Deloitte.
デロイト トーマツ

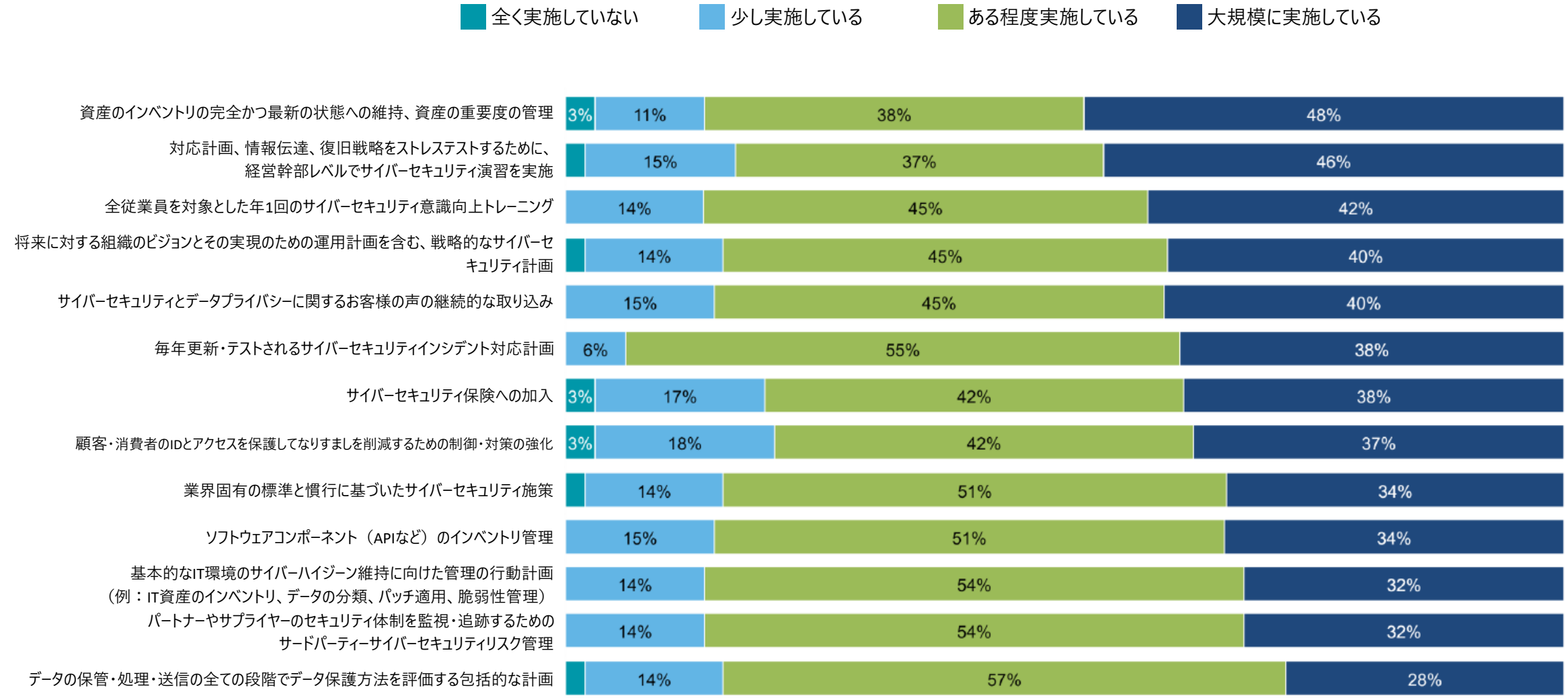
Future of Cyber Survey 第4版

データダッシュボード：日本
回答者数：65

デロイト トーマツ サイバー合同会社

サイバーセキュリティ向上のための対策実施状況

n =65

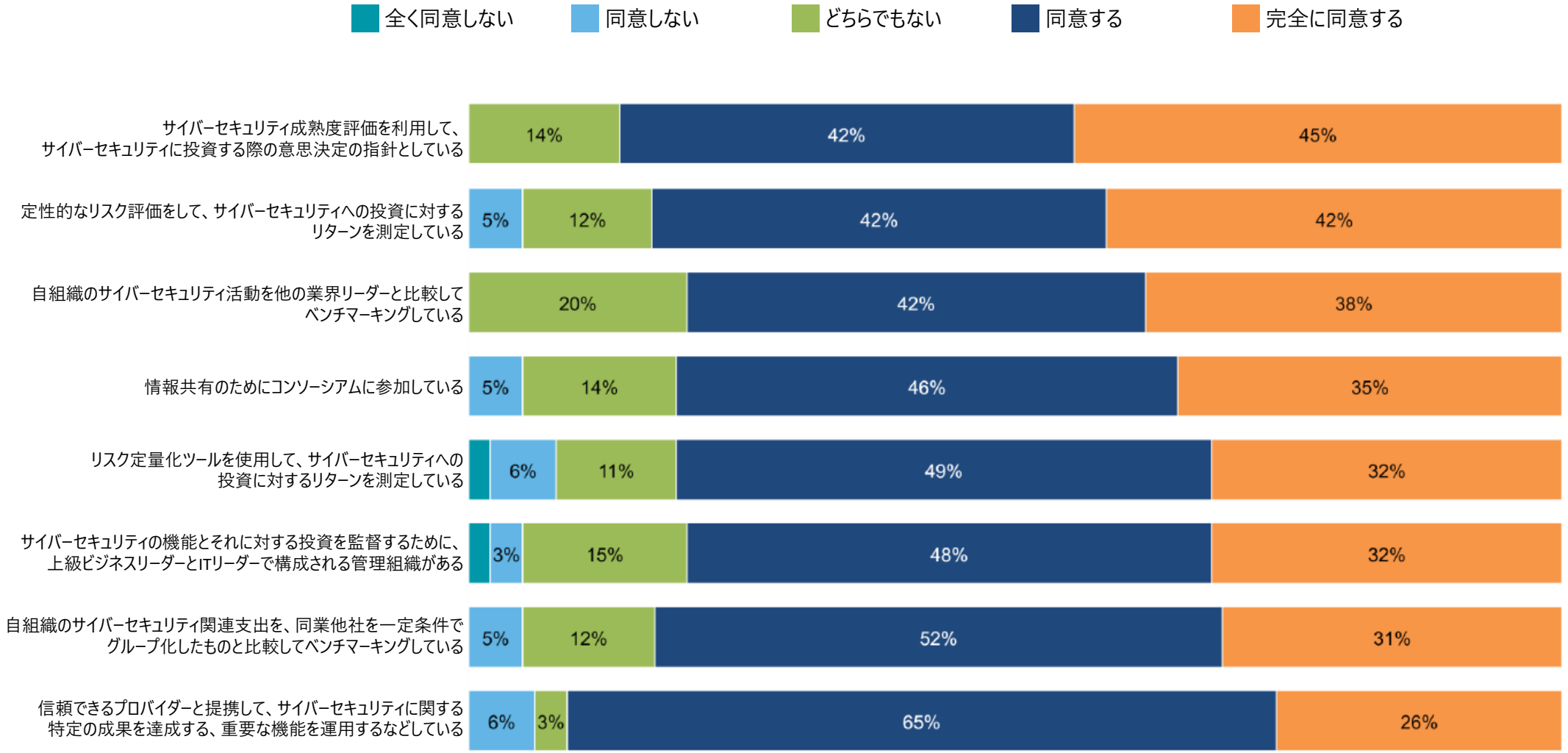


適用した国（国群）フィルター：日本

質問1：サイバーセキュリティ向上のために、次の各対策をどの程度実施していますか。

サイバーセキュリティ戦略

n =65

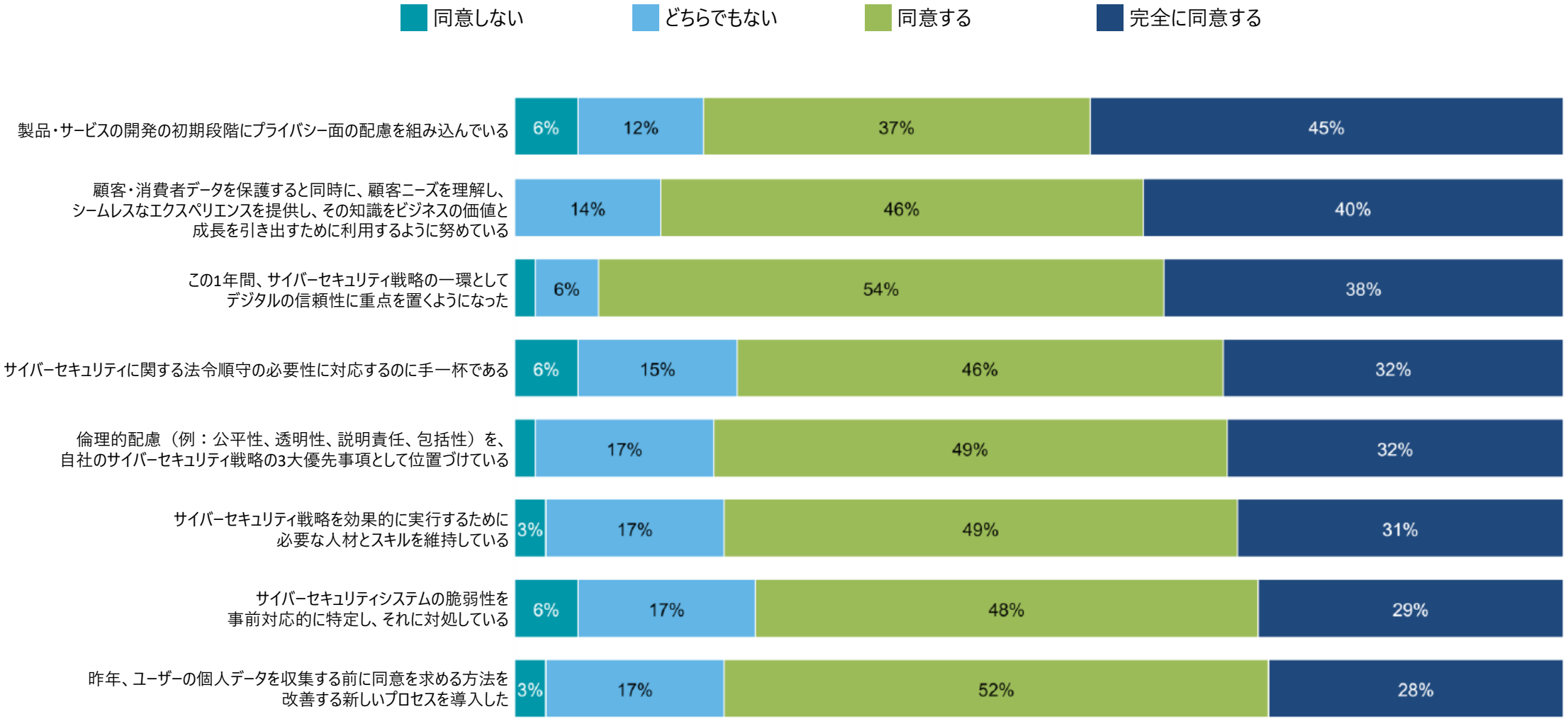


適用した国（国群）フィルター：日本

質問2：次の各対策が自組織のサイバーセキュリティ戦略に盛り込まれているかどうかについて、それぞれの同意度はどのくらいですか。

プライバシー、デジタルの信頼性、倫理に関する合意度

n =65

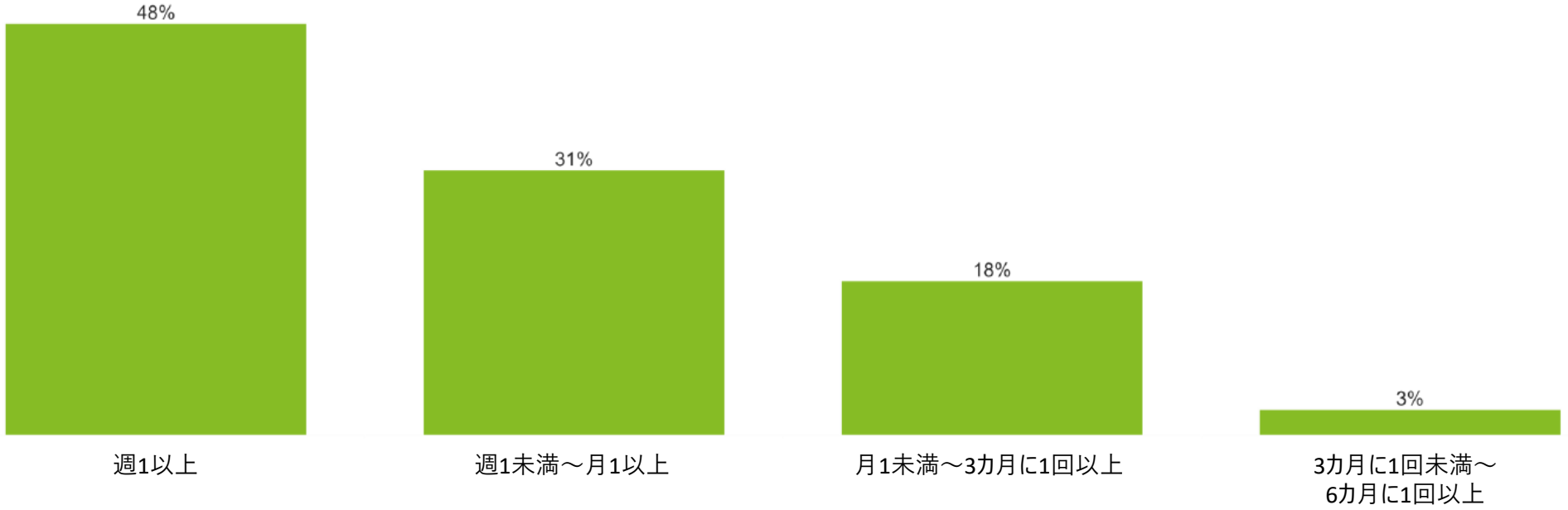


適用した国（国群）フィルター：日本

質問3：プライバシー、デジタル信頼、倫理に関する次の点について、自組織の状況としてどの程度同意しますか。

取締役会がサイバーセキュリティの課題に対処している頻度

n =65

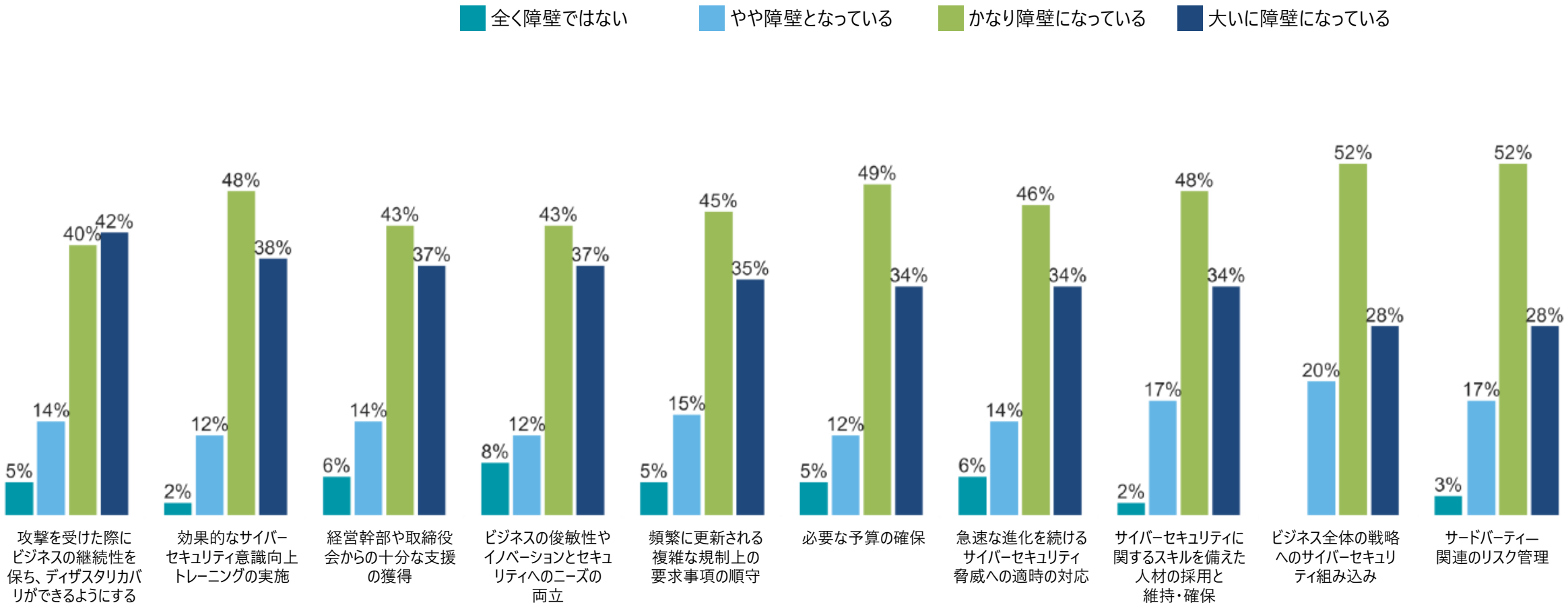


適用した国（国群）フィルター：日本

質問4：取締役会がサイバーセキュリティ関連の課題（リスク評価、成熟度評価、サイバーセキュリティ戦略）に対処している頻度はどのくらいですか。

サイバーセキュリティ戦略の障壁となっている課題とその程度

n =65

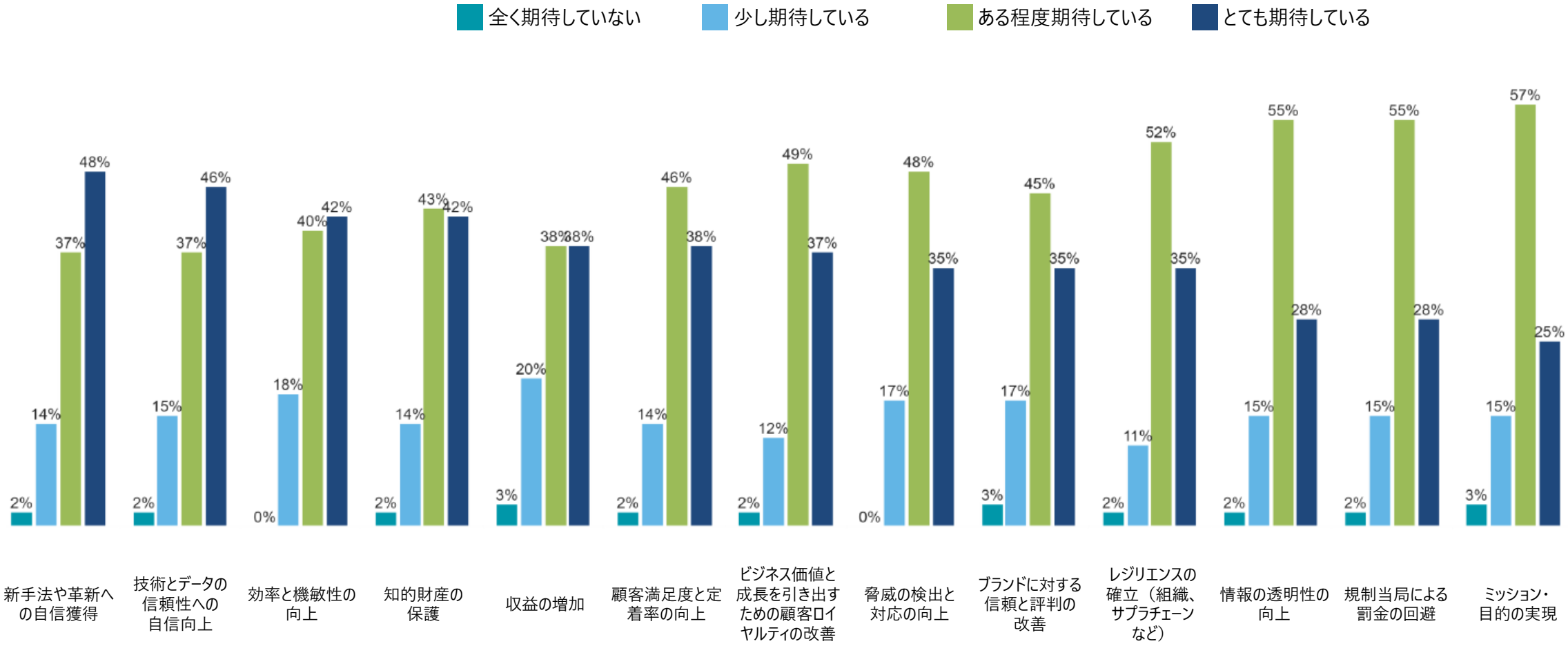


適用した国（国群）フィルター：日本

質問5：次の課題は、自組織のサイバーセキュリティ戦略にとってどの程度の障壁となっていますか。

サイバーセキュリティ施策を実施することで期待されるビジネス上の成果とそれぞれへの期待度

n =65

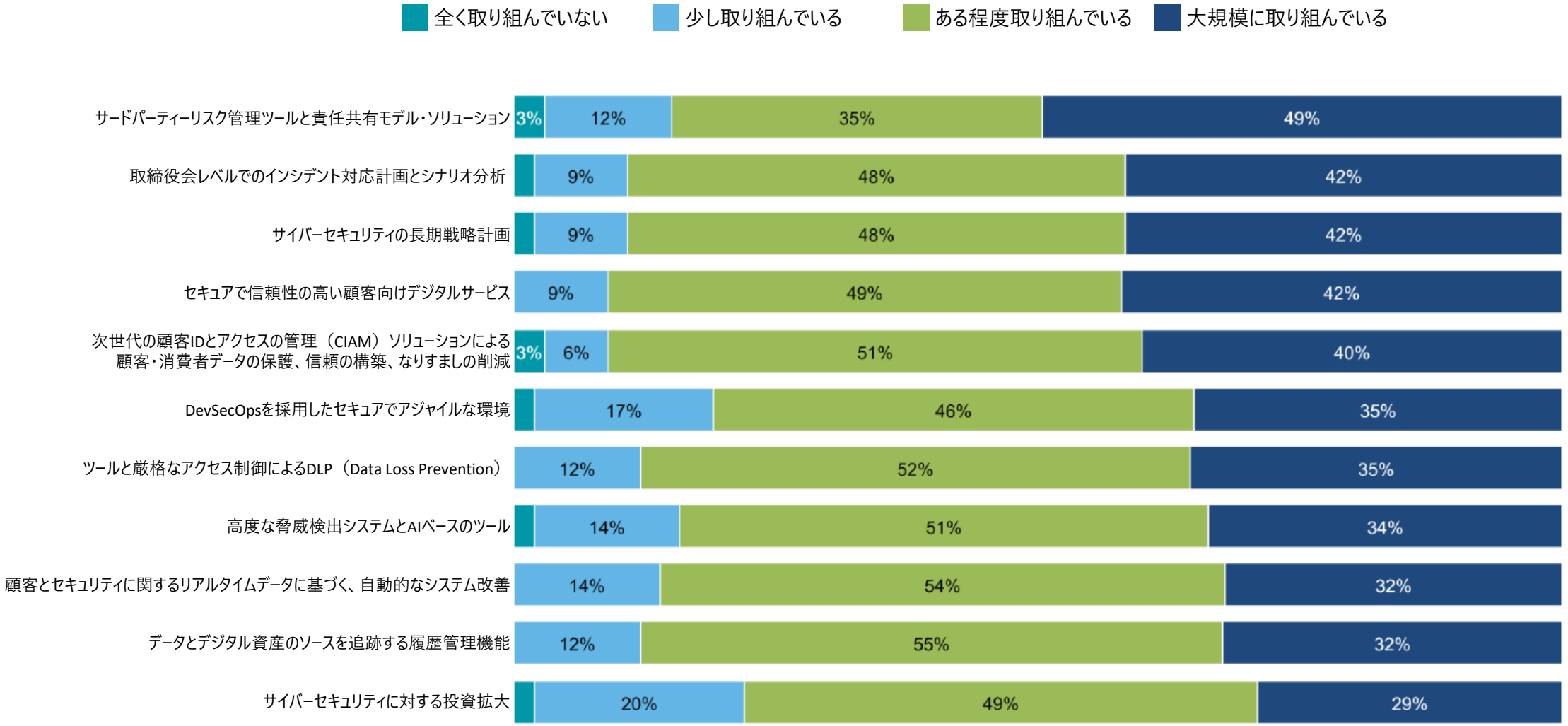


適用した国（国群）フィルター：日本

質問6：サイバーセキュリティ施策の実施が次のビジネス上の成果達成につながることをどの程度期待していますか。

サイバーセキュリティ機能やコンピテンシーの開発への取り組み状況

n =65

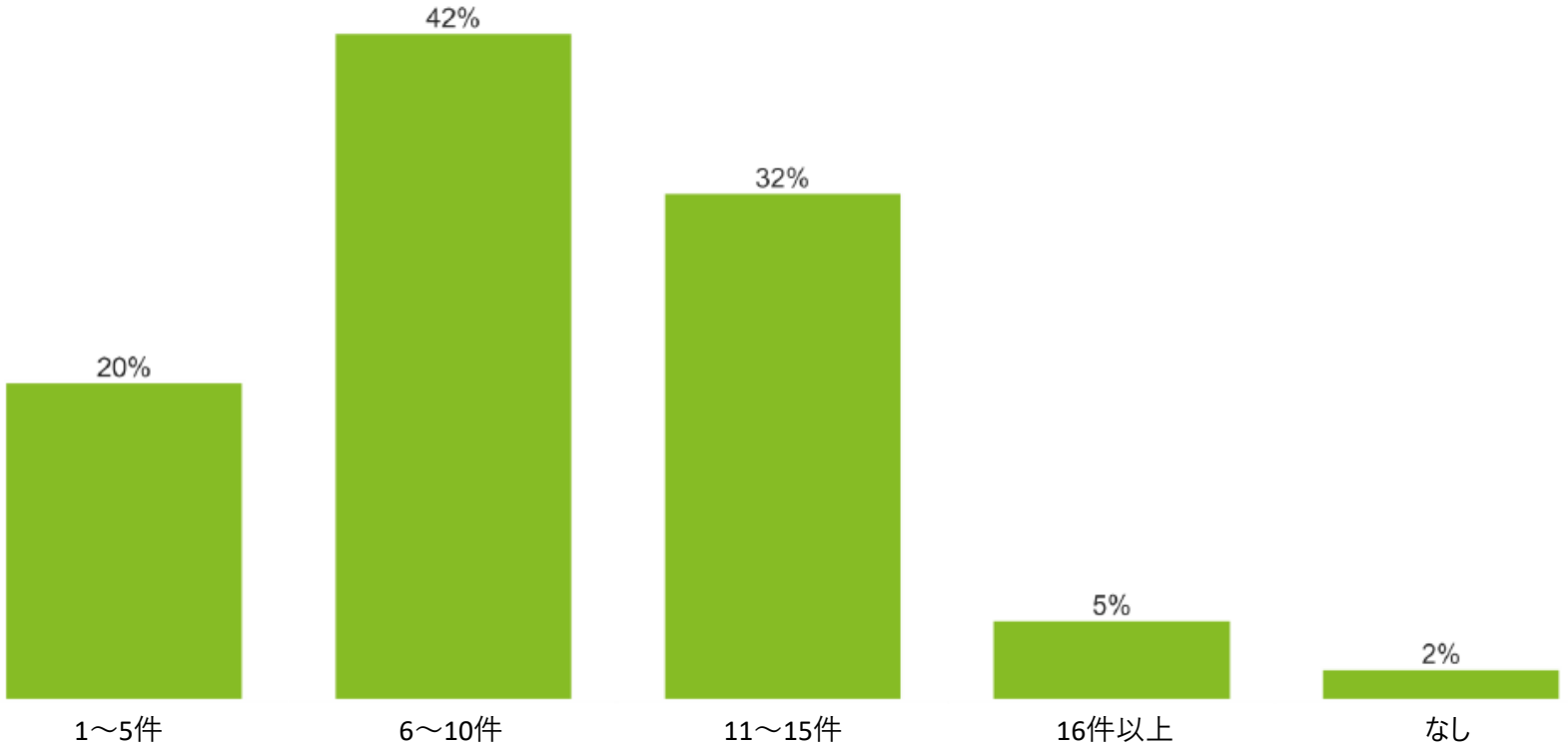


適用した国（国群）フィルター：日本

質問7：ビジネス上の成果を達成するために、次のサイバーセキュリティ機能やコンピテンシーの開発にどの程度取り組んでいますか。

過去1年間に公表したサイバーセキュリティ侵害件数

n =65

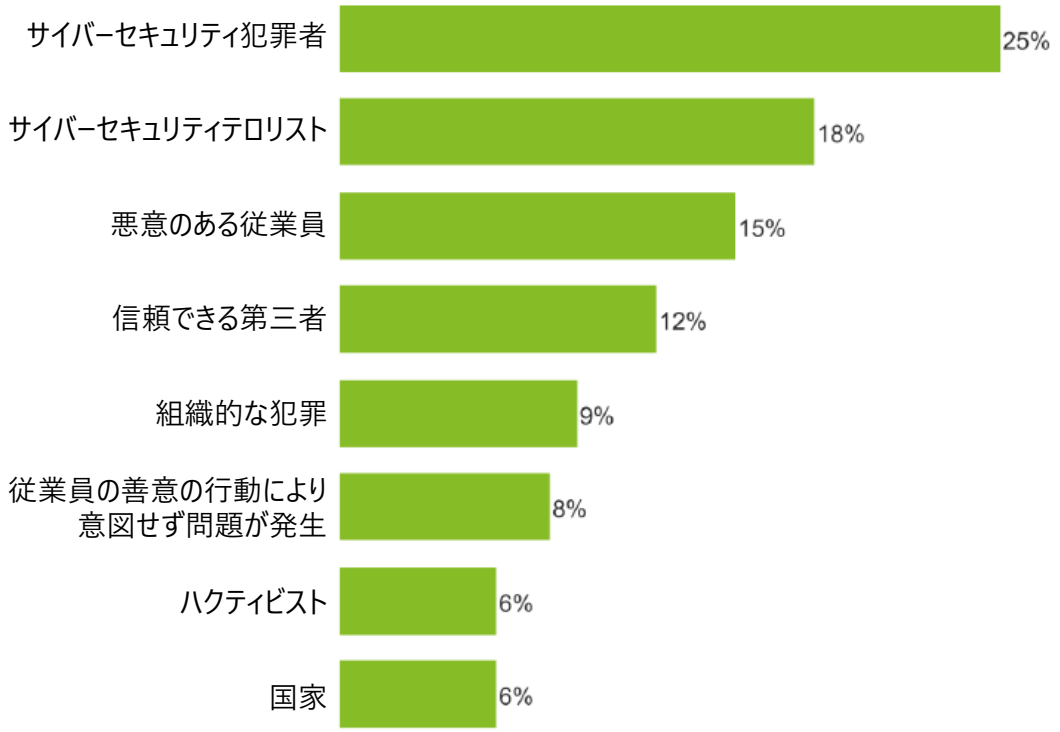


適用した国（国群）フィルター：日本

質問8：過去1年間に公表したサイバーセキュリティ侵害は何件ですか。

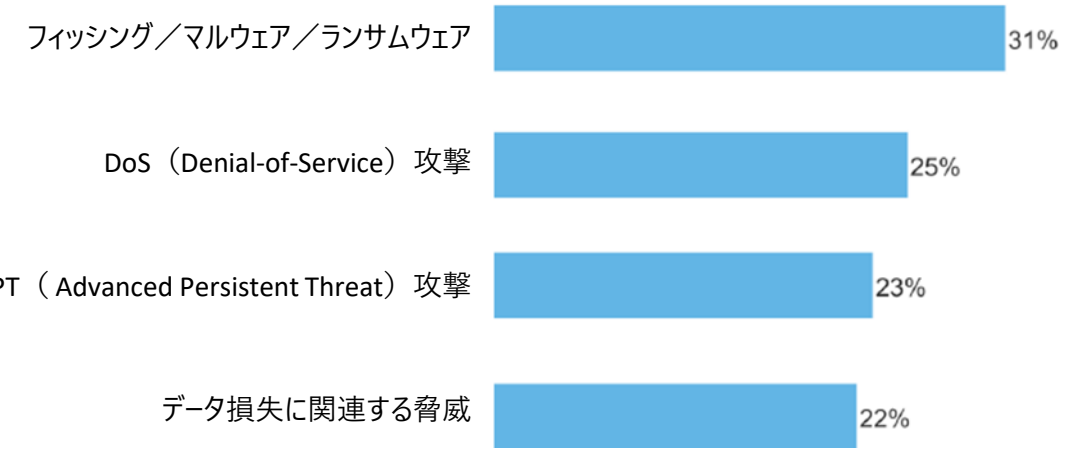
サイバーセキュリティに関する懸念

脅威アクター・ソース



適用した国（国群）フィルター：日本

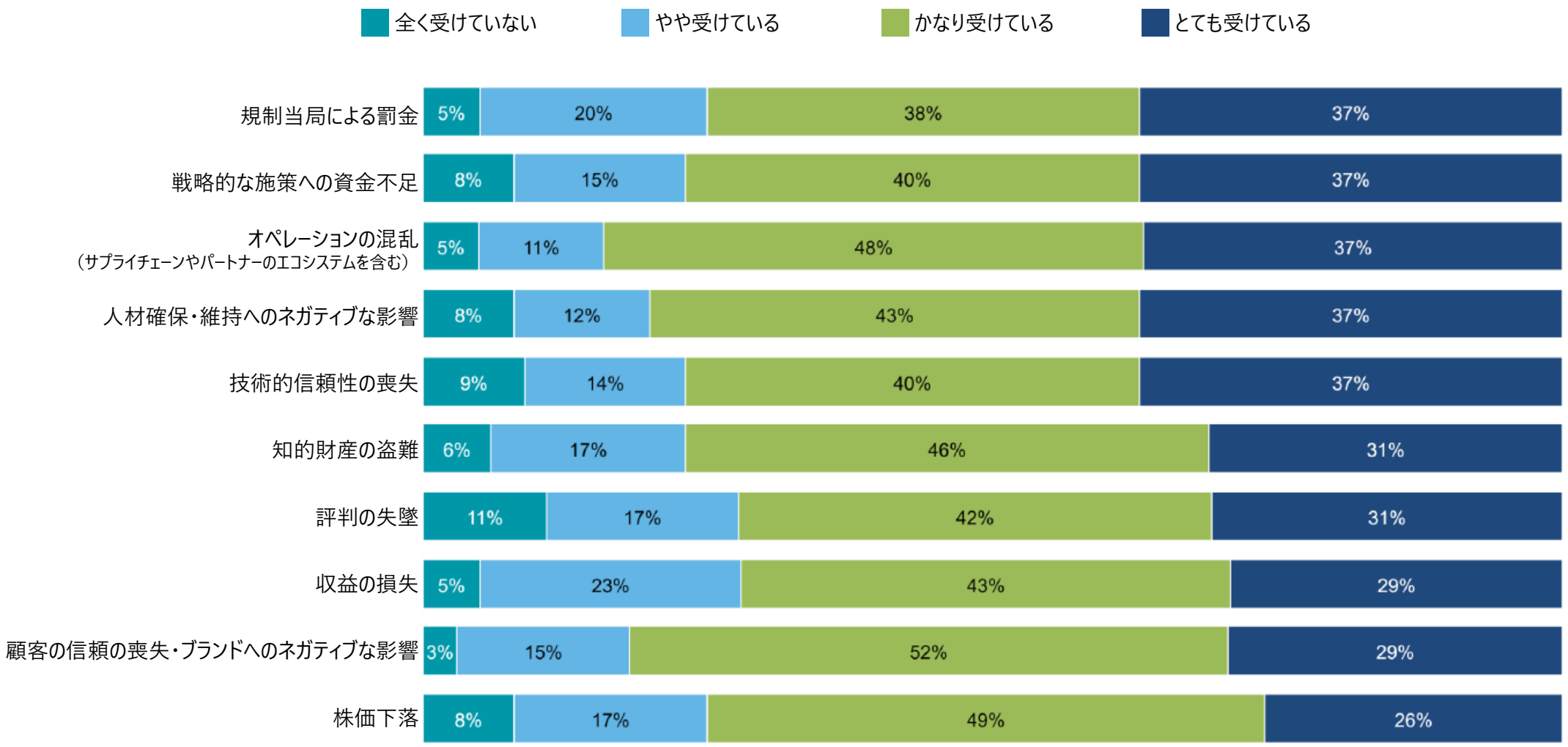
ツール・手法



適用した国（国群）フィルター：日本

質問9：最も懸念しているサイバーセキュリティの脅威の発生源は何ですか（1つ選択）。

サイバーセキュリティのインシデントや侵害による悪影響



適用した国（国群）フィルター：日本

質問10：サイバーセキュリティのインシデントまたは侵害によって、次の悪影響をそれぞれどの程度受けていますか。

ITとサイバーセキュリティの予算

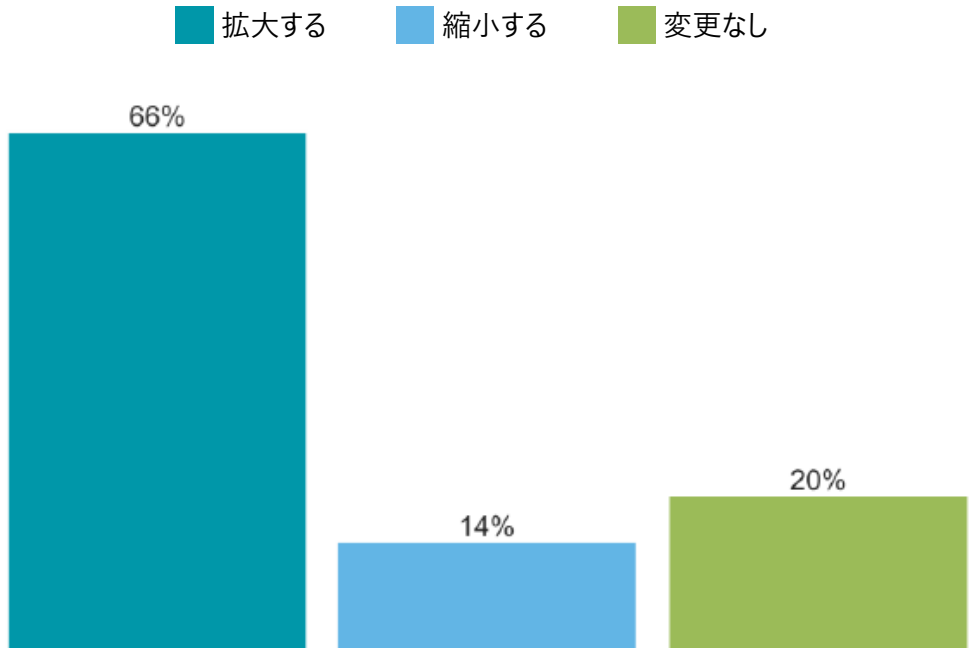
	最低額平均	最高額平均
年間IT予算（米ドル）	128M	306M

	平均割合
IT予算のうちサイバーセキュリティ関連活動への割り当て	20%

質問11A：今年度のITの年間予算はどのくらいですか。（単位：百万米ドル）。
質問11B：そのうち、今年度のサイバーセキュリティ関連活動（例：テクノロジーへの投資、運用、コンプライアンスなど）に割り当てられているのはおよそ何%でしょうか。

サイバーセキュリティに対する投資

投資額の変動見込み



サイバーセキュリティの割り当ての純増加割合**

1%

**サイバーセキュリティ予算に関して見込まれる変動の全体規模を、全ての回答に基づいて算出

適用した国（国群）フィルター：日本

質問12：予算のうちサイバーセキュリティに割り当てられる割合は、今後12～24カ月でどのように変化すると思いますか。

サイバーセキュリティ予算に含まれる領域

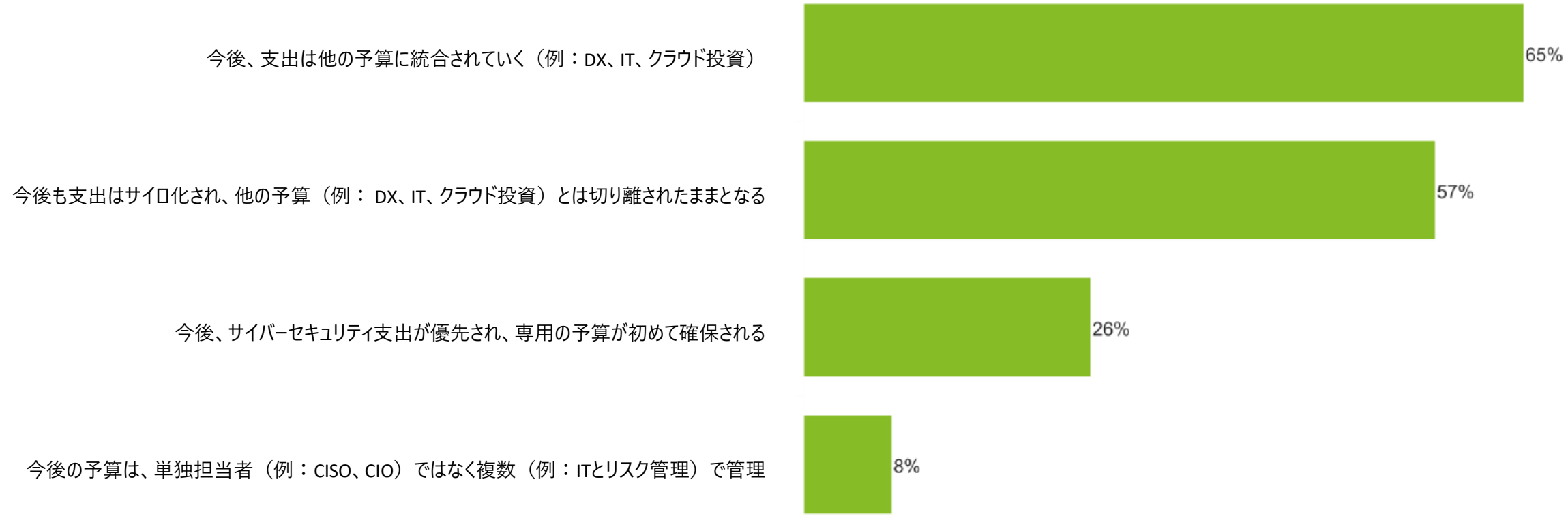
n =65

	サイバーセキュリティ予算に含めているという組織の割合	サイバーセキュリティ予算内での割り当て
戦略とガバナンス（例：変革プログラム、リスク評価）	28%	10%
人材とトレーニング（例：人材モデル、採用、トレーニング、育成プログラム、人材採用と確保・維持）	31%	10%
脅威の検出と対応（例：SOC、脅威ハンティングと検出、プロアクティブな分析機能、脅威インテリジェンス）	20%	9%
データ保護とプライバシー（例：データの分類、データ漏洩防止、データベースアクティビティの監視）	26%	11%
IDとアクセスの管理業務（例：管理のためのコールセンターやファイアウォール）	18%	6%
アプリケーション（例：アプリケーションセキュリティ、内部統制、セキュアなソフトウェア導入）	25%	8%
新興テクノロジー（例：オペレーション変革、5G、AI、量子コンピューティング、ブロックチェーン）	25%	8%
インフラストラクチャ（例：モバイル端末とエンドポイントのセキュリティ、技術面のレジリエンス、IT資産管理、ゼロトラスト、攻撃サーフェス）	20%	6%
ネットワークセキュリティ（例： line 1ネットワークセキュリティ）	22%	7%
クラウド（例：DevSecOps、アプリケーションのモダナイゼーションと移行、クラウドセキュリティのオーケストレーションと自動化）	29%	5%
サードパーティーセキュリティ（例：ベンダーのセキュリティ評価、マネージドサービス）	17%	4%
AIおよびGenAI（生成AI）への投資（例： 予測監視）	22%	3%
AI 倫理（AIモデルの透明性、AIの倫理的な開発）	20%	8%
業界固有の標準とガイドライン	18%	5%

質問13：今年度のサイバーセキュリティ予算に含まれる領域は、次のうちどれですか。

デジタル環境の進化によるサイバーセキュリティ関連支出への影響

n =65

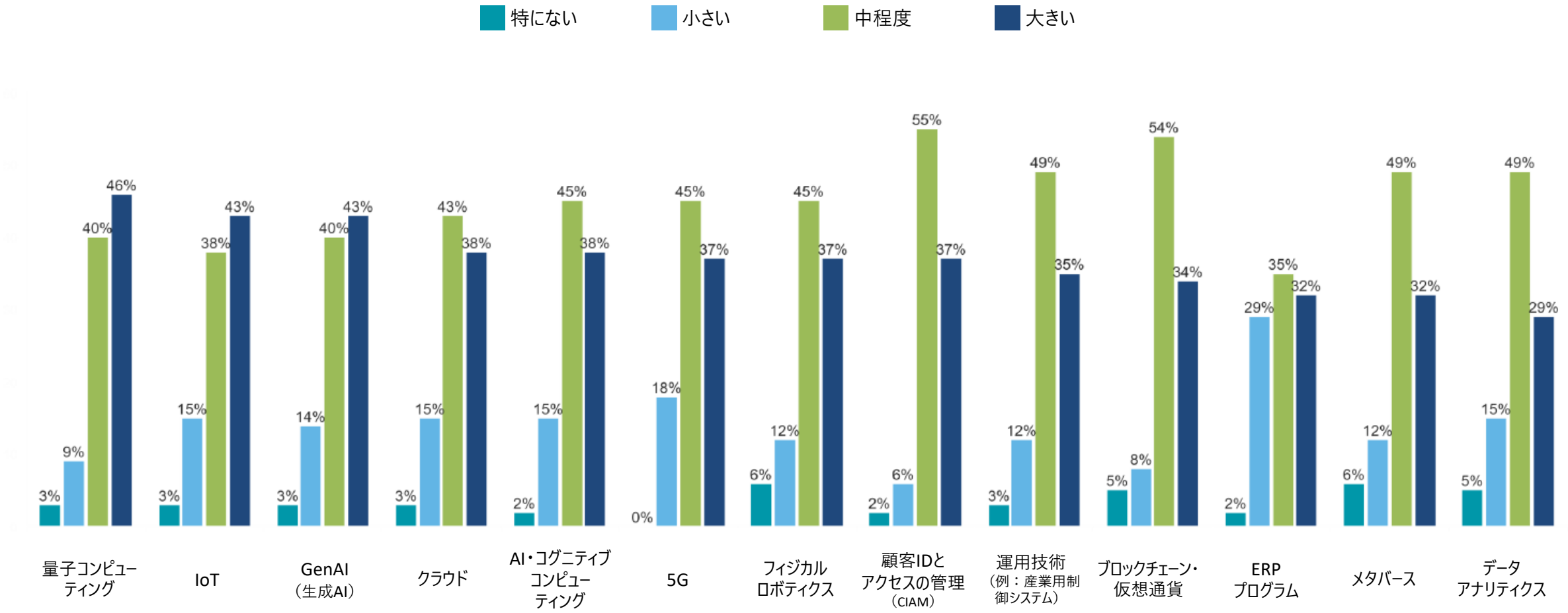


適用した国（国群）フィルター：日本

質問14：デジタル環境が進化することで、自組織のサイバーセキュリティ関連の支出にどのような影響が出ると思いますか。

テクノロジー機能への投資確保におけるサイバーセキュリティの役割

n =65

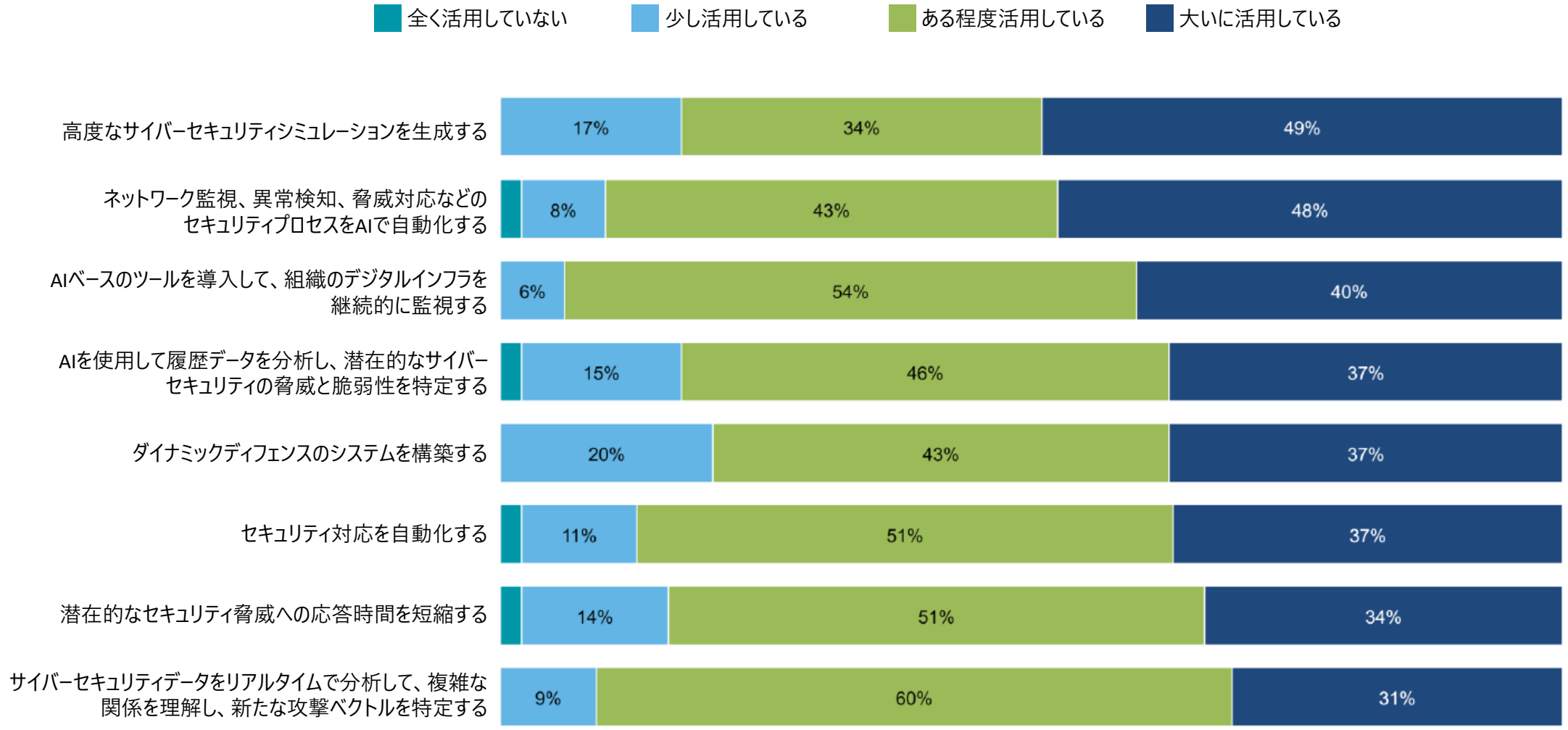


適用した国（国群）フィルター：日本

質問15：次の各テクノロジー機能に対する投資を確保する上でサイバーセキュリティはどの程度の役割を果たしていますか。

サイバーセキュリティプログラムにおけるAI機能の活用状況

n =65

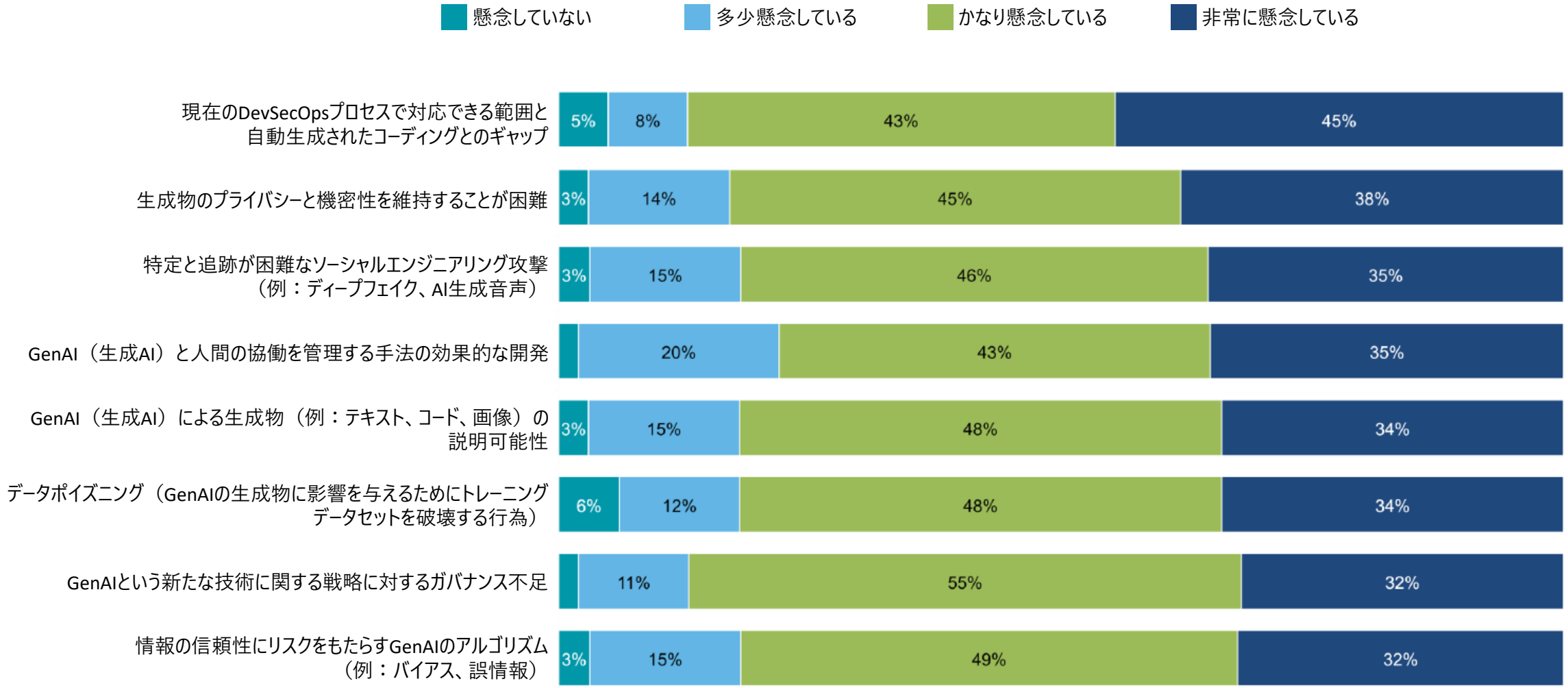


適用した国（国群）フィルター：日本

質問16：サイバーセキュリティプログラムにおいてAI機能をどの程度活用していますか。

サイバーセキュリティ戦略におけるGenAI関連のリスクへの懸念

n =65

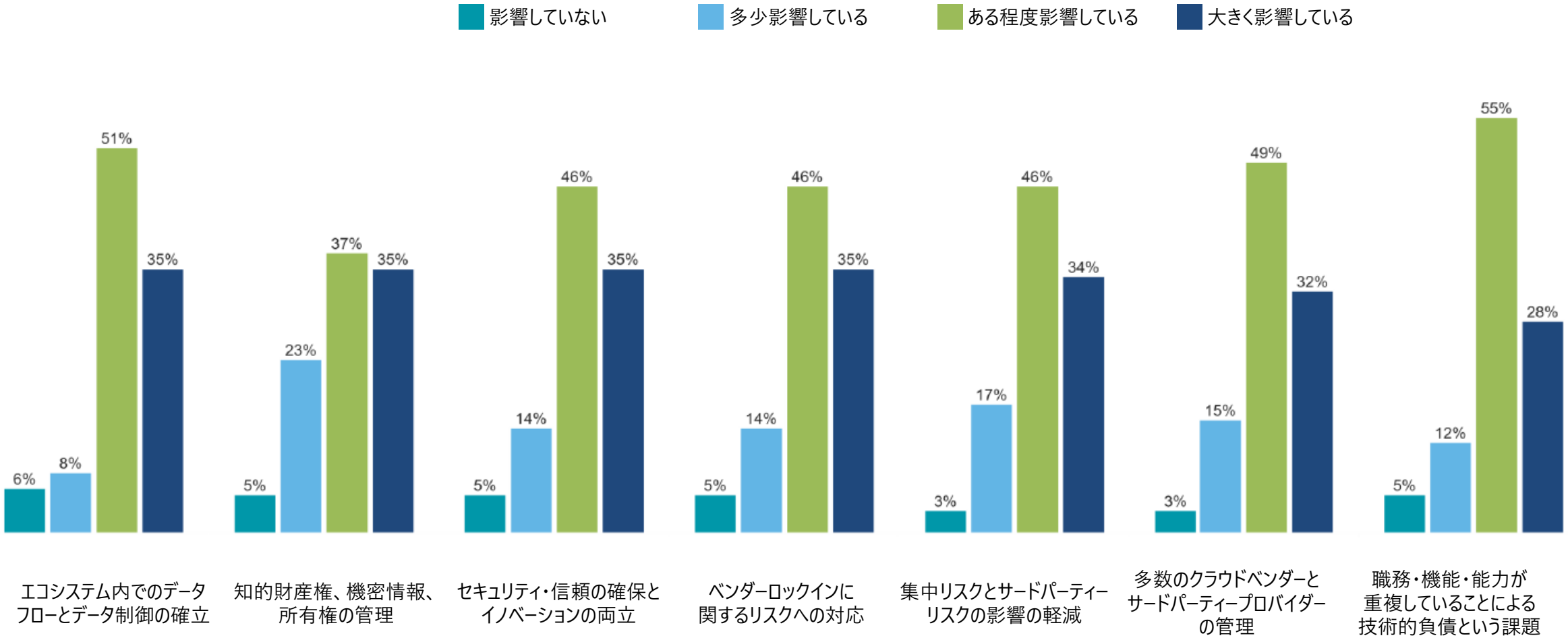


適用した国（国群）フィルター：日本

質問17：特にGenAIに起因する、サイバーセキュリティ戦略における新しいリスクについて、どの程度懸念していますか。

クラウドエコシステムの複雑さに影響を与えている事項

n =65



適用した国（国群）フィルター：日本

質問18：次のそれぞれはクラウドエコシステム全体の複雑さにどの程度影響していると思いますか。

クラウド、コンサルティング、サイバーセキュリティの各エコシステムにおけるパートナーの数

n =65

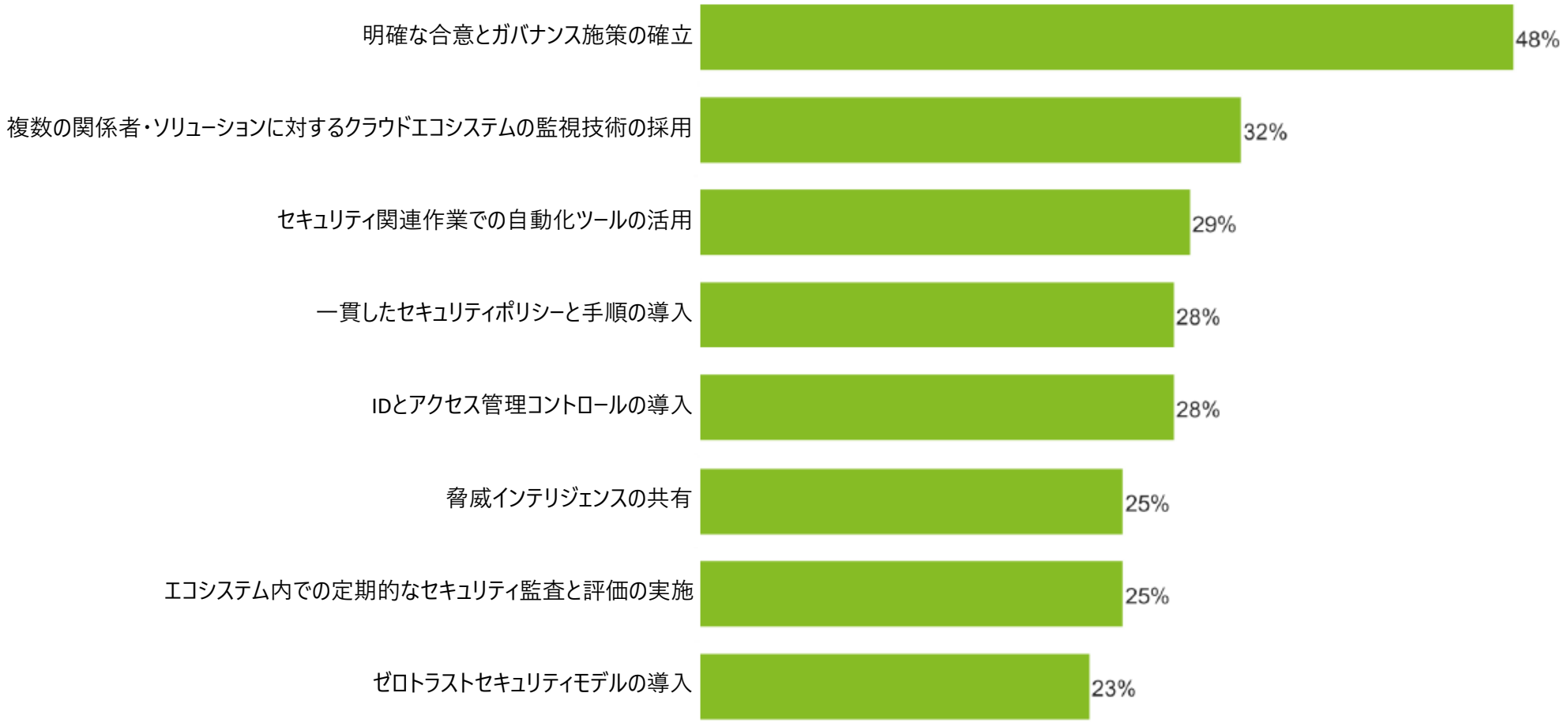
パートナーの数に基づくエコシステムの複雑度

	小規模（1～20社）	中規模（21～40社）	大規模（40社超）
クラウドエコシステム （例：マネージドサービス、システムインテグレーター、テクノロジー）	52％	32％	15％
コンサルティング （例：戦略、リスク、セキュリティ）	43％	32％	25％
サイバーセキュリティ （例：アセスメント、モニタリング、フォレンジック）	43％	38％	18％

質問19：次の各エコシステムで何社のパートナーと提携していますか。

クラウドエコシステムの複雑さを軽減するためのサイバーセキュリティ対策

n =65

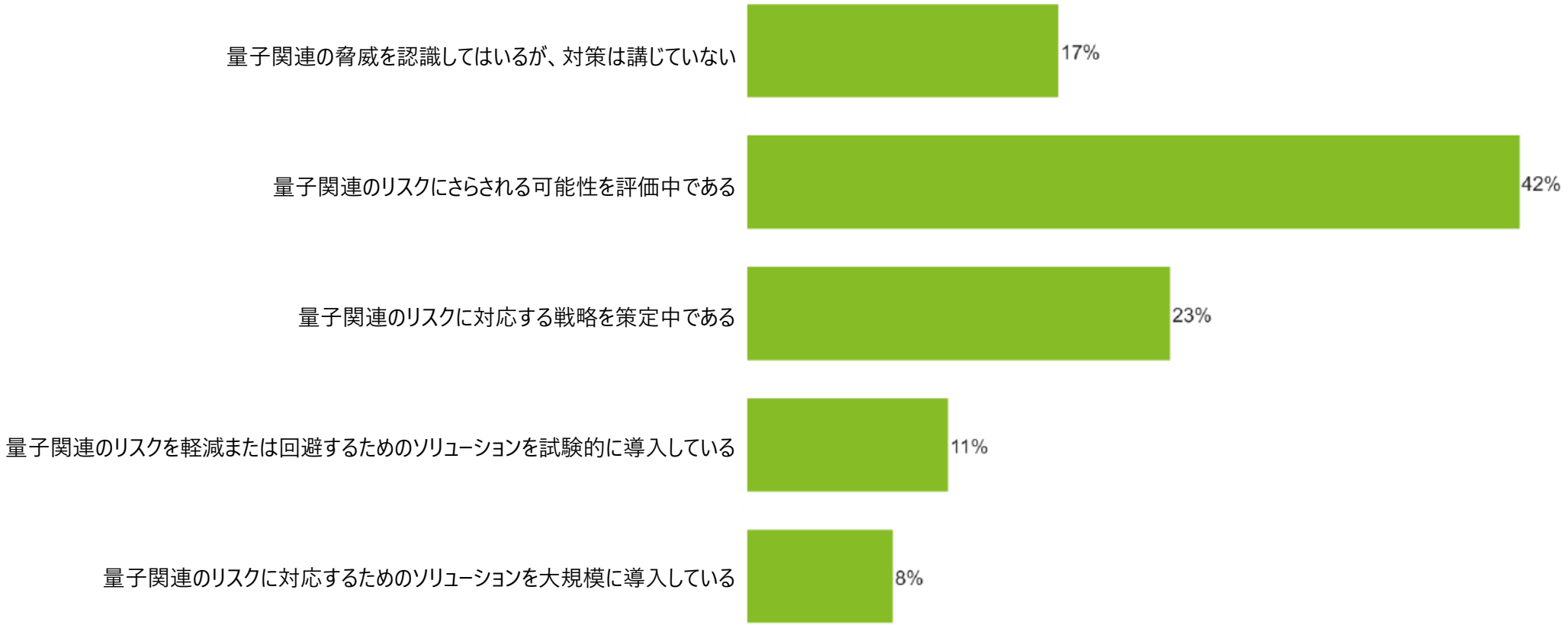


適用した国（国群）フィルター：日本

質問20：クラウドエコシステムの複雑さを軽減するために、どのようなサイバーセキュリティ対策を講じていますか。

量子関連のサイバーセキュリティへの主な対応策実施状況

n =65

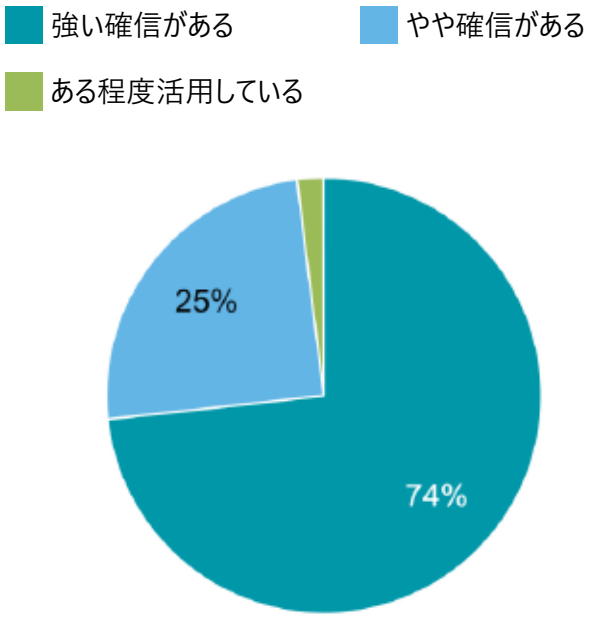


適用した国（国群）フィルター：日本

質問21：量子サイバーセキュリティへの主な対応策の実施状況として、最も近いものは次のどれですか。

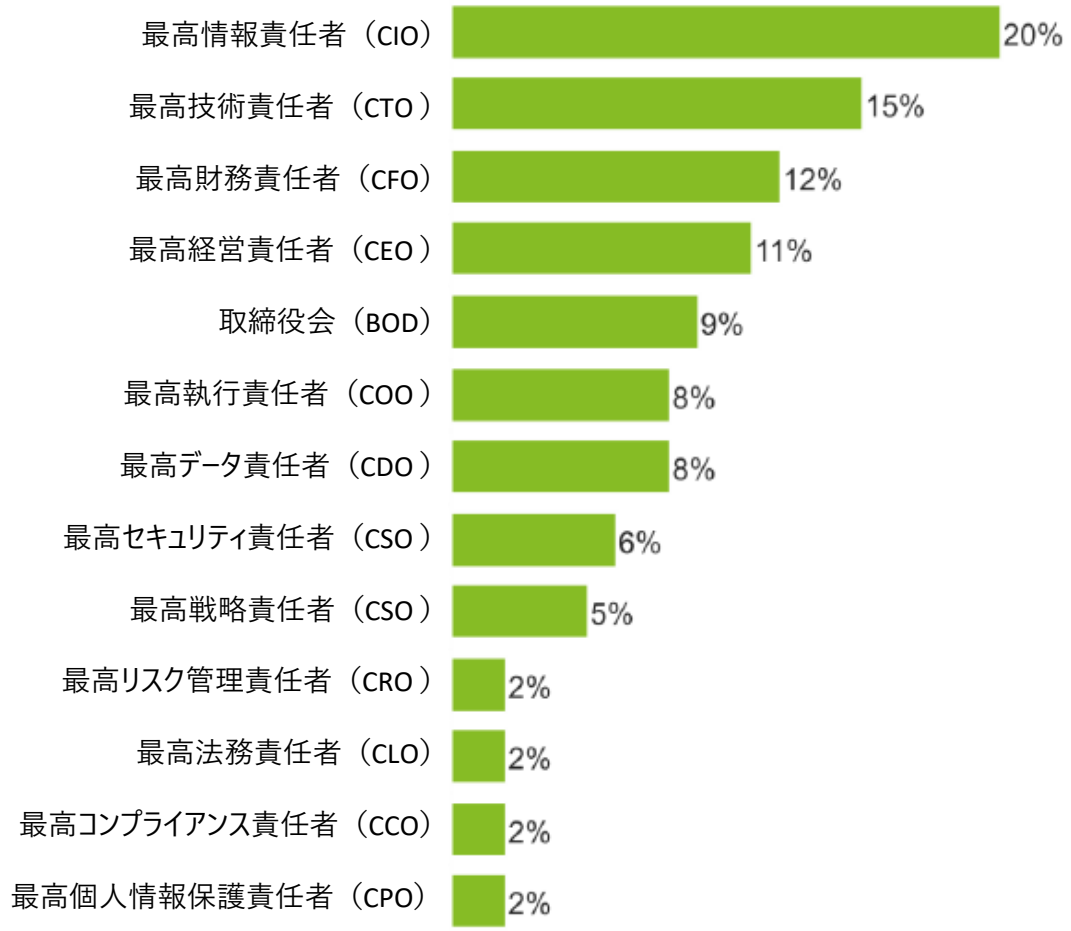
経営幹部のサイバー成熟度

経営幹部と取締役会がサイバーセキュリティに適切に対応できると確信を持てるか



適用した国（国群）フィルター：日本

CISO・サイバーセキュリティリーダーの直属先



適用した国（国群）フィルター：日本

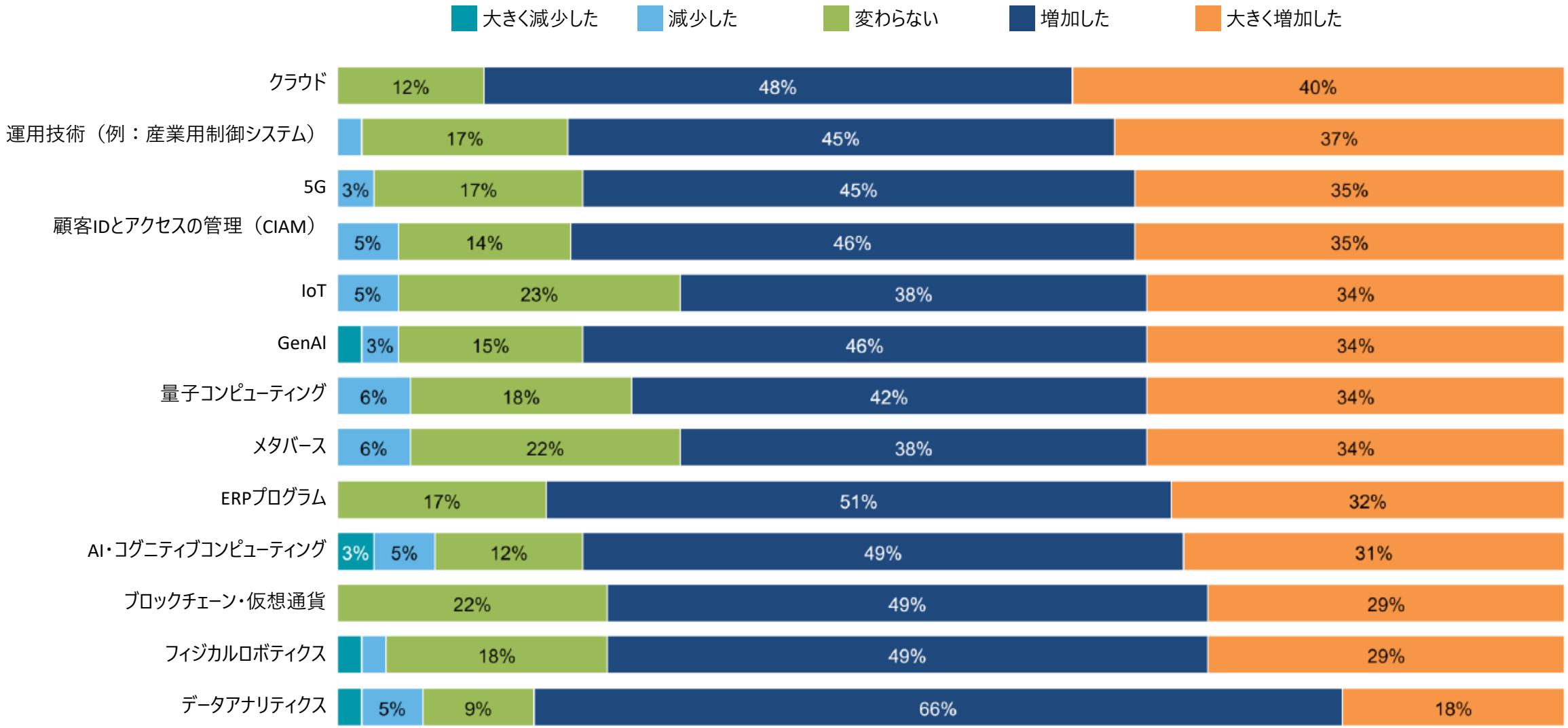
質問22：経営幹部や取締役会がサイバーセキュリティに適切に対処できるかどうかについて、どの程度確信がありますか。
質問23：CISOまたは同等のサイバーセキュリティリーダーの直属先はどこですか。

各取り組みの主要責任者

	CISO	CIO
サイバーセキュリティ侵害・攻撃への対応	54％	43％
なりすましや情報漏洩から顧客・消費者データを保護するための戦略策定	51％	43％
IT担当メンバーの管理、部門目標とベストプラクティスの構築と実践	51％	48％
セキュリティ意識向上トレーニングの実施	49％	46％
新技術に当初からセキュリティを組み込む設計と、その後の導入と管理	48％	48％
リスク対応のシナリオプランニングへの関与	48％	51％
新興技術に関連した新たなリスクの評価	48％	54％
サイバーセキュリティの脅威から組織を保護するための戦略の策定	46％	52％
サイバーセキュリティやテクノロジーに関する予算の策定と管理	46％	51％
取締役会へのサイバーセキュリティに関する最新情報の共有	45％	51％
サイバーセキュリティの脅威から組織を保護するための戦略の実行	43％	54％
セキュリティ監査と評価の実行	43％	57％
規制順守の徹底	43％	52％
サイバーセキュリティへの投資が明確なビジネス上の成果につながっているかの追跡	43％	54％

質問25：次の各取り組みの主要責任者は誰ですか。

CISOやサイバーセキュリティリーダーがテクノロジーの機能に関する戦略的な議論に参加する度合い

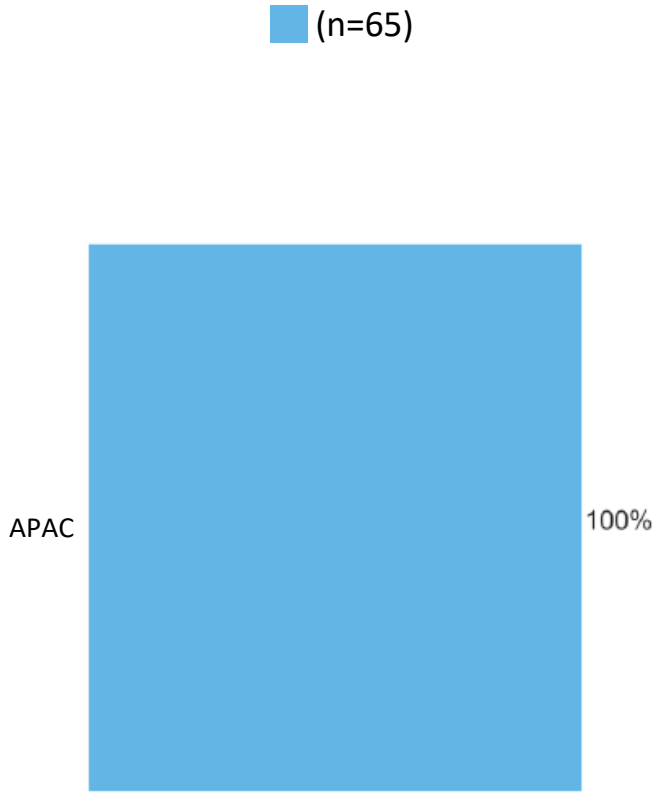


適用した国（国群）フィルター：日本

質問26：次の各テクノロジー機能に関する戦略的な議論について、CISO（または同等のサイバーセキュリティ責任者）が議論に関与する度合いは過去1年でどの程度変わりましたか。

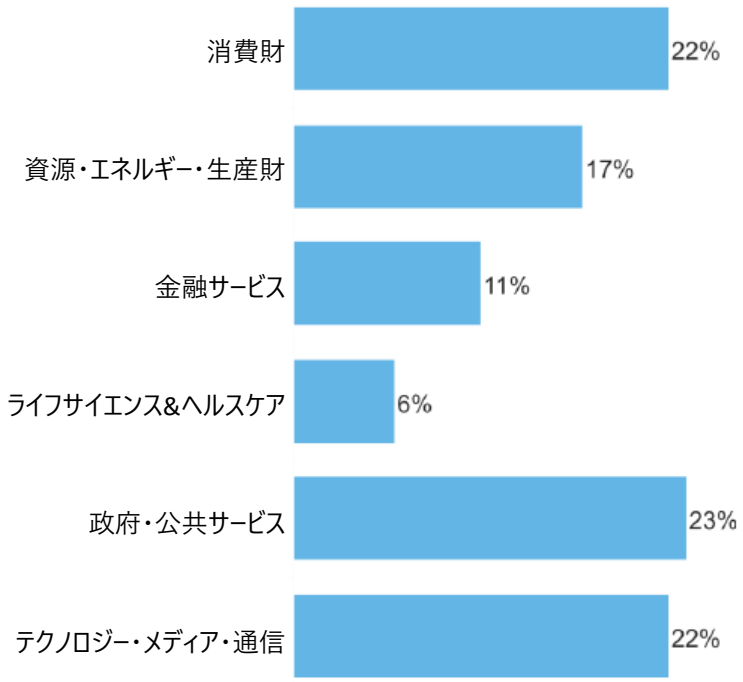
回答者の詳細

地域



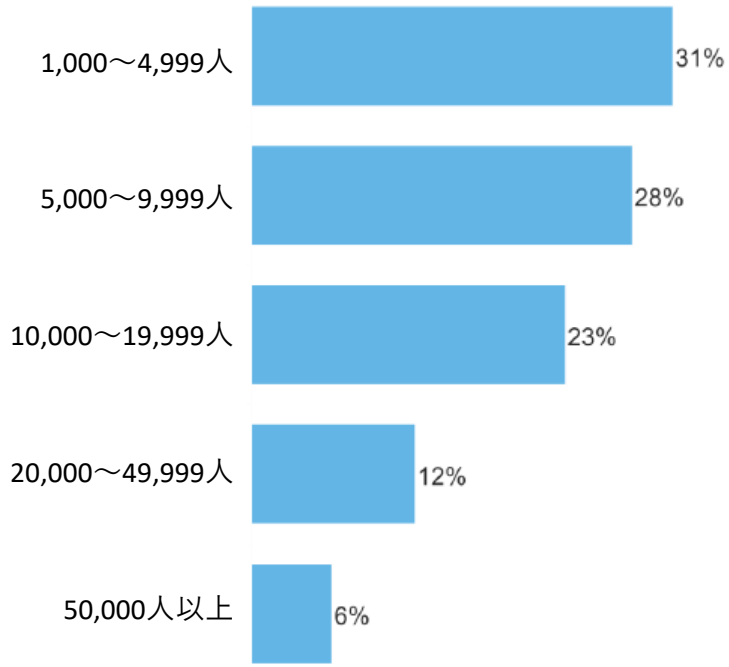
適用した国（国群）フィルター：日本

業界



適用した国（国群）フィルター：日本

組織の規模

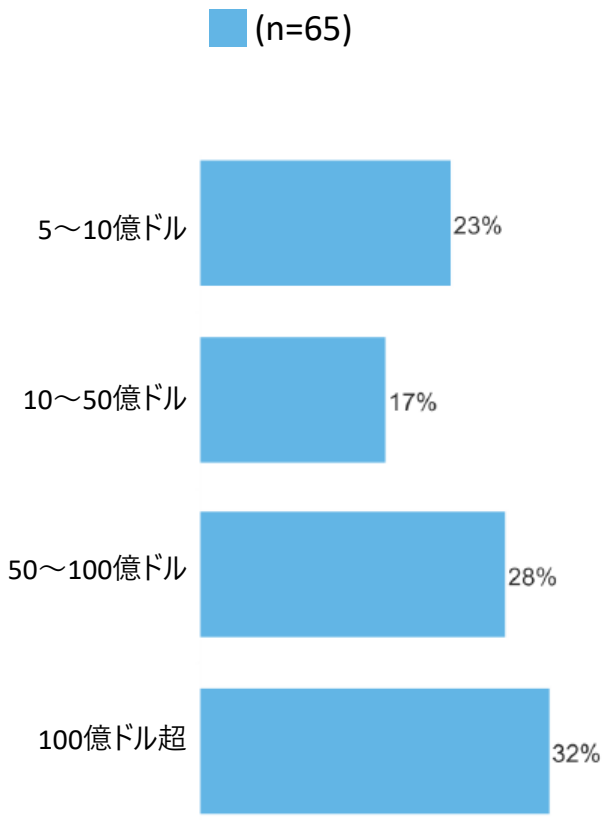


適用した国（国群）フィルター：日本

S1：自組織の主な所在地はどこですか。（1つ選択）
S2：自組織の事業は主にどの産業にあたりますか。（1つ選択）
S3：世界中の全拠点で合計したフルタイム従業員数は何人ですか。（1つ選択）

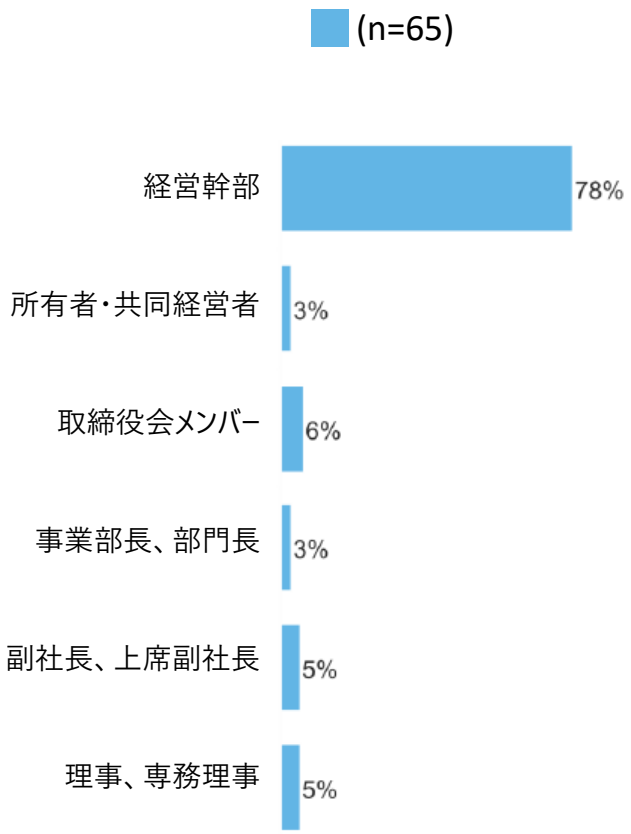
回答者の詳細

組織の売上高



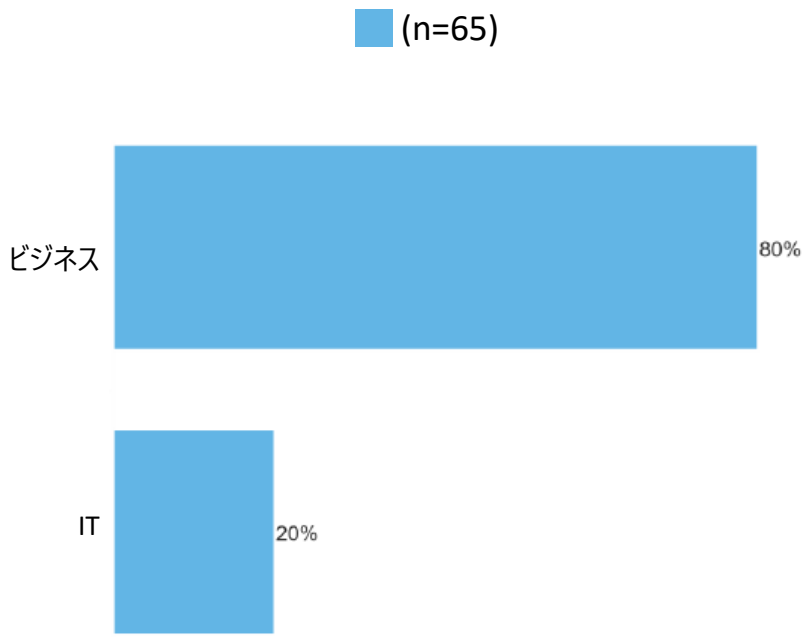
適用した国（国群）フィルター：日本

役割



適用した国（国群）フィルター：日本

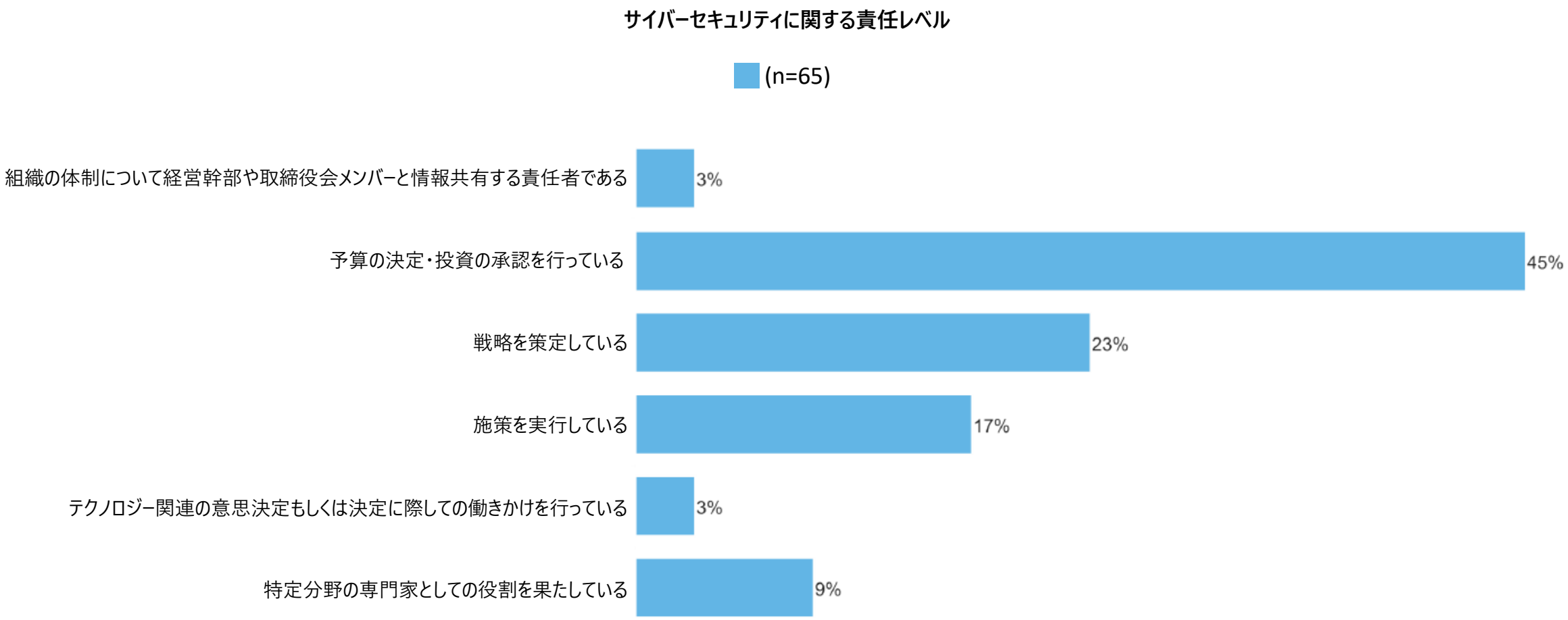
職務



適用した国（国群）フィルター：日本

S4：自組織の昨年度の年間売上高はどのくらいですか。（1つ選択）
S5：次のうち、ご自身の役職に最も近いものはどれですか。（1つ選択）
S6：ご自身の主な職務は何ですか。（1つ選択）

回答者の詳細



適用した国（国群）フィルター：日本

S7：次の各領域におけるサイバーセキュリティに関する意思決定に関する記述のうち、ご自身の責任レベルを最もよく表しているのはどれですか。

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ リスクアドバイザリー合同会社、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人、DT弁護士法人およびデロイト トーマツ グループ合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約30都市に約2万人の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト、www.deloitte.com/jpをご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTLおよびDTTLの各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTLはクライアントへのサービス提供を行いません。詳細はwww.deloitte.com/jp/aboutをご覧ください。
デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務・法務などに関連する最先端のサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促し、より豊かな経済、公正な社会、持続可能な世界の実現に向けて自ら率先して取り組むことを通じて、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来175年余りの歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの45万人超の人材の活動の詳細については、www.deloitte.comをご覧ください。

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

Member of
Deloitte Touche Tohmatsu Limited