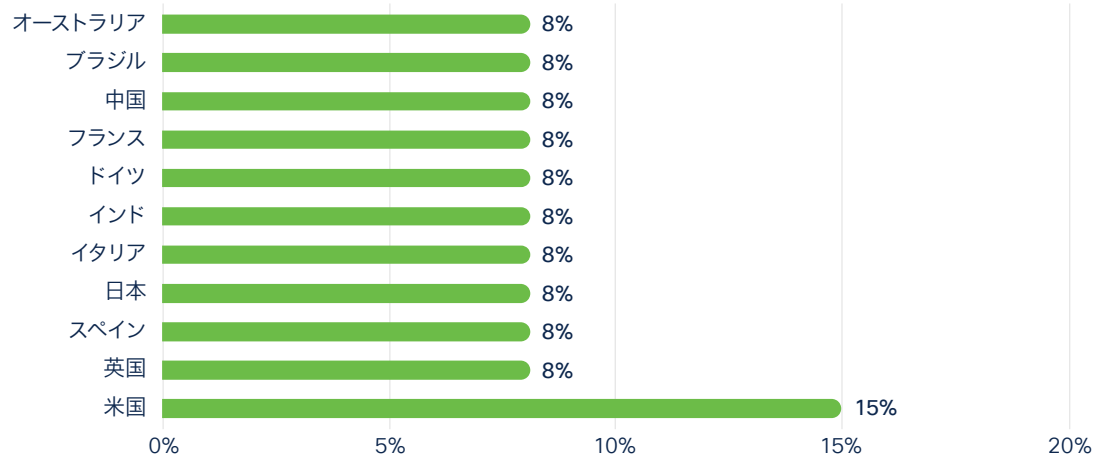
シスコは年次のデータ プライバシー ベンチマーク レポートとコンシューマ プライバシー レポートに加え、主要な製品とサービスについてプライバシーデータシートと プライバシーデータマップを発行しており、関心のある人は誰でも、どのような個人データが使用され、誰がアクセスし、どのくらいの期間保持されているかを把握することができます。シスコの責任ある AI の原則とフレームワークでは、これらの原則と実践がシスコの広範な AI ガバナンスのフレームワークをどのように形成しているかが示されています。また、シスコ パーパスレポートとシスコ パーパスレポートハブでは、シスコが環境、社会、ガバナンス（ESG）の取り組みにおいてどのように信用性、透明性、説明責任を優先しているかに関連する情報を提供しています。

これらすべてのレポートやその他の資料は Cisco Trust Center から入手できます。

シスコのプライバシー調査に関する詳細については、Cisco Privacy Center of Excellence にメール（ask_privacy@cisco.com）でお問い合わせください。

付録

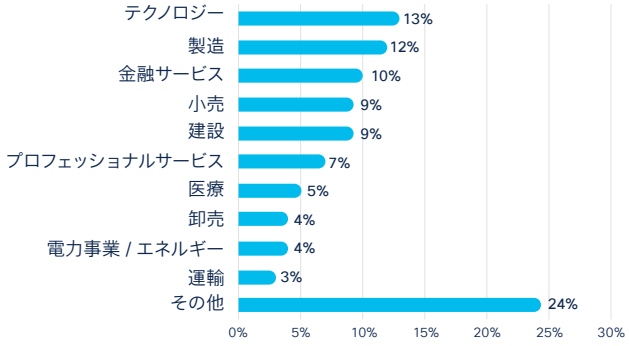
付録 A. 調査回答者の属性（地域別）



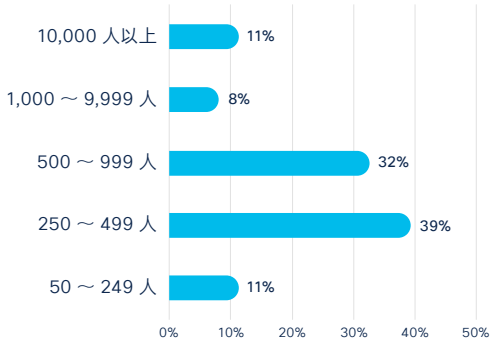
出典：シスコ 2025 データ プライバシー ベンチマーク調査

付録 B. 調査回答者の属性（業界および規模別）

業界別



企業規模別（従業員数）



出典：シスコ 2025 データ プライバシー ベンチマーク調査

サイバーセキュリティ レポート シリーズについて

シスコは過去 10 年間にわたり、全世界のサイバーセキュリティの状態に関心を持つセキュリティプロフェッショナルを対象とした、セキュリティと脅威インテリジェンスに関する多くの情報を公開してきました。これらの包括的なレポートでは、脅威の状況や組織に対する影響を詳しく解説するとともに、データ漏洩がもたらす悪影響から組織を守るためのベストプラクティスを紹介してきました。

シスコのソートリーダーシップに対する新しいアプローチの中で、シスコセキュリティは 一連の調査とそのデータに基づく出版物を発行しています。シリーズの分野は徐々に増え、業界や担当が異なるセキュリティの専門家に向けた幅広いレポートが登場してきました。シスコは、セキュリティ業界の脅威研究者やイノベータの幅広い高度な専門知識を集約したレポートを毎年発行しています。その中には、コンシューマプライバシー調査、データ プライバシー ベンチマーク調査、脅威インサイト、『優先順位付けから予測へ』などがあり、他にも、年間を通して発行しているレポートがあります。


CISCO