情報セキュリティを確保するために

アーンスト・アンド・ヤング
2012 グローバル情報セキュリティサーベイ

新日本有限責任監査法人

ERNST & YOUNG

Quality In Everything We Do

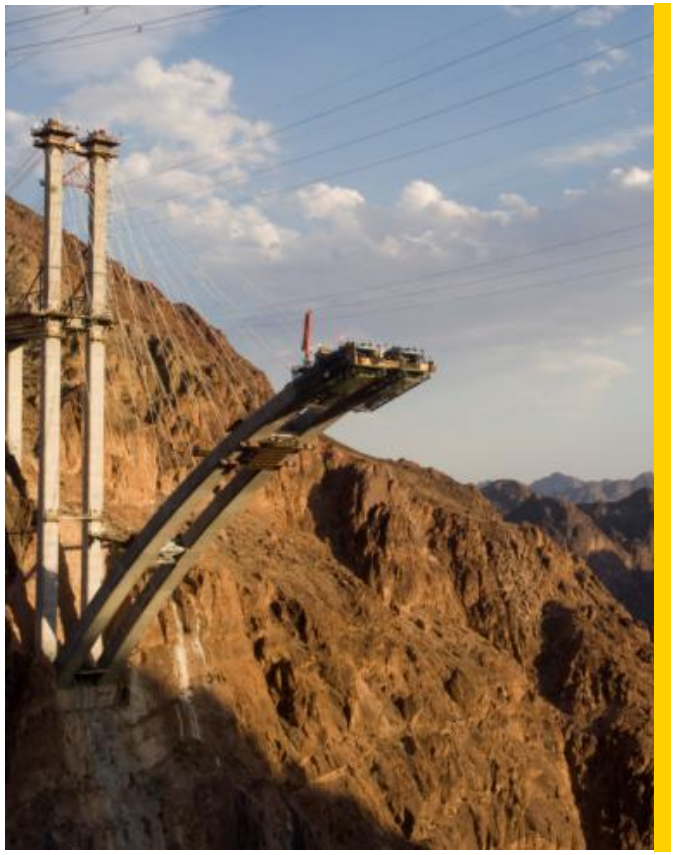
はじめに

今年で15年目を迎えるアーンスト・アンド・ヤングのグローバル情報セキュリティグローバルサーベイ（GISS）は、この種の調査では最も長期にわたっており、お客様に情報セキュリティの問題による影響を他社と比較し、重要な意思決定を支援するものとしてお役立て頂いております。

本年度のサーベイは、2012年6月から8月の期間、全主要産業において、64カ国、1,836社（日本では201社）のお客様にご参加頂きました。

Contents

調査結果概要



今年度のアーンスト・アンド・ヤングのグローバル情報セキュリティサーベイの前半では、情報セキュリティの管理状況を、後半では、注目されている領域についてグローバルをベンチマークとし、日本との差異が著しい点を中心に考察しています。

「1. セキュリティ予算と投資」では、事業継続計画を始めとする情報セキュリティ対応を年々強化していることが分かる一方、「4. 脅威、リスク及びインシデント」では、内部の脆弱性について日本が過小評価している可能性が読み取れます。

「2. セキュリティガバナンス」「3. 情報セキュリティの有効性」では、日本が情報セキュリティに関する組織が会社の要件を満たしていないこと、スキルを有する人材不足という課題を抱えていることが明確になっています。

「6.クラウドコンピューティング」では、サービスを利用する際のリスクを認識し、対応している一方、「5.モバイルコンピューティング」「7.ソーシャルメディア」では、急速な普及に情報セキュリティ面の対応が追い付いていない状況です。

「8.情報セキュリティ技術」では、既存の製品を十分に活用できていない一方、セキュリティポリシーを実現する技術としてDLP（情報漏洩防止）ツールが活用され始めていることが確認できます。

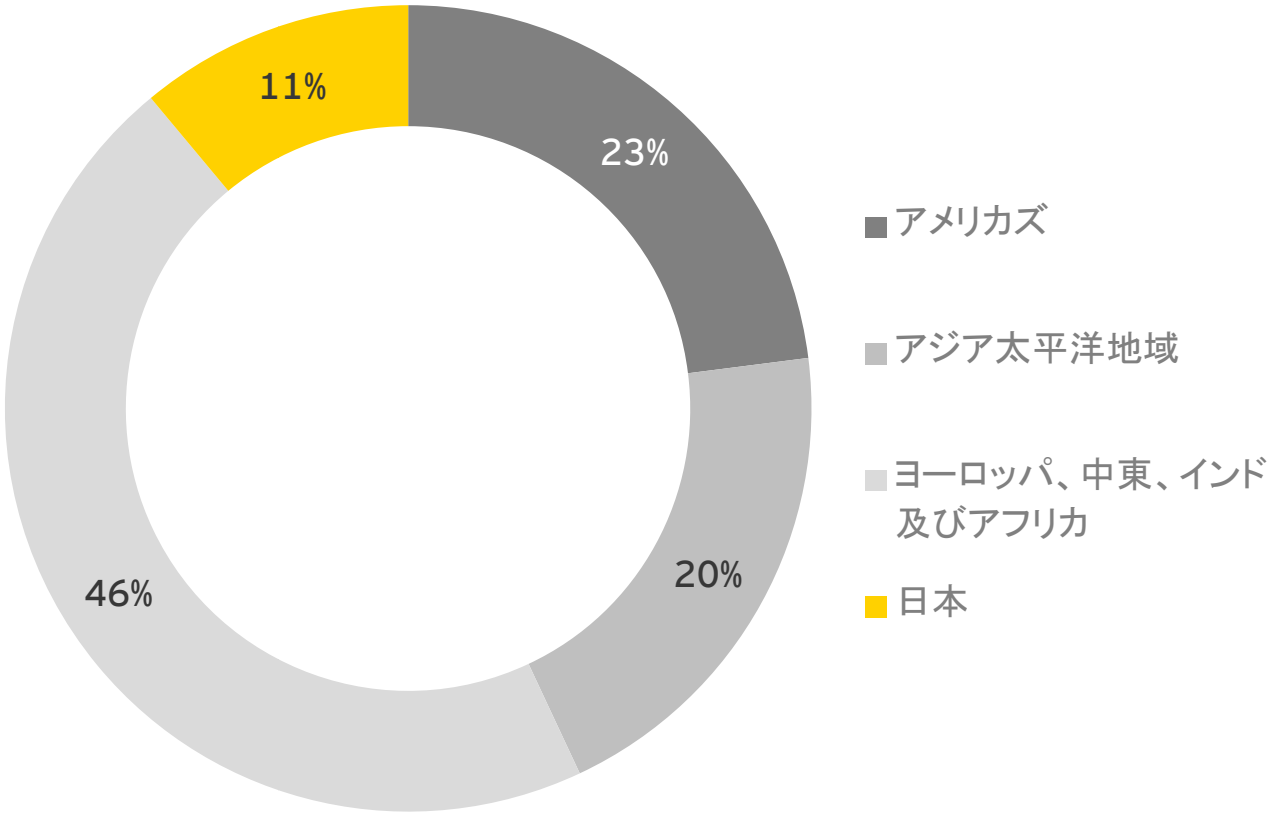
サーベイ参加者の属性

地域別内訳

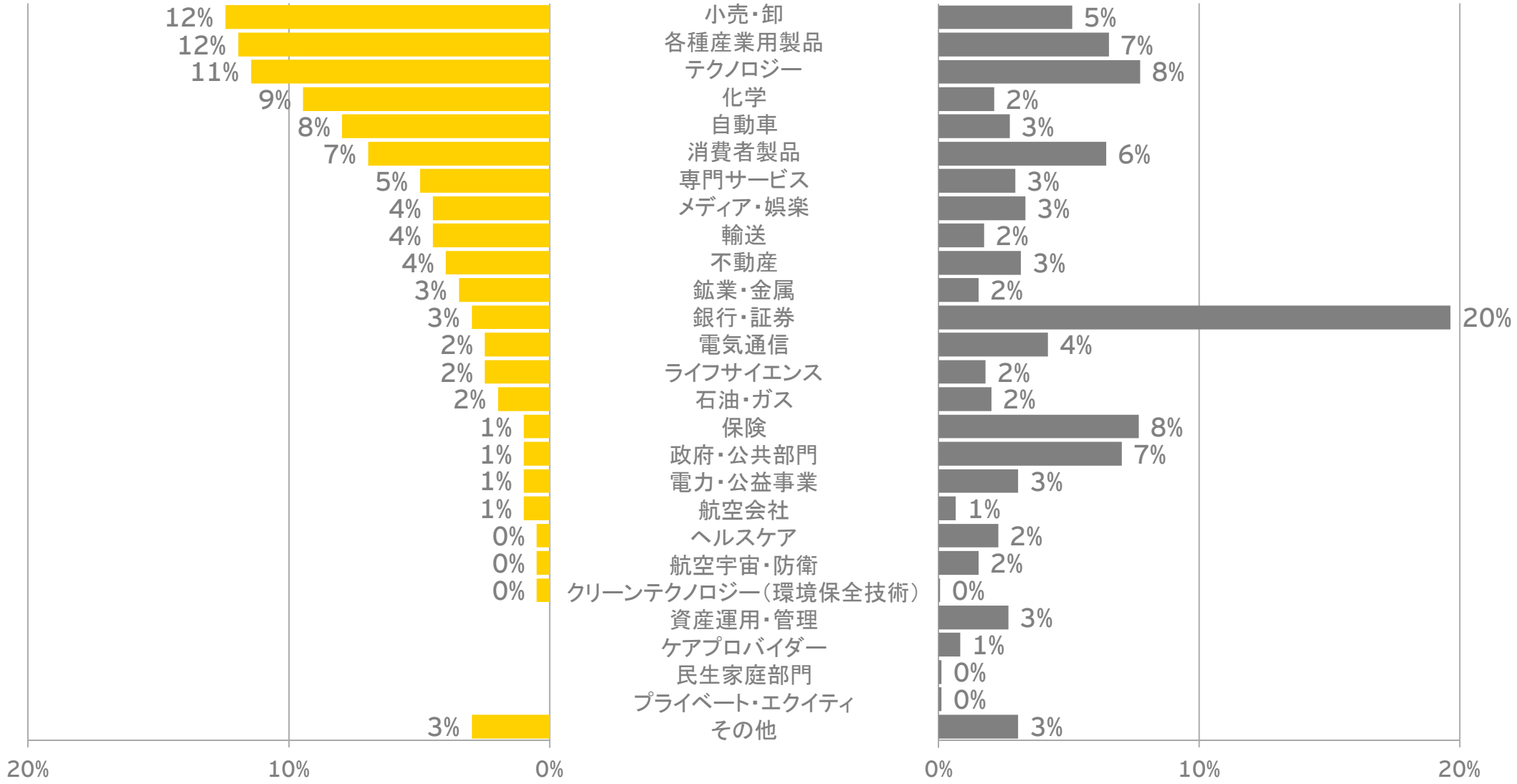
- 今年度のアーンスト・アンド・ヤングのグローバル情報セキュリティサーベイには、64カ国1,836社（日本では201社）のお客様にご参加頂きました

- 主要な参加国（回答数トップ10）

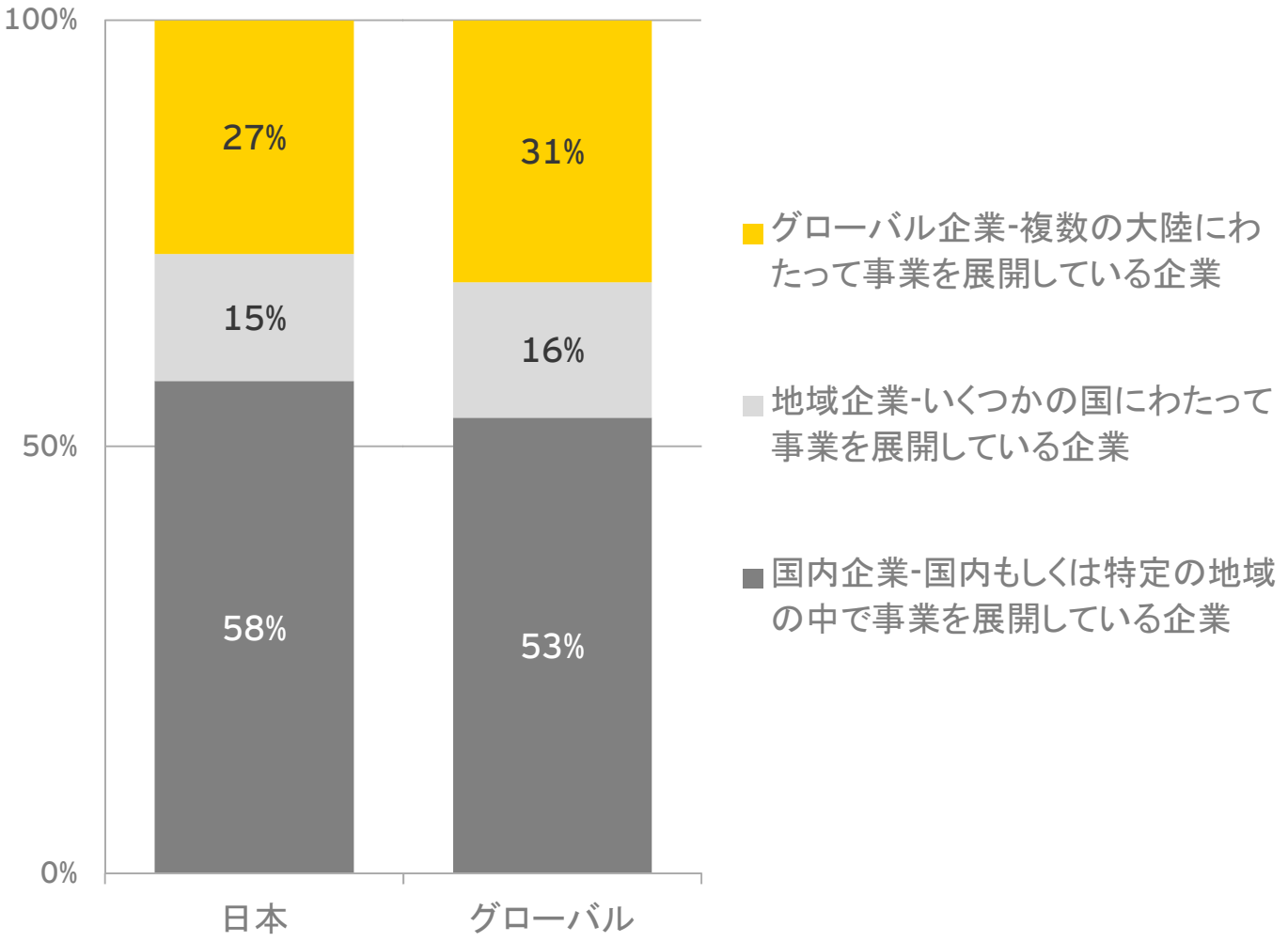
1.	アメリカ	16%
2.	日本	11%
3.	オーストラリア	7%
4.	中国（香港含む）	7%
5.	インド	5%
6.	ジンバブエ	4%
7.	オランダ	4%
8.	スイス	3%
9.	イタリア	3%
10.	ルクセンブルグ	3%



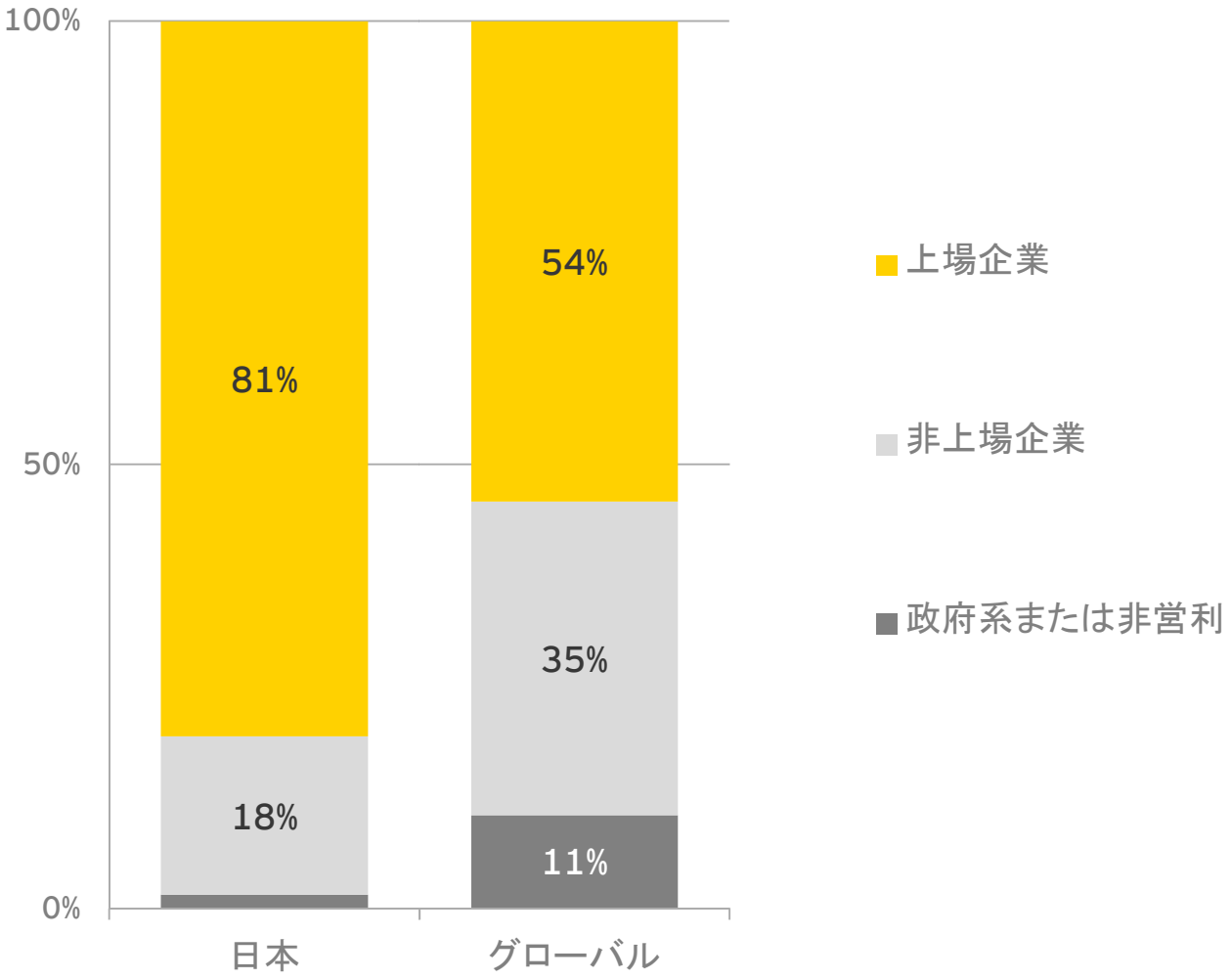
産業別内訳



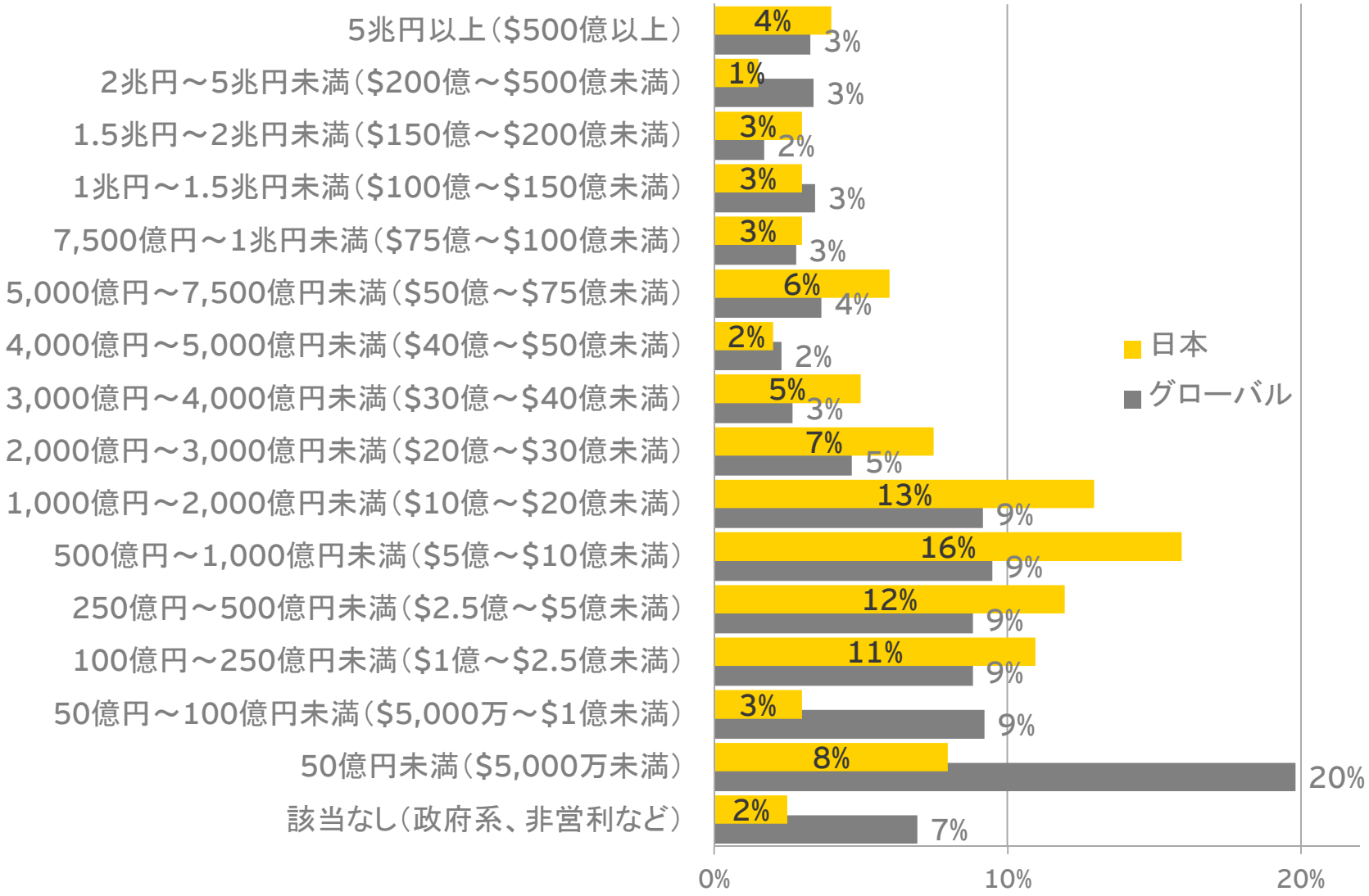
事業形態別



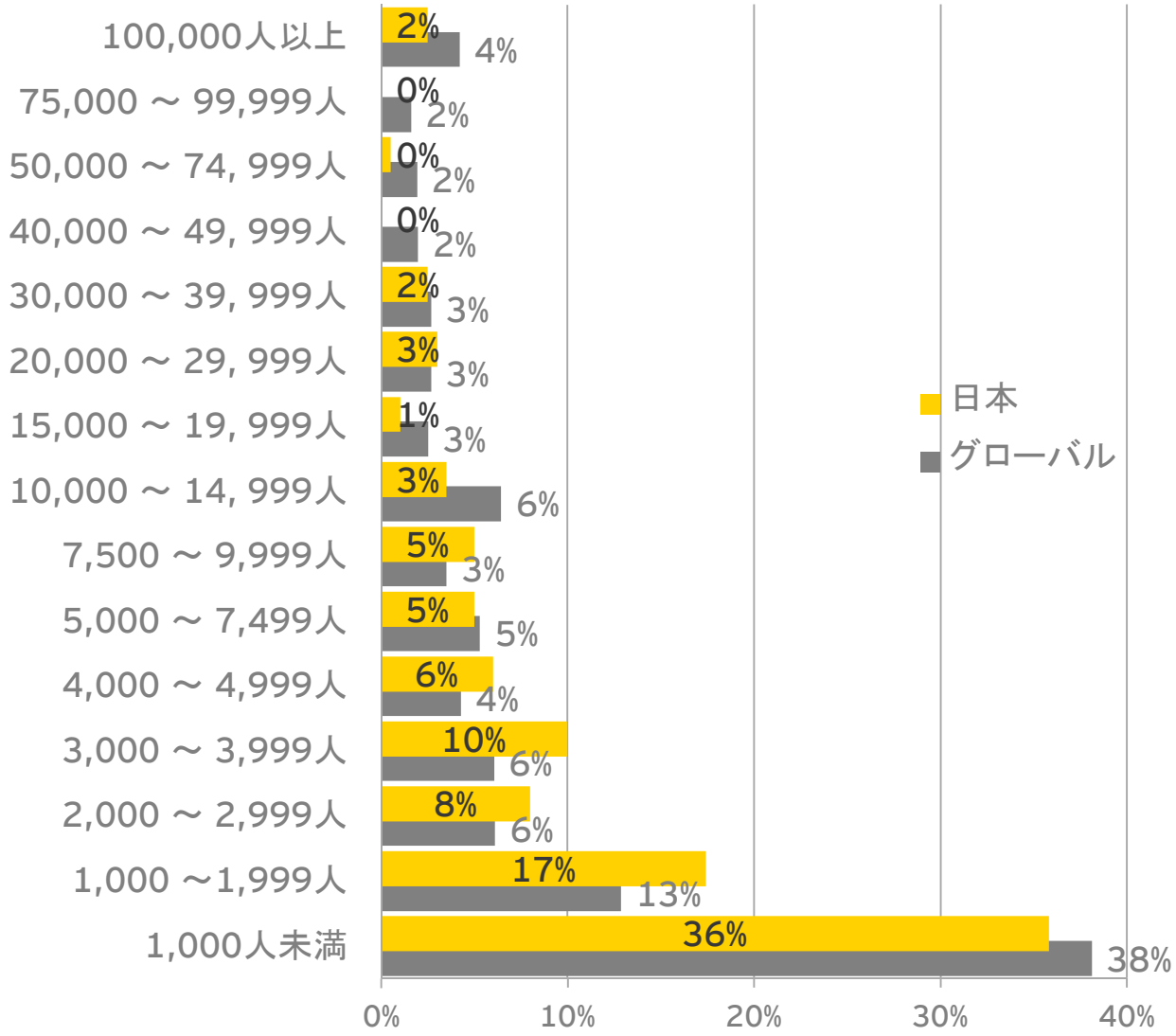
企業形態別



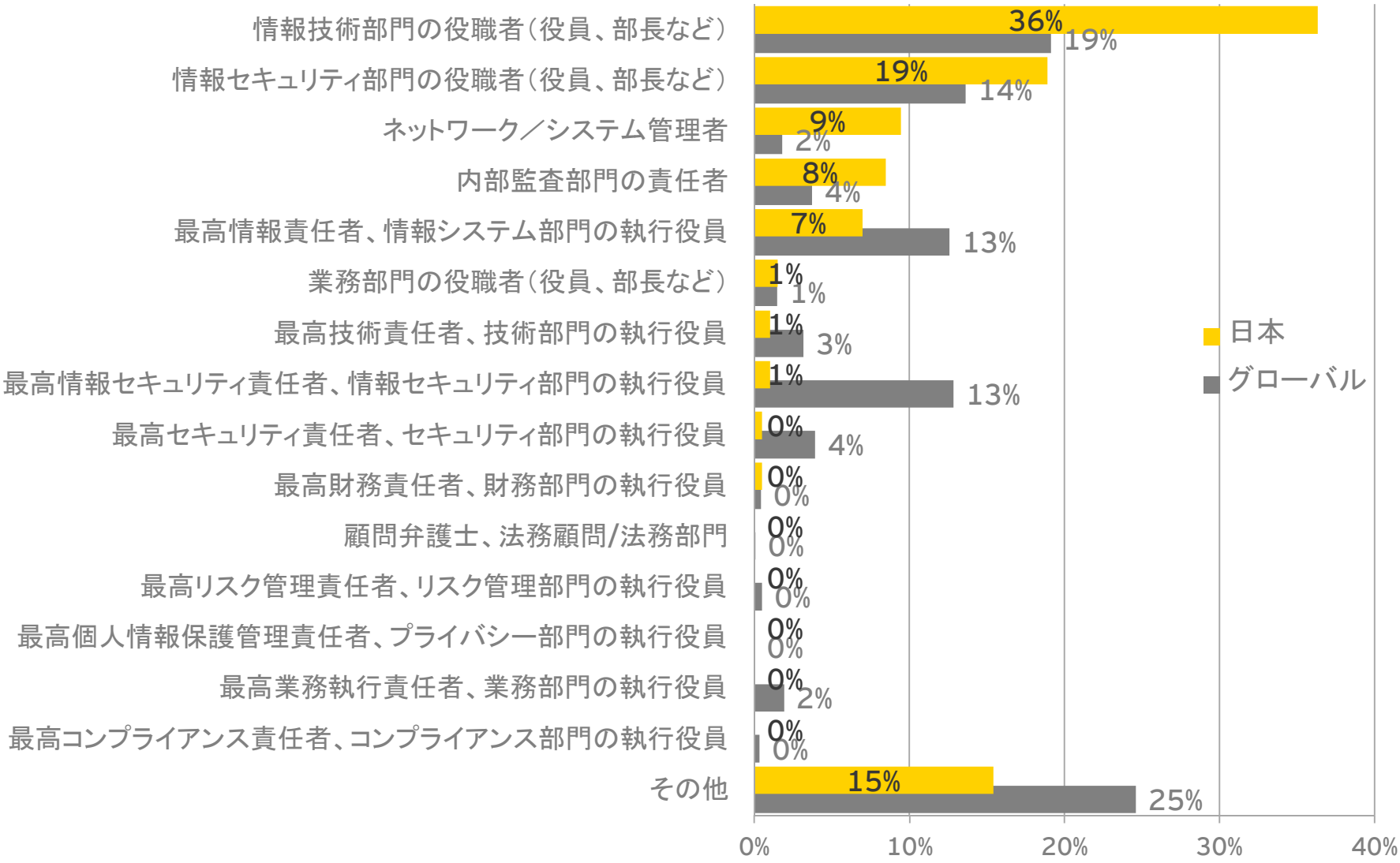
年間収益(売上)別内訳



従業員数別内訳



回答者別内訳



調査結果

1.セキュリティ予算と投資

1.セキュリティ予算と投資

調査結果の概要と私たちの見解

企業は、これまでの情報セキュリティの対応を見直しつつ、より高いレベルを目指しています

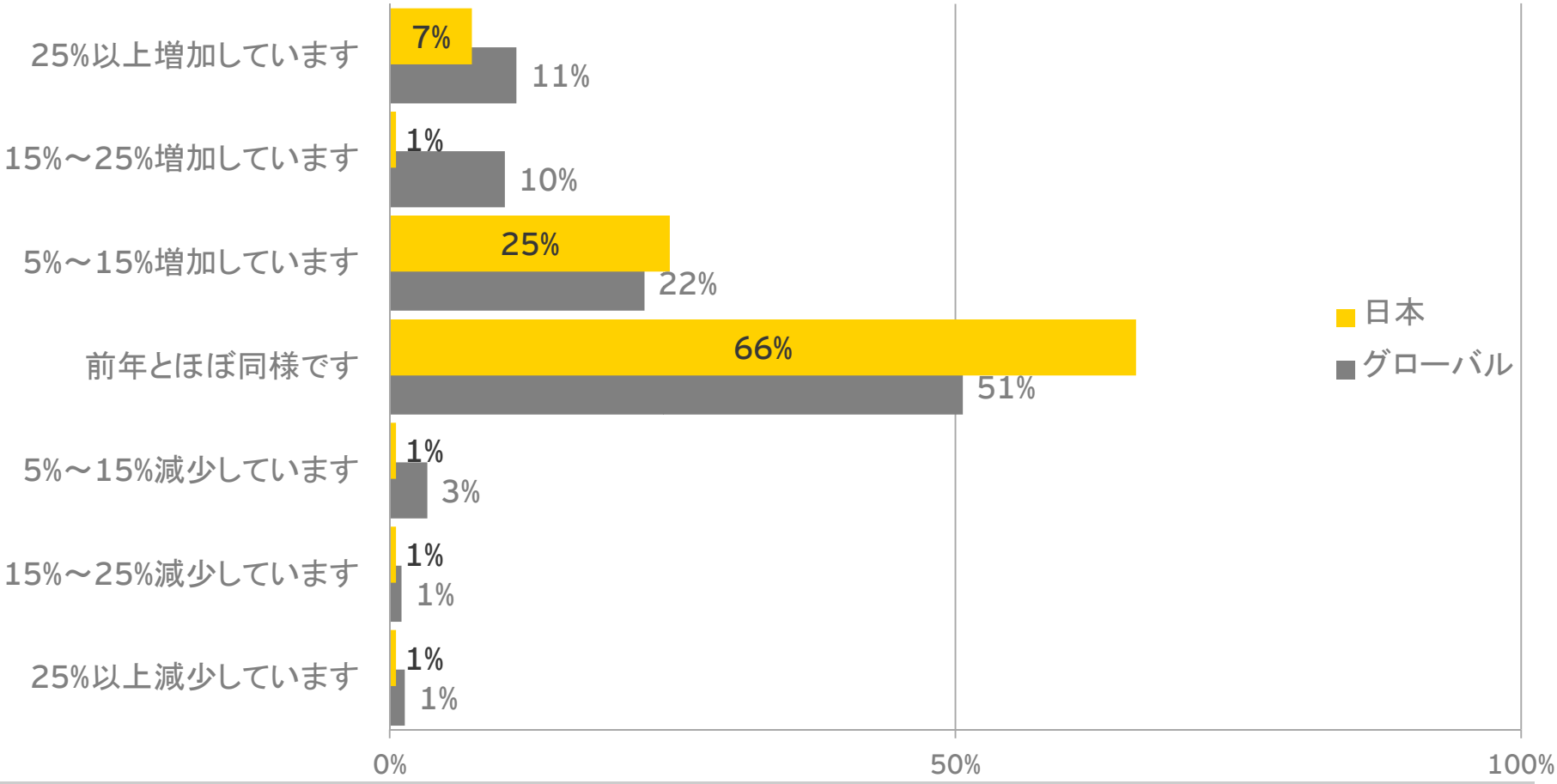
- 情報セキュリティ予算を増やす企業の比率が高まっています
- セキュリティ改善への支出額が増えています
- 日本では、過半数が情報セキュリティに1,000万円～1億円未満を支出しています
- 日本では、セキュリティ運用を含む技術面への支出割合が、グローバルより14ポイント高い32%です

昨年から引き続き「事業継続/緊急復旧計画」が、情報セキュリティにおいて最も関心の高い分野です

- 支出が増加している分野の上位2位は、「セキュリティの新技術」「事業継続/緊急時復旧計画」です
- 今後12か月で優先度の高いセキュリティ項目は、「事業継続/緊急時復旧計画」「情報漏洩技術およびプロセス」です

1.1.過去12か月の情報セキュリティ予算の状況

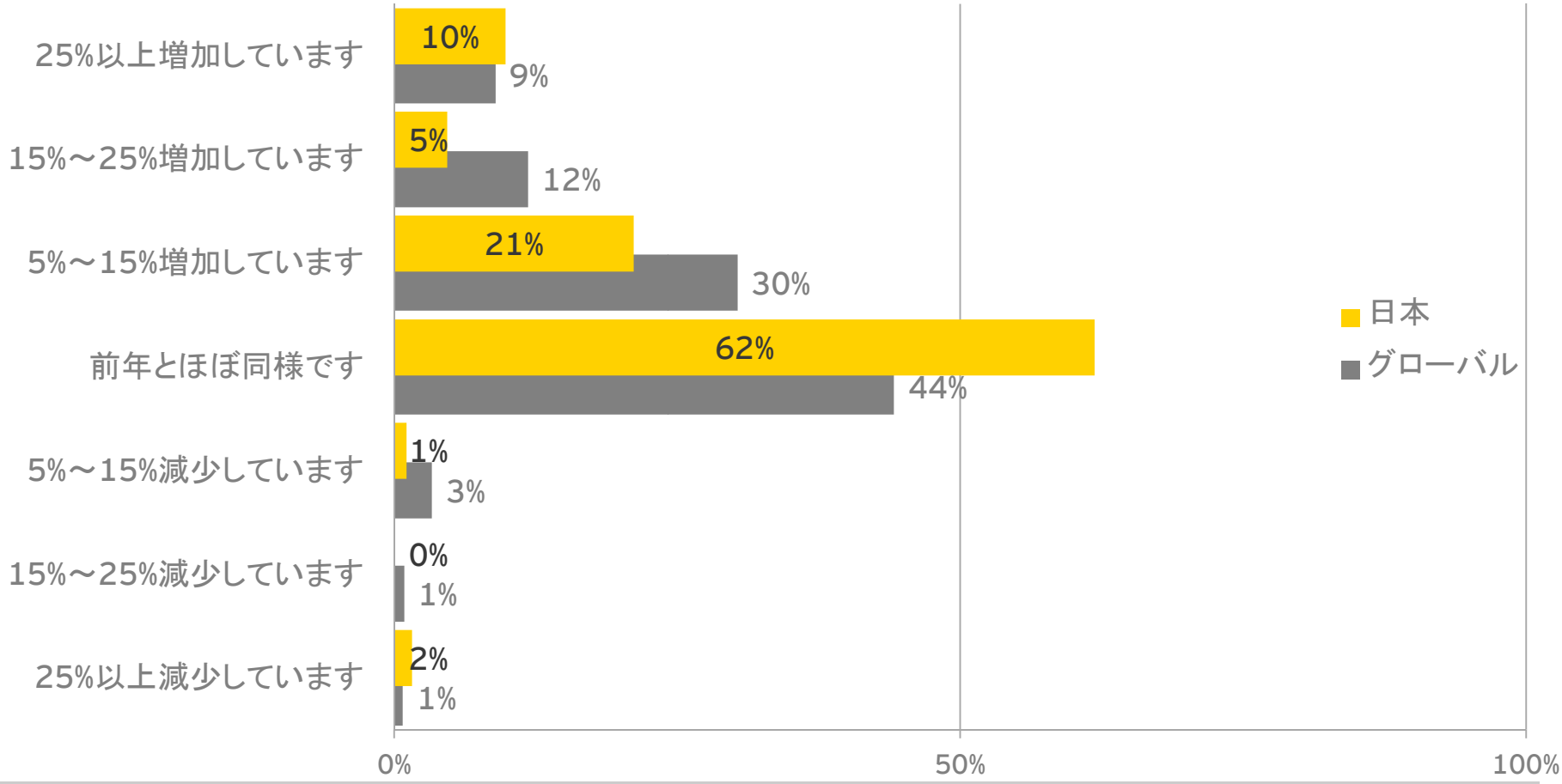
Q1.　過去12か月間（または前年度）の情報セキュリティ予算の変化について、貴社に該当するものを1つ選択して下さい。



- 情報セキュリティ予算を増やす企業の比率が高まっています
- 過去12か月では、日本で33%、グローバルで43%の企業が、過去12か月間（または前年度）より情報セキュリティ予算を増加させています

1.2.今後12か月の情報セキュリティ予算計画の状況

Q2.　今後12か月間（または当年度）の情報セキュリティ予算計画の変化について、貴社に該当するものを1つ選択して下さい。

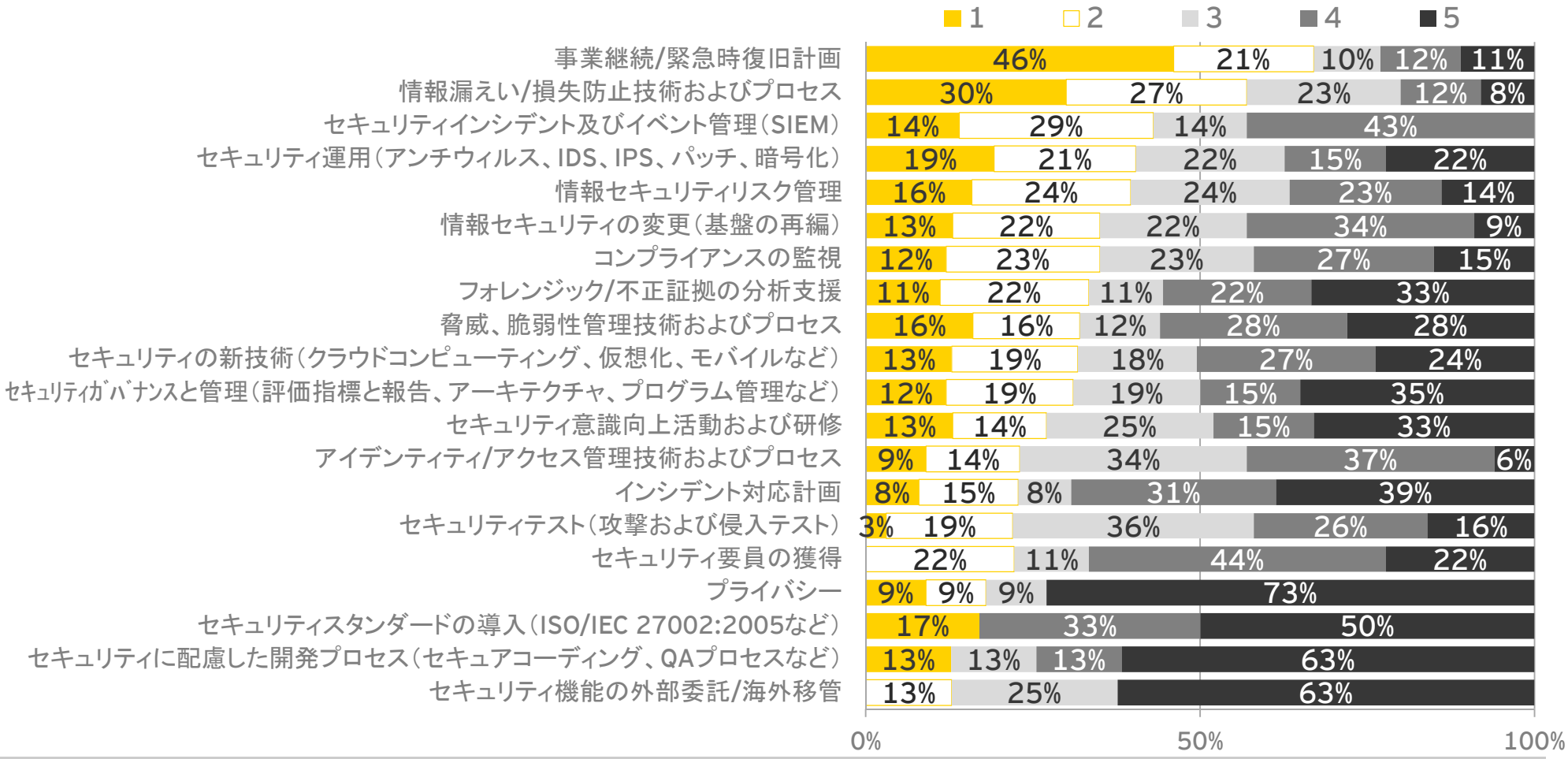


- 日本で36%、グローバルで51%の企業が、今後12か月間（または当年度）の情報セキュリティ予算を増加させます

日本

1.3.セキュリティ項目の優先度

Q3. 今後12か月間（または当年度）で最優先と考えるセキュリティ項目を下記より5つ選択し、優先度の高いものから順に1、2、3、4、5と番号を記入ください。

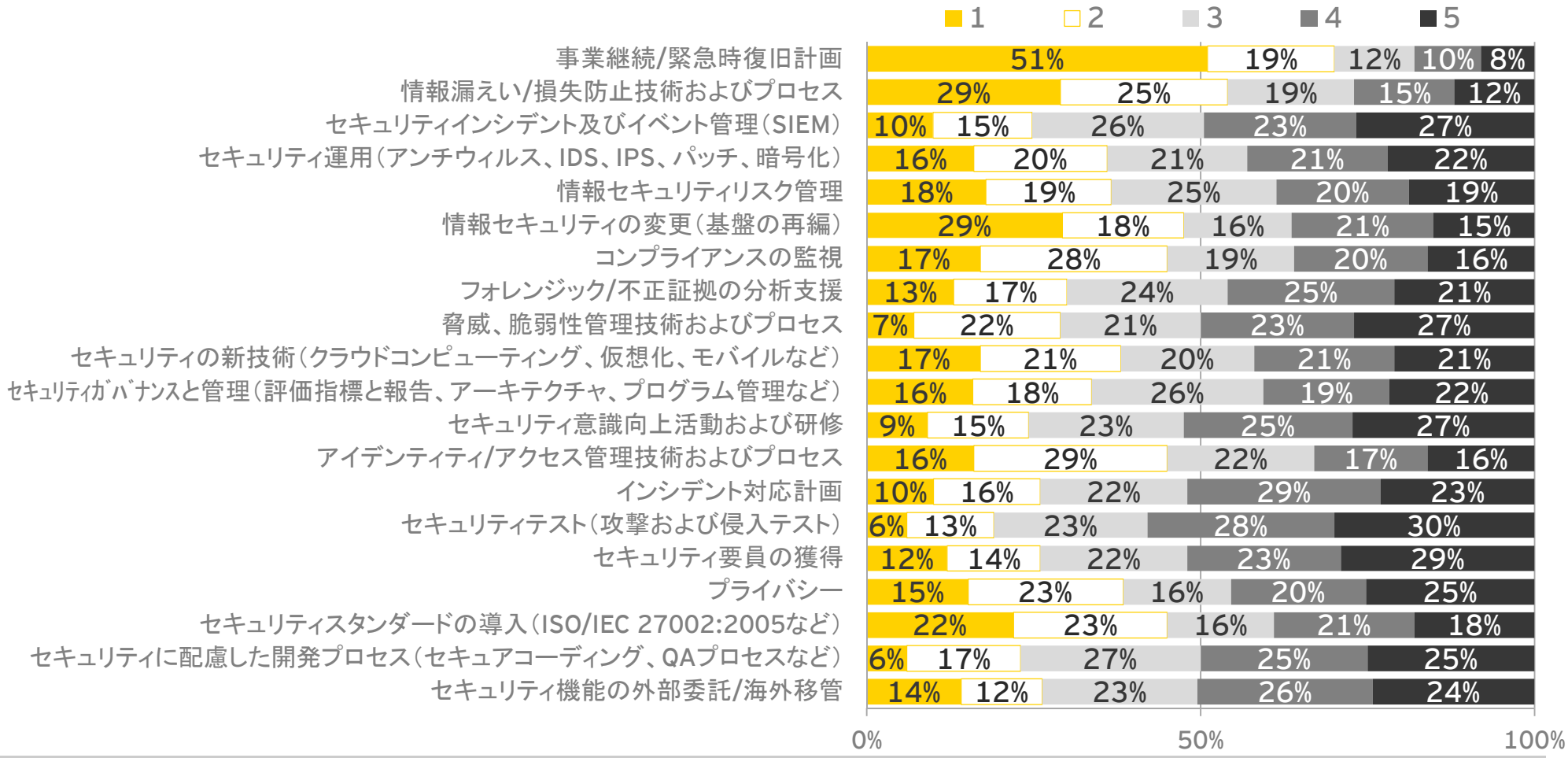


- 日本では、「事業継続/緊急時復旧計画」「情報漏えい/損失防止技術およびプロセス」「セキュリティインシデント及びイベント管理（SIEM）」が、優先度が高いセキュリティ項目として認識されている傾向があります

グローバル

1.3.セキュリティ項目の優先度

Q3. 今後12か月間（または当年度）で最優先と考えるセキュリティ項目を下記より5つ選択し、優先度の高いものから順に1、2、3、4、5と番号を記入ください。

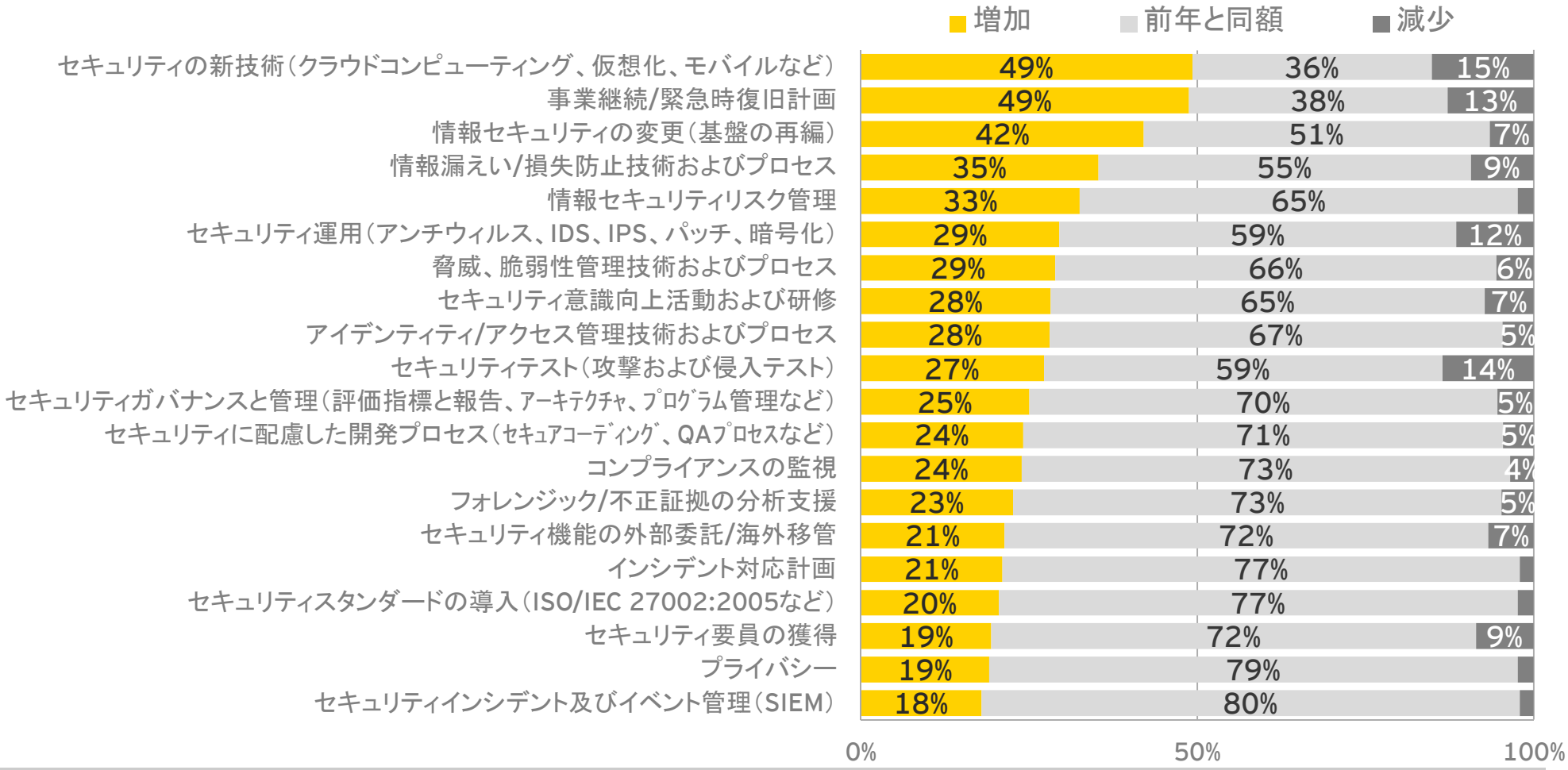


- グローバルでは、「事業継続/緊急時復旧計画」「情報漏えい/損失防止技術およびプロセス」「情報セキュリティの変更（基盤の再編）」が、優先度が高いセキュリティ項目として認識されている傾向があります

日本

1.4.セキュリティ分野における支出計画

Q4. 当年度の予算を前年度と比較した場合、下記の項目で支出（計画）のある分野についてのみ「増加」「減少」「前年と同額」から該当するものを1つ選択してください。

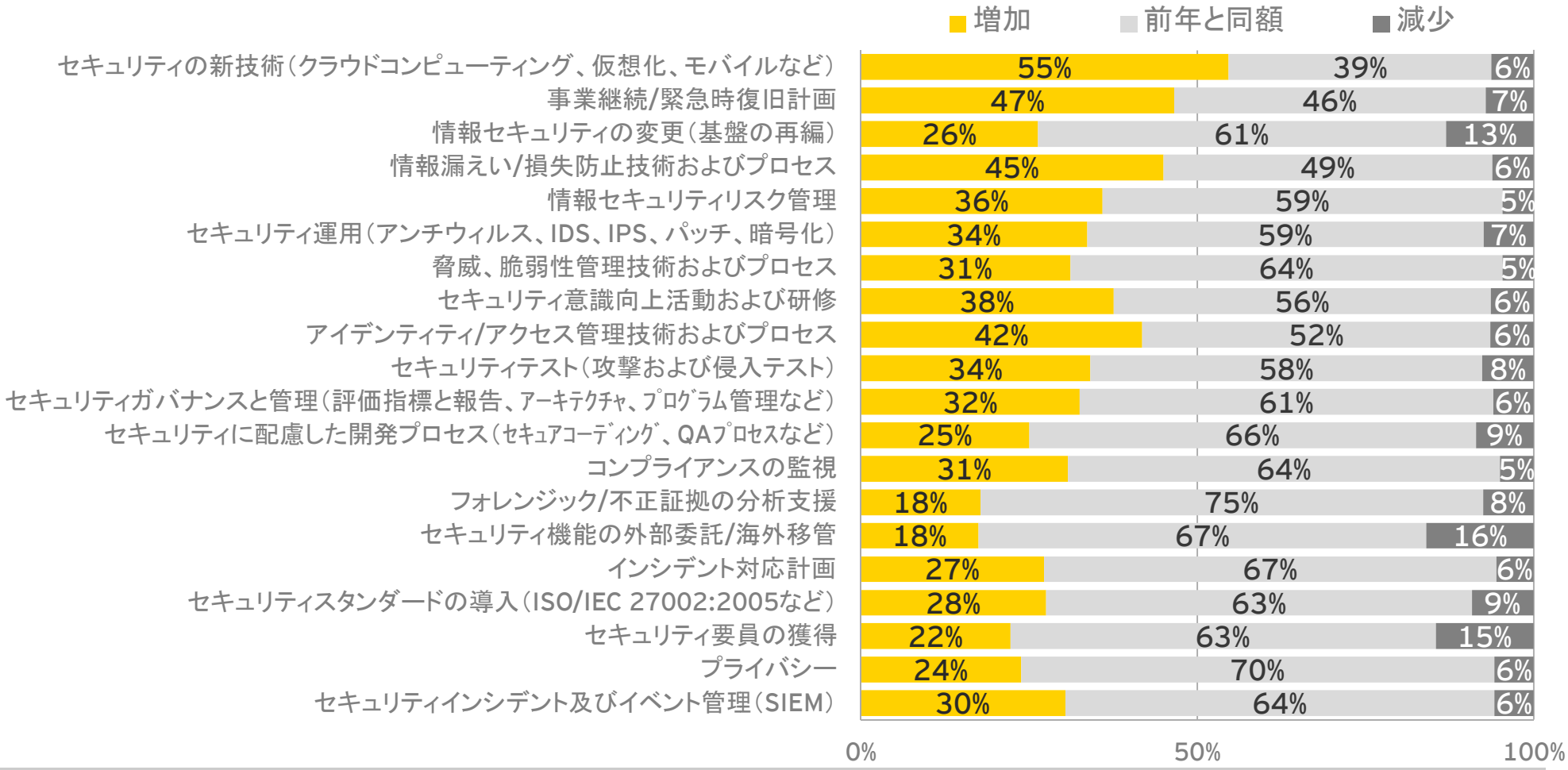


- 日本では、「セキュリティの新技術」「事業継続/緊急時復旧計画」「情報セキュリティの変更（基盤の再編）」に関する分野の支出（計画）を増加させている傾向があります

グローバル

1.4.セキュリティ分野における支出計画

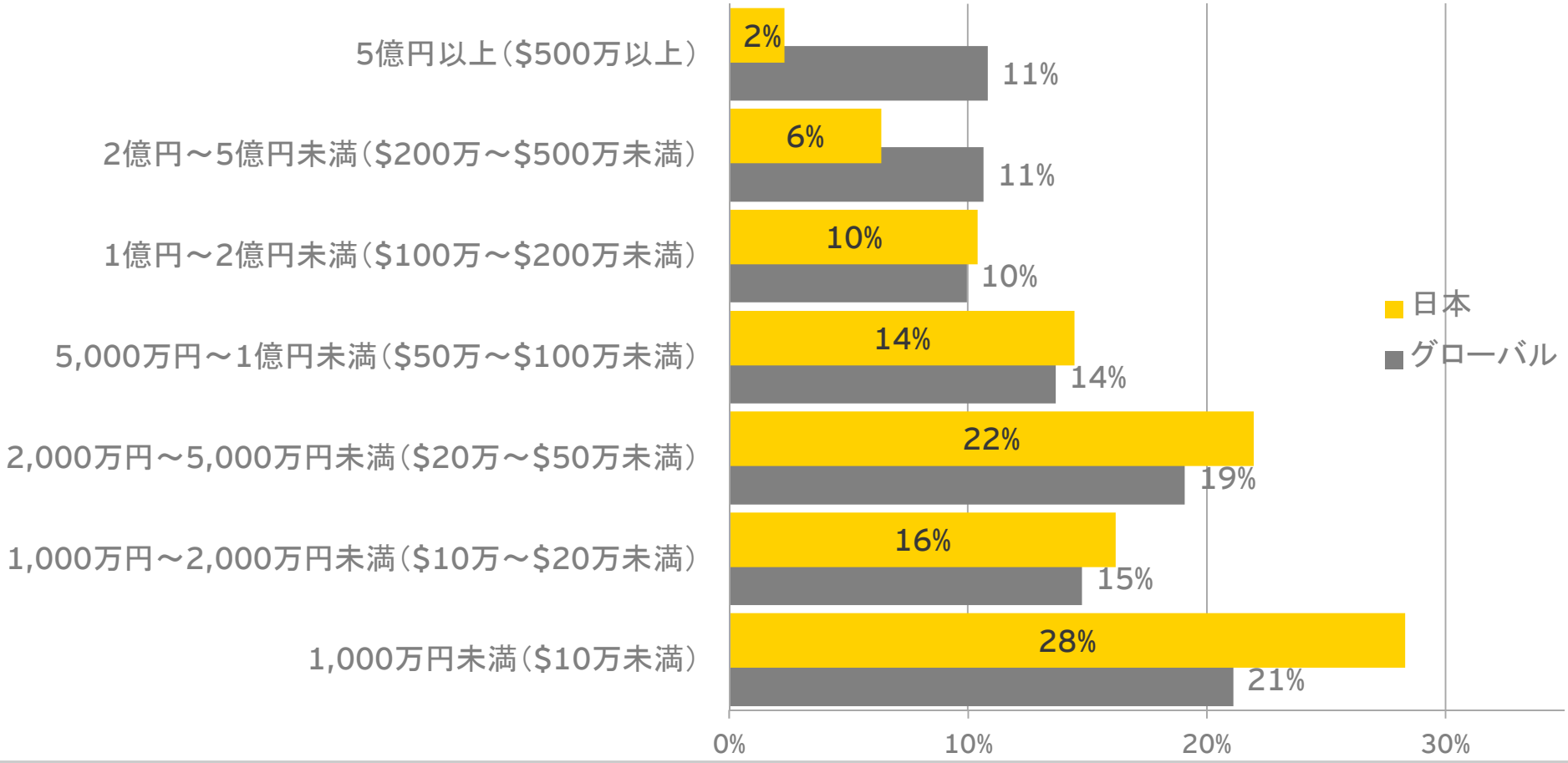
Q4. 当年度の予算を前年度と比較した場合、下記の項目で支出（計画）のある分野についてのみ「増加」「減少」「前年と同額」から該当するものを1つ選択してください。



- グローバルでは、「セキュリティの新技術」「事業継続/緊急時復旧計画」「情報漏えい/損失防止技術およびプロセス」「アイデンティティ/アクセス権管理技術およびプロセス」に関する分野の支出(計画）を増加させている傾向があります

1.5.情報セキュリティに関する会社全体の支出額

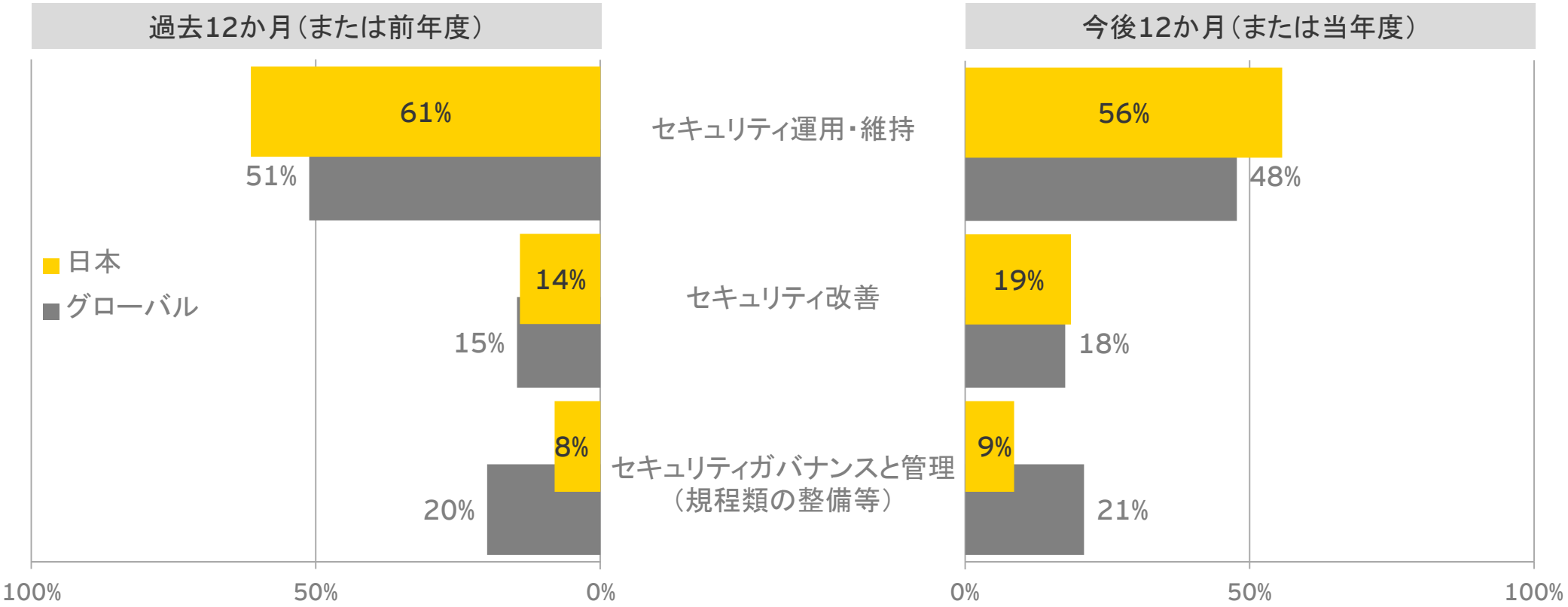
Q5. 情報セキュリティに関する会社全体の支出額（人件費（研修、コンサルタント契約、セキュリティ部門の給与等）、プロセス（運用に関するセキュリティ費用等）、技術費用（セキュリティ技術のライセンスや技術メンテナンス等）の前年度実績）について、貴社に該当するものを1つ選択してください。



- 日本では、過半数の企業が、情報セキュリティに1,000万円～1億円未満を支出しています
- グローバルとの比較において、日本は売上規模に対するセキュリティ支出の割合が低い傾向にあります（p.9との比較）

1.6.情報セキュリティ分類毎の支出割合

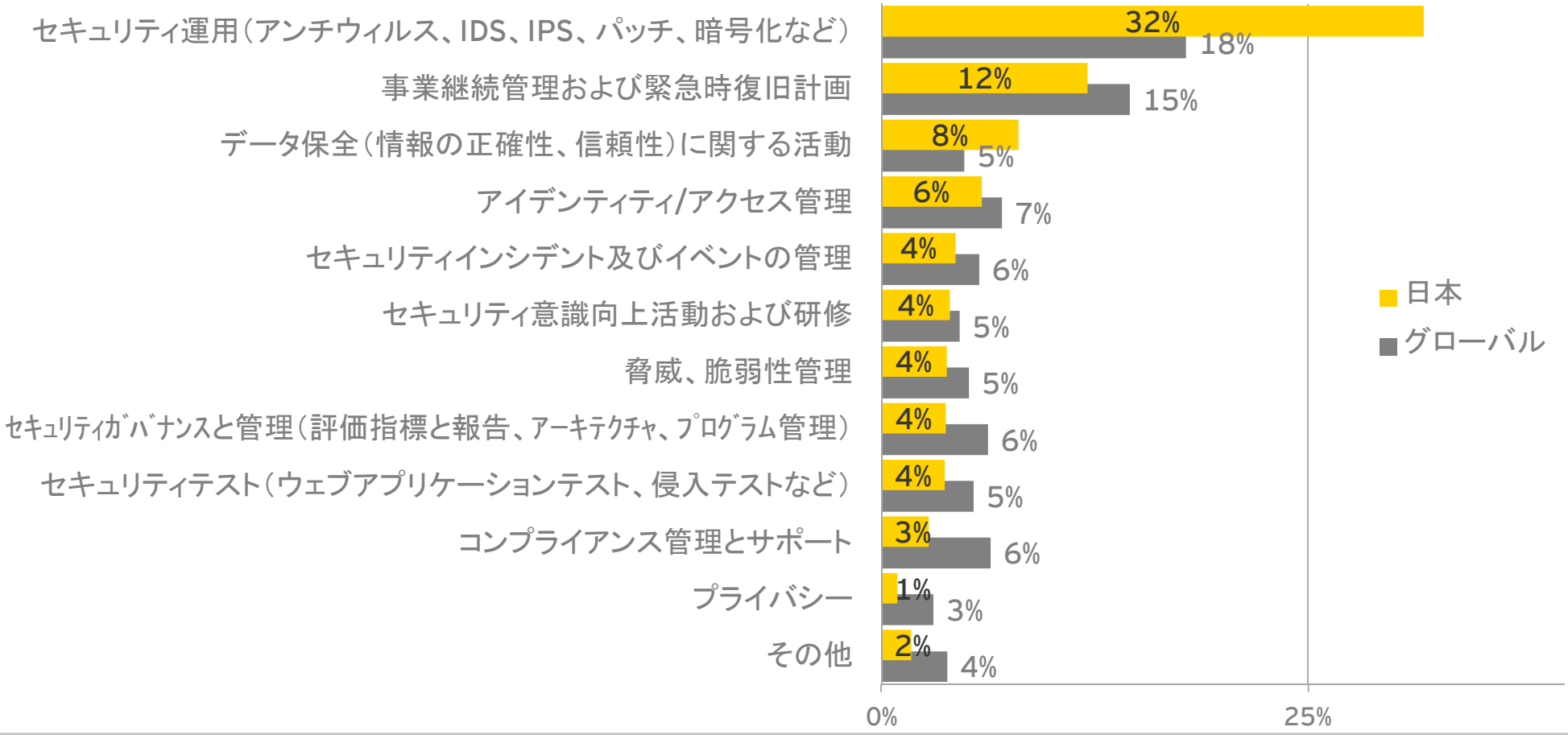
Q6. 次の支出分類における過去12か月（または前年度）及び今後12か月（または当年度）の支出額の割合（概算）を記入してください。



- 日本では、セキュリティ運用・維持に対する支出の割合が減少する一方で、セキュリティ改善への支出割合を増やしていく傾向があります

1.7.情報セキュリティの分野に対する支出割合

Q7.　次の情報セキュリティの分野に対する支出額（前年度実績）の割合（概算）を記入してください。



- 日本では、セキュリティ運用を含む技術面への支出割合が突出して高い傾向があります
- グローバルでは、様々なセキュリティ分野に分散して支出している傾向があります

調査結果

2.セキュリティガバナンス

2.セキュリティガバナンス

調査結果の概要と私たちの見解

日本では、情報セキュリティに関して各部門と経営層の連携を促す機能をより充実させることが期待されます

- 日本では、情報セキュリティ戦略をIT戦略と一致させている一方で、会社の業務戦略との整合が不足しています
- 約半数が、情報セキュリティに関するトピックを4半期に1度以上取り上げています
- 日本では、情報セキュリティ組織が最高経営責任者へ直接報告する割合が、グローバルより10ポイント高い18%であるのが特徴です
- 日本では、安否確認を含む連絡体制が充実している一方、重要な事業を継続するための対応が不足しています

日本では、他の組織の活用や他の組織との連携をより充実させることが期待されます

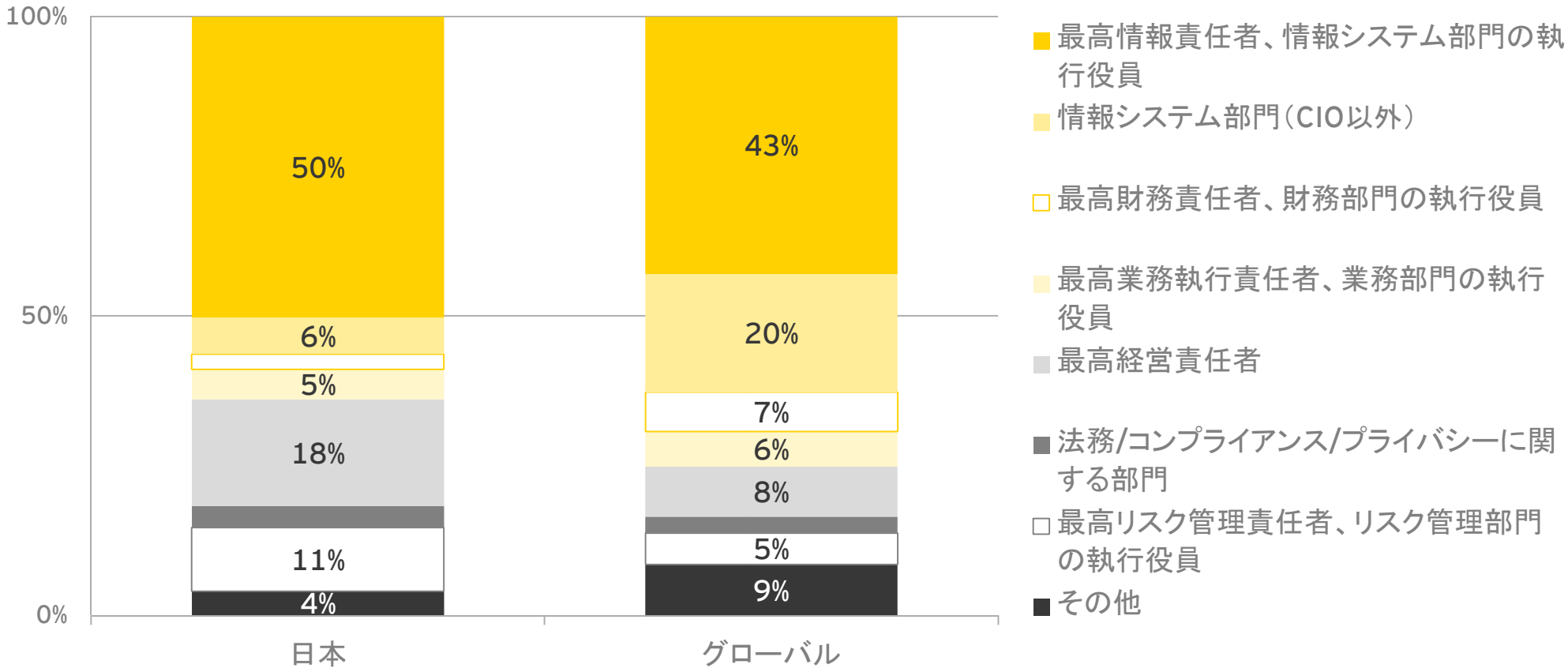
- 日本では、パートナー企業等への外部評価の活用がグローバルの23%に対して、1%とほとんど活用されていません
- 日本では、脅威情報を把握するためのプログラムへの取り組みが、グローバルより22ポイント低い41%にとどまります

日本では、情報セキュリティ全般を管理するために、「ISO/IEC 27000」シリーズを最も利用しています

- 日本では、「セキュリティテスト」「セキュリティ意識向上活動、研修、コミュニケーション」「セキュリティガバナンスと管理」分野において、セキュリティ機能の成熟度が低いと考えている傾向があります
- 日本では、国際標準化機構が発行している「ISO/IEC 27000」シリーズを最も利用しています

2.1.情報セキュリティの報告先

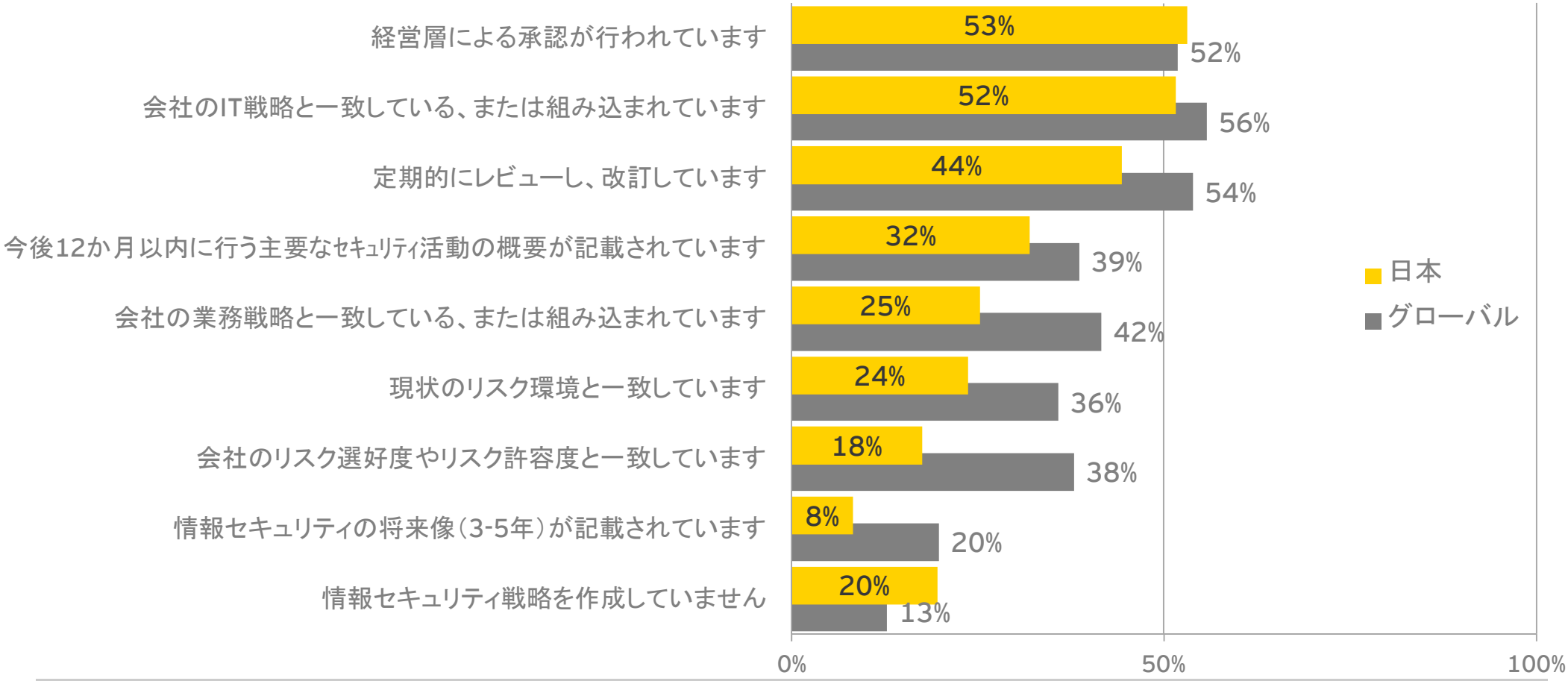
Q8.　情報セキュリティ組織が報告を行う主な報告先について、下記の項目から該当するものを1つ選択してください。



- 日本では、情報セキュリティ組織が最高経営責任者へ直接報告する割合が、グローバルより10ポイント高い18%であるのが特徴です

2.2.情報セキュリティ戦略の状況

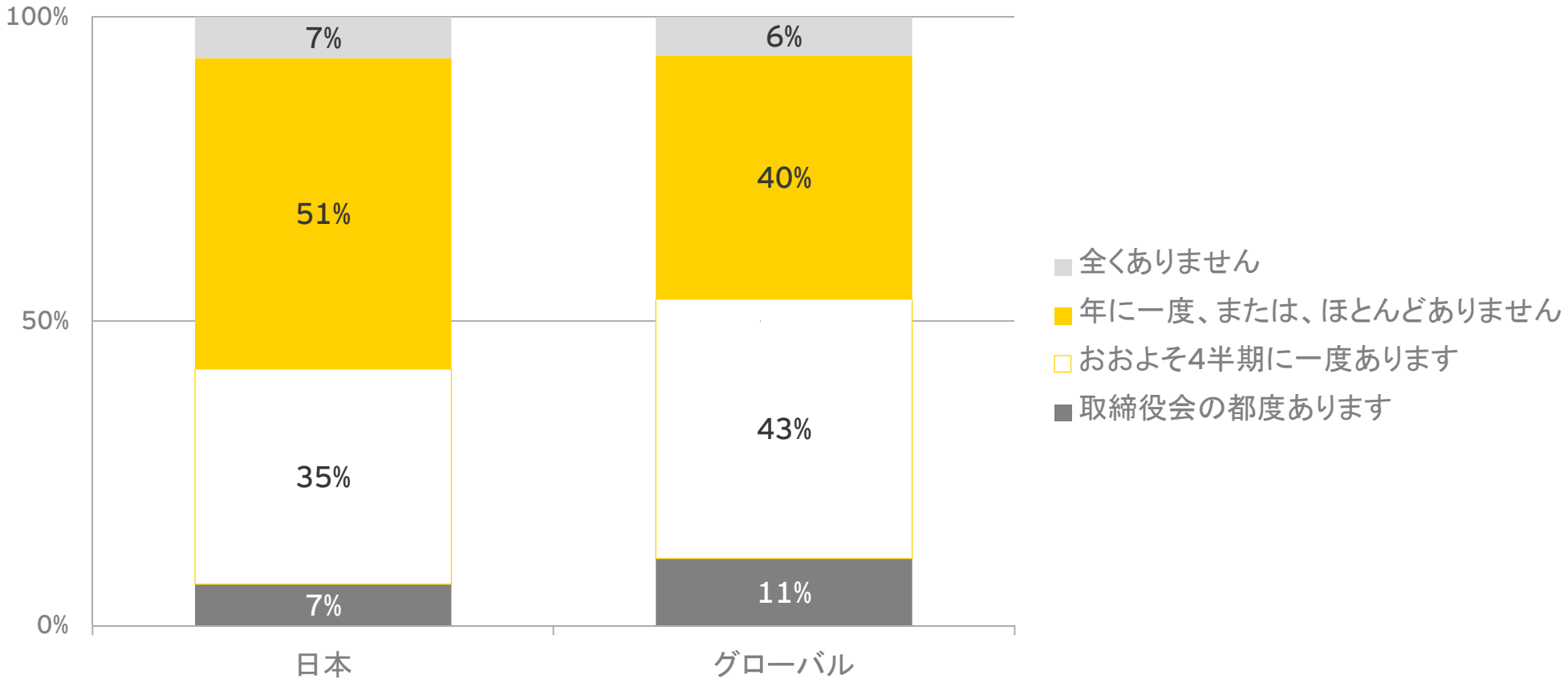
Q9.　貴社の情報セキュリティ戦略について、該当するものをすべて選択してください。



- 日本では、「企業の業務戦略と一致している、または組み込まれています」「現状のリスク環境と一致しています」「会社のリスク選好度やリスク許容度と一致しています」と回答した企業の割合が、少ない傾向にあります

2.3.取締役会での報告・検討状況

Q10. どのくらいの頻度で、情報セキュリティに関するトピックが貴社の取締役会（または経営トップの会議）で取り上げられますか？ 該当するものを1つ選択してください。

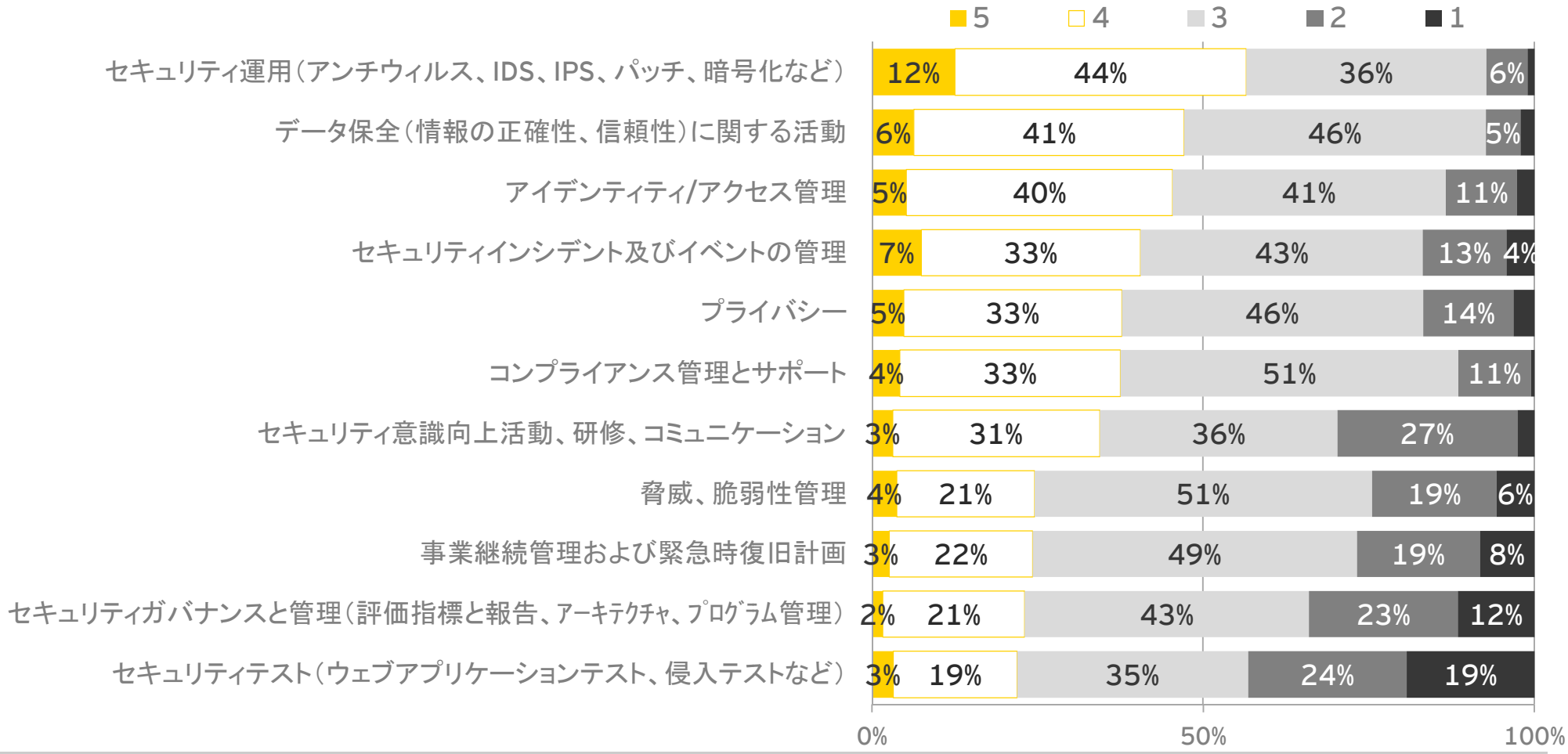


- 日本では、半数以上の企業が、情報セキュリティに関するトピックが取締役会で取り上げられることは「全くありません」「年に一度、または、ほとんどありません」と回答しています

日本

2.4.セキュリティ機能の成熟度自己評価

Q11. 下記セキュリティ機能の成熟度に関する自己評価として、5段階評価で該当するものを選択してください。
（1～5のうち1は存在しない、5は大変成熟している）

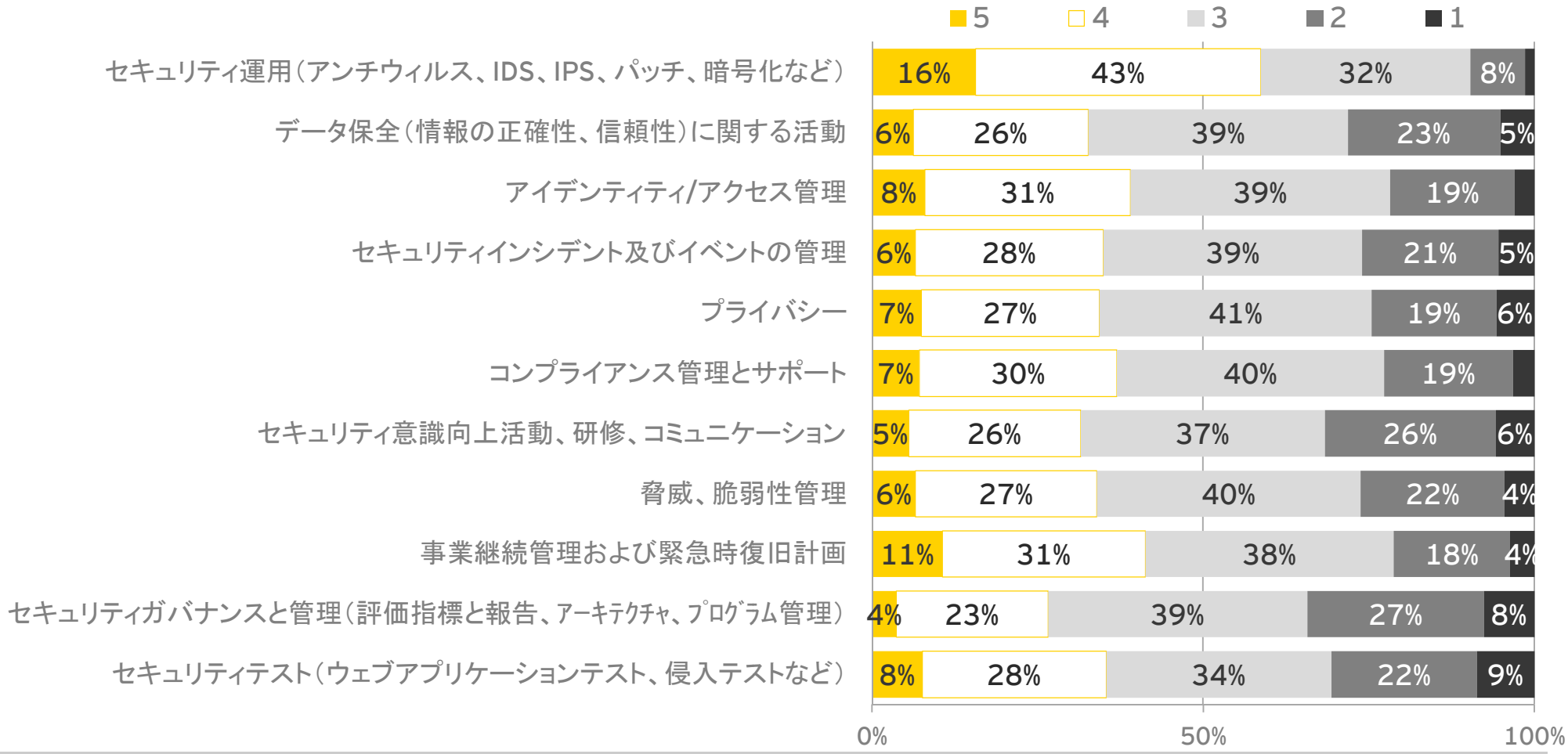


- 日本では、「セキュリティ運用」「データ保全」「アイデンティティ/アクセス権管理」分野において、セキュリティ機能の成熟度が高いと考えている傾向があります
- 一方「セキュリティテスト」「セキュリティ意識向上活動、研修、コミュニケーション」「セキュリティガバナンスと管理」分野においては、セキュリティ機能の成熟度が低いと考えている傾向があります

グローバル

2.4.セキュリティ機能の成熟度自己評価

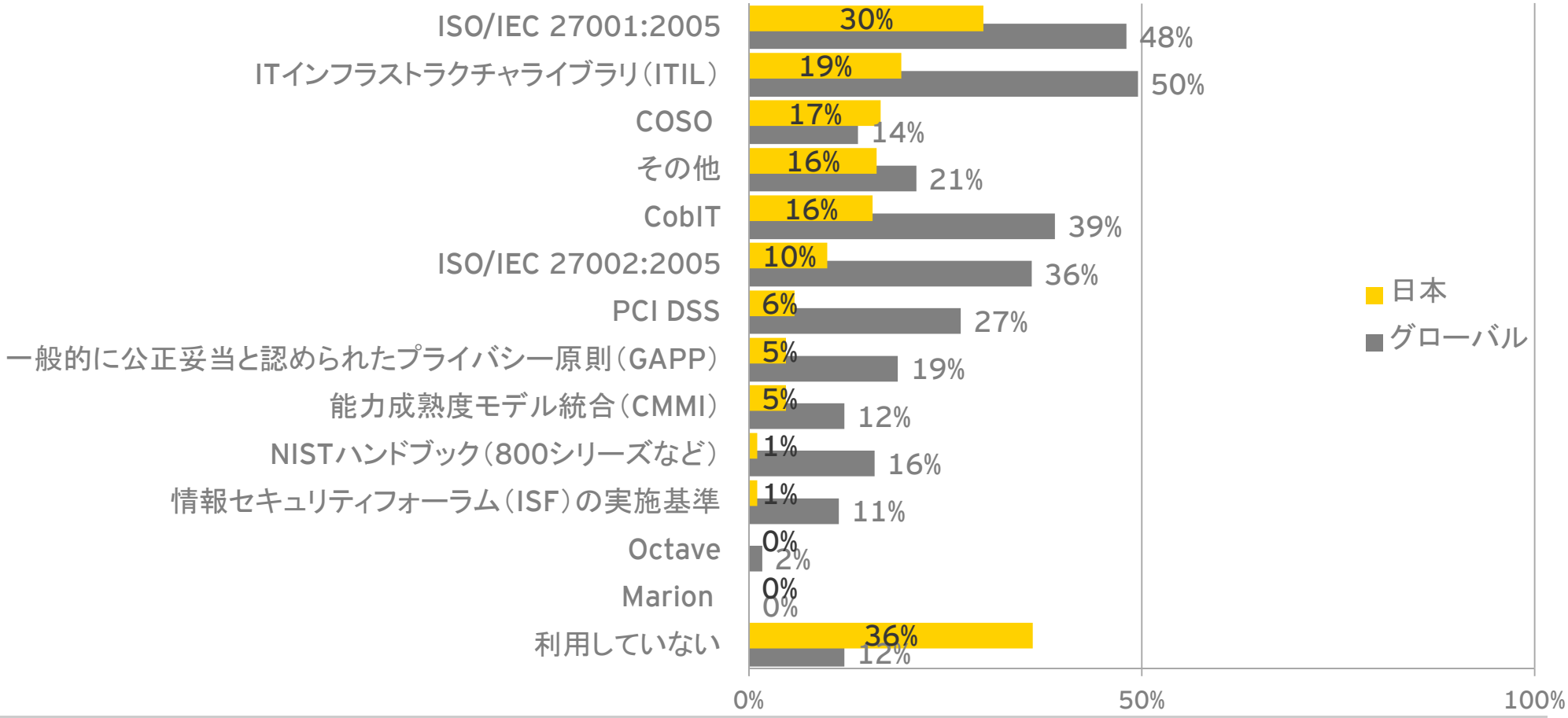
Q11. 下記セキュリティ機能の成熟度に関する自己評価として、5段階評価で該当するものを選択してください。
（1～5のうち1は存在しない、5は大変成熟している）



- グローバルでは、「セキュリティ運用」「事業継続管理および緊急時復旧計画」「アイデンティティ/アクセス権管理」分野において、セキュリティ機能の成熟度が高いと考えている傾向があります
- 一方で、日本と比較すると、成熟度が低いと考えているセキュリティ機能の割合が全体的に多い傾向があります

2.5.利用しているセキュリティ基準・フレームワーク

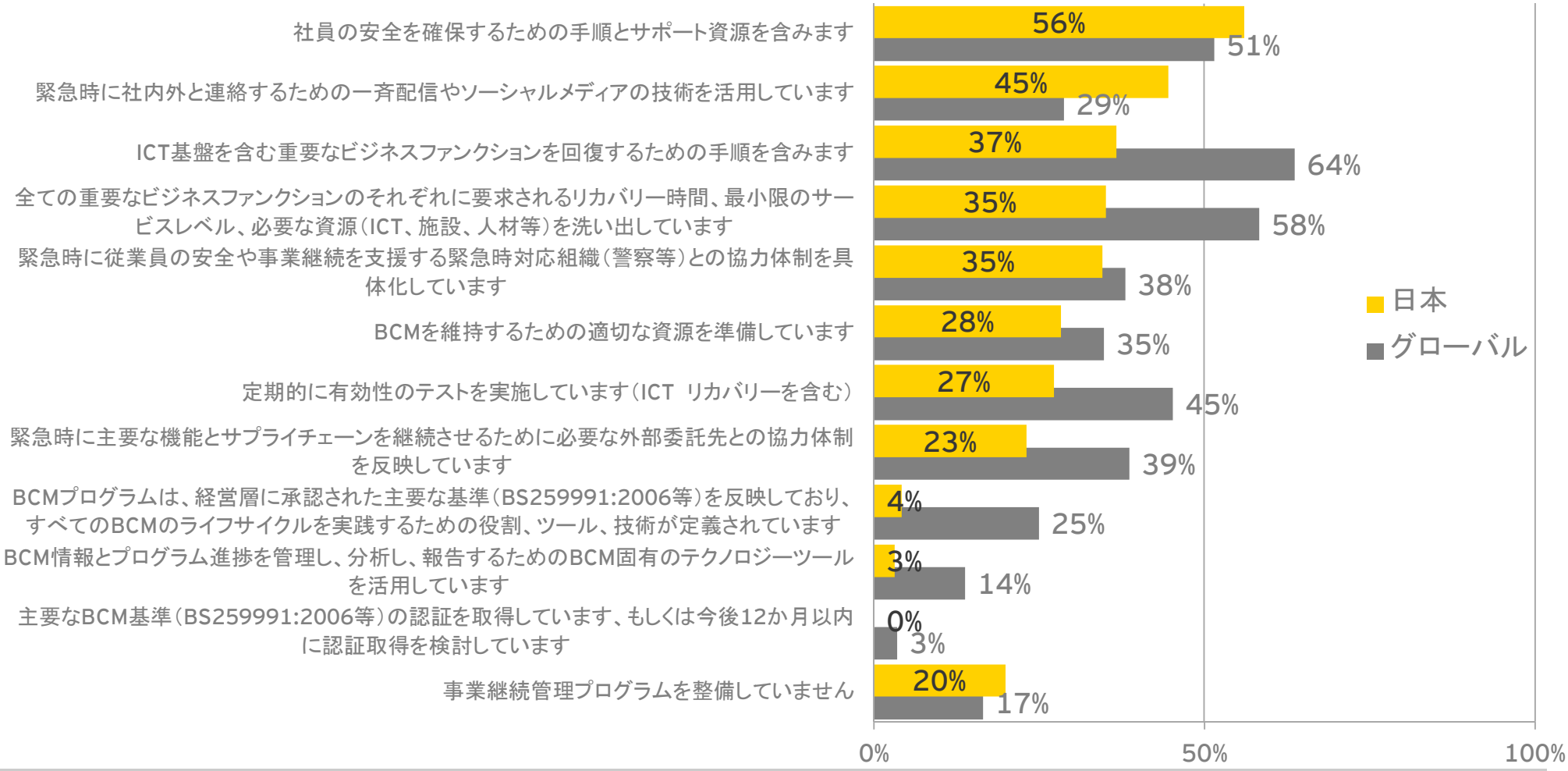
Q12.貴社で利用しているセキュリティ基準・フレームワークについて、該当するものをすべて選択してください。



- 日本では、国際標準化機構が発行している「ISO/IEC 27000」シリーズが最も利用されています
- 日本では、グローバルと比較すると、セキュリティ基準・フレームワークは全体的に利用されていない傾向があります

2.6.事業継続管理(BCM)プログラムの状況

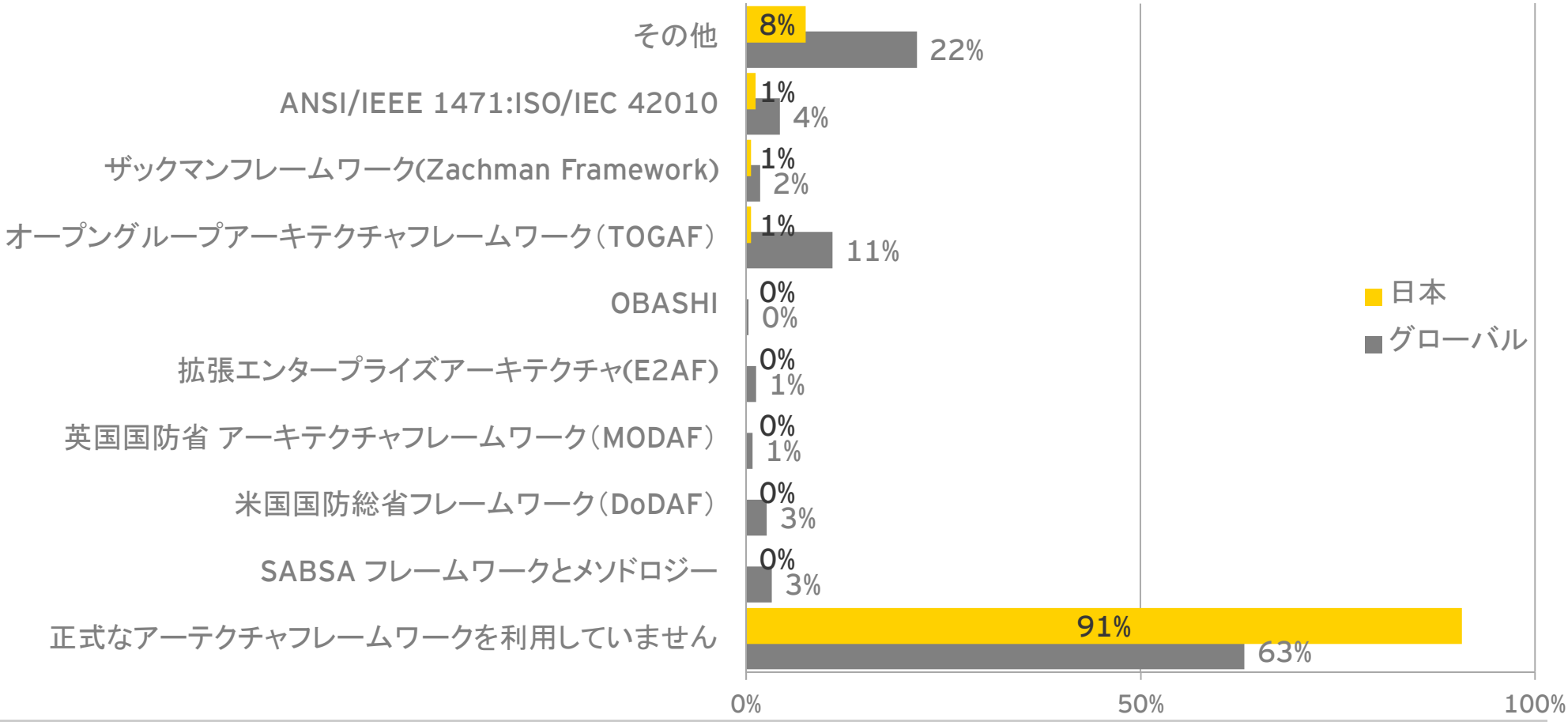
Q13. 貴社の事業継続管理(BCM)プログラムについて、該当するものをすべて選択してください。



- 日本では、安否確認を含む連絡体制が充実している傾向があります
- 一方で「全ての重要なビジネスファンクションのそれぞれに要求されるリカバリー時間、最小限のサービスレベル、必要な資源(ICT、施設、人材等)を洗い出しています」「 ICT基盤を含む重要なビジネスファンクションを回復するための手順を含みます」等の、重要な事業を継続するための活動が不足してる傾向があります

2.7.使用しているセキュリティアーキテクチャのフレームワーク

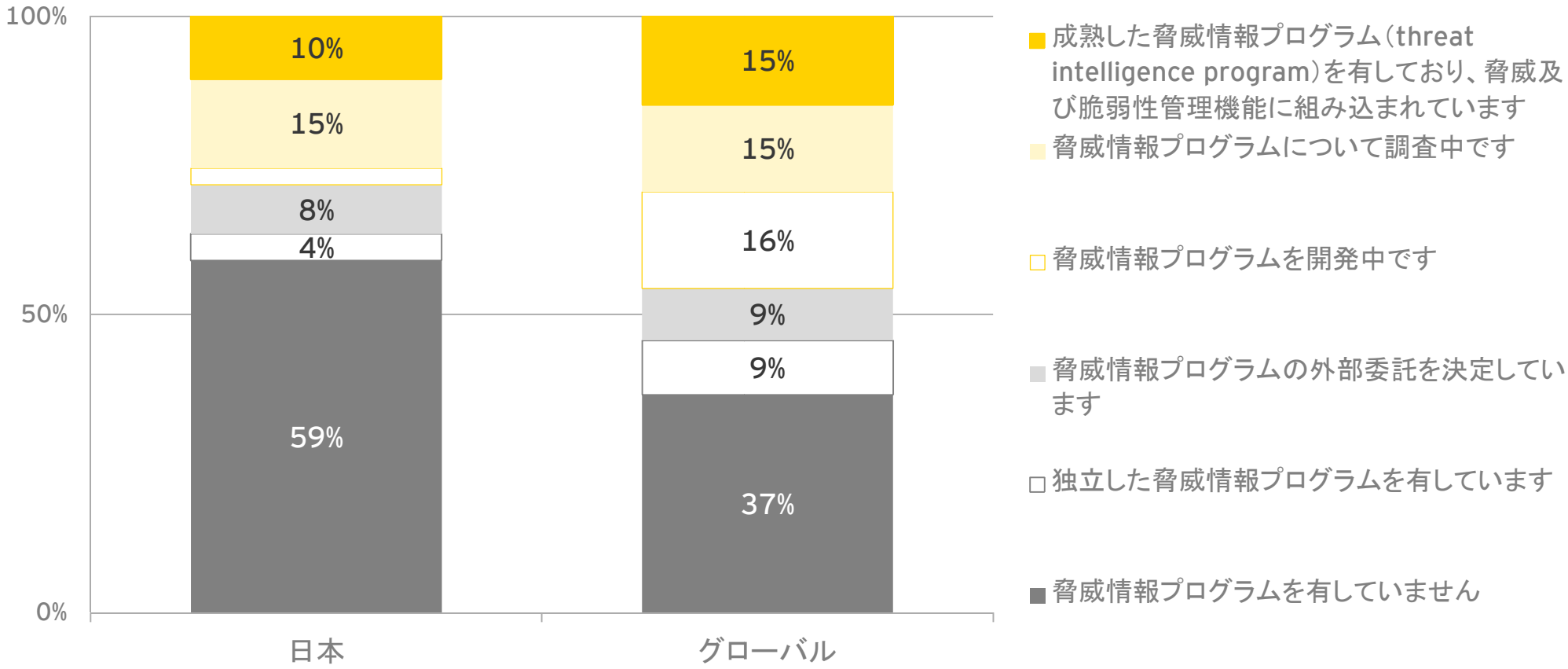
Q14. どの正式なセキュリティアーキテクチャのフレームワークが使われていますか？　該当するものをすべて選択してください。



- 日本では、情報セキュリティ管理の仕組みを構築するための正式なアーキテクチャフレームワークは、ほとんど利用されていません

2.8.脅威情報(threats intelligence)の状況

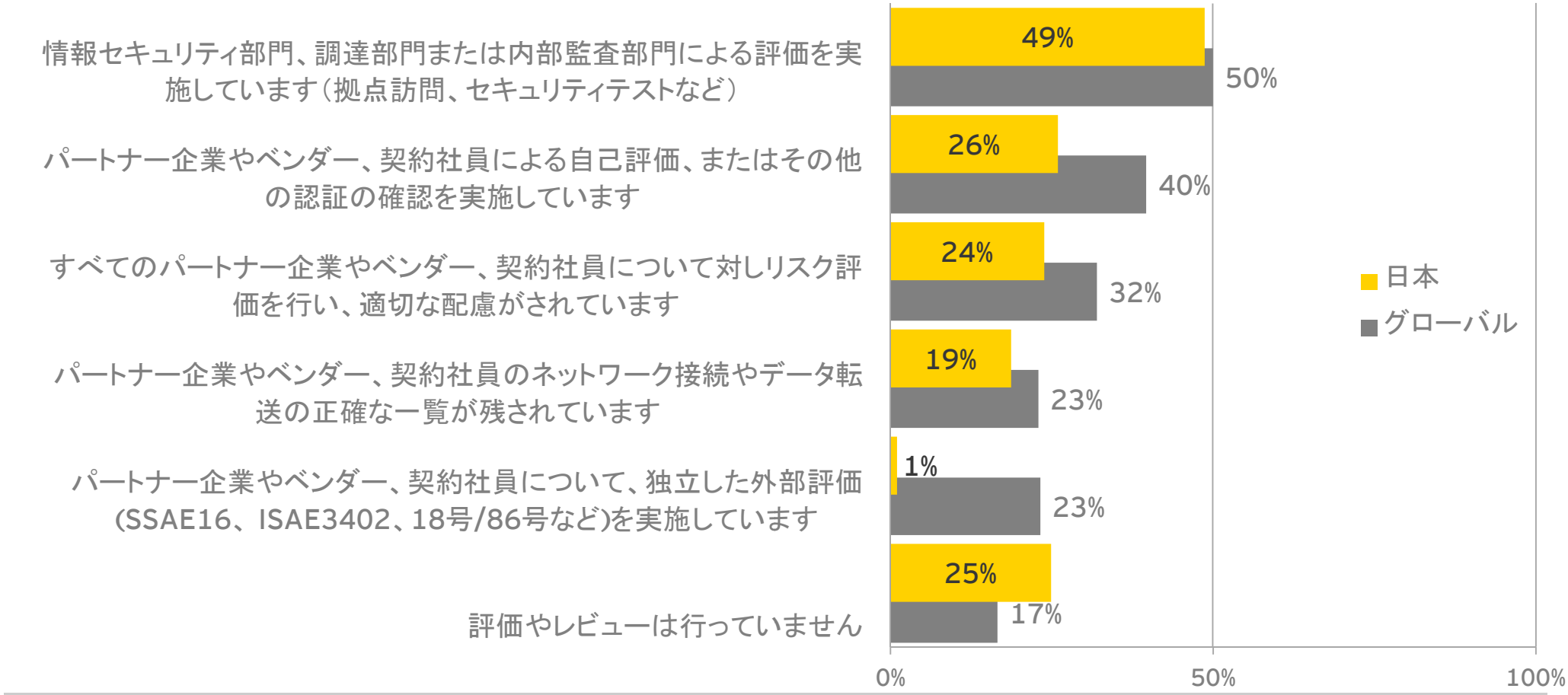
Q15. 脅威情報(threats intelligence)について、次のうち適切なものを1つ選択してください。



- 日本では、脅威情報を把握するためのプログラムへの取り組みが、グローバルより22ポイント低い41%にとどまります

2.9.パートナー企業、ベンダー、契約社員の情報セキュリティ管理

Q16. パートナー企業、ベンダー、契約社員が貴社の情報を適切に取り扱い、管理するために、どのような対策を実施していますか？ 該当するものをすべて選択してください。



- 日本では、パートナー企業等に対して独立した外部評価を実施している企業が約1%のみとなっており、グローバルの23%と比較すると、大きな差があります
- また、約25%の企業が、パートナー企業等に対して評価やレビューを行っていないと回答しています

調査結果

3.情報セキュリティの有効性

3.情報セキュリティの有効性

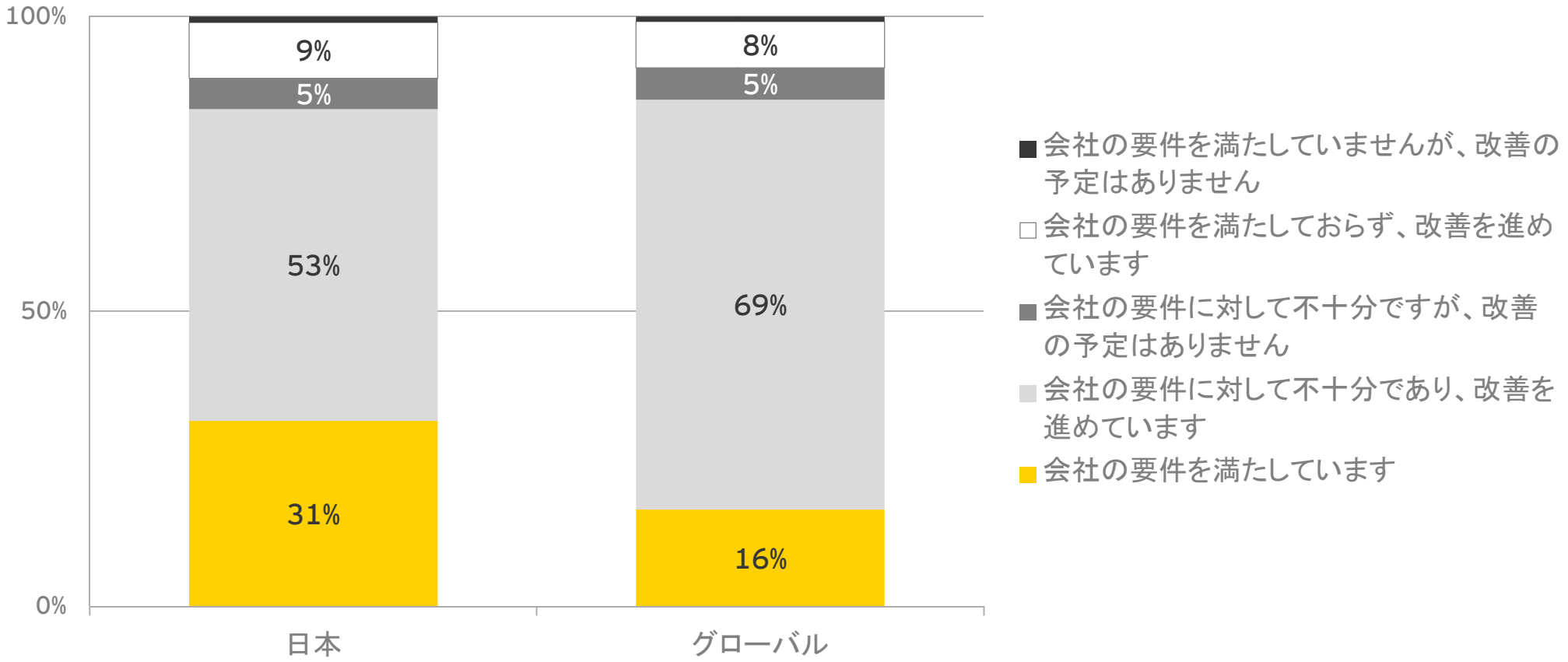
調査結果の概要と私たちの見解

日本では、内部組織に加えて外部機関を活用することで情報セキュリティの人材不足を補完することができます

- 日本では、情報セキュリティ部門が企業のニーズを満たしていると回答した企業は31%にとどまります
- 日本では、スキルを有する人材の不足が、情報セキュリティ運用に関する最大の課題として認識されています
- 日本では、「外部機関による評価」の活用がグローバルの3分の1程度である21%にとどまります

3.1.情報セキュリティ部門の状況

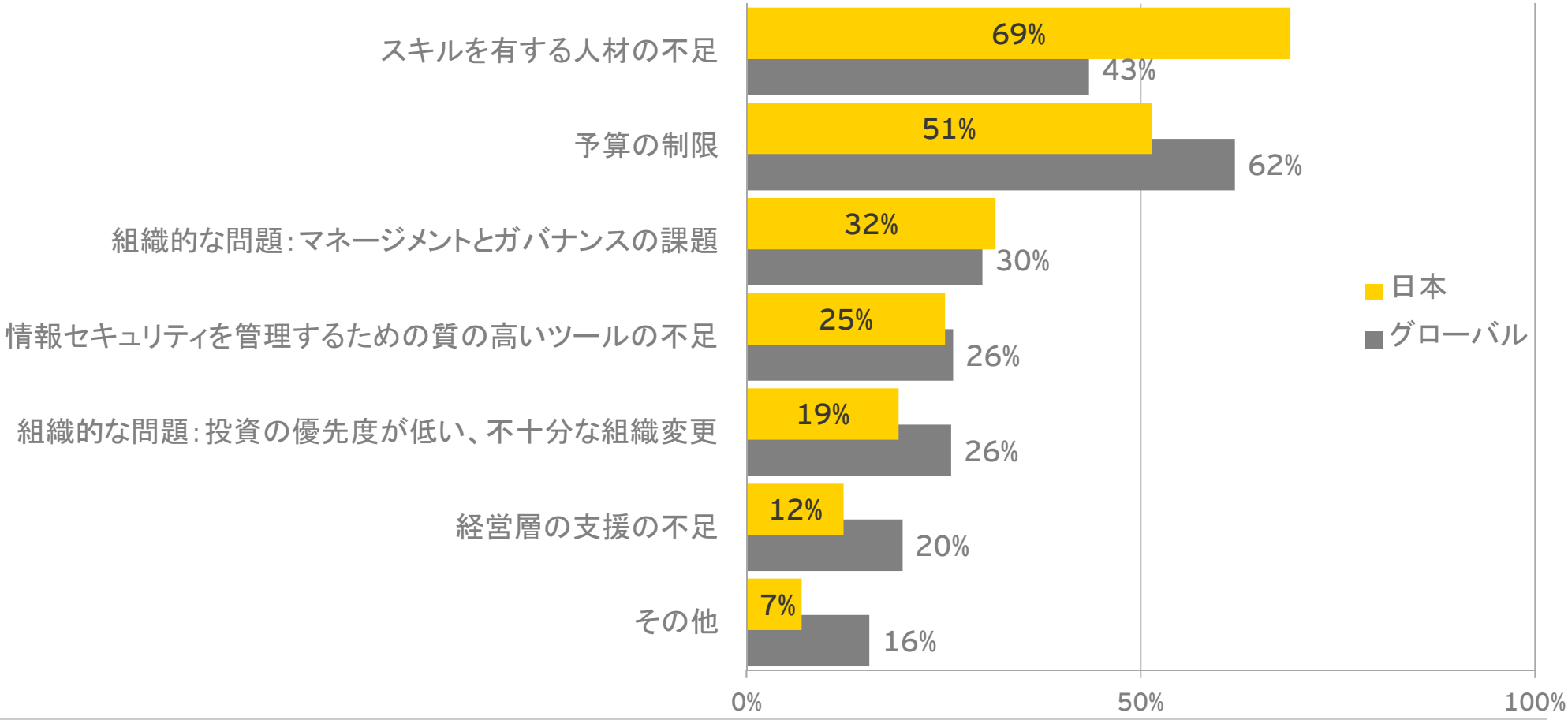
Q17. 情報セキュリティ部門は貴社のニーズを満たしていますか？



- 日本では、情報セキュリティ部門が企業のニーズを満たしていると回答した企業は31%にとどまります

3.2.情報セキュリティ課題の障害、原因

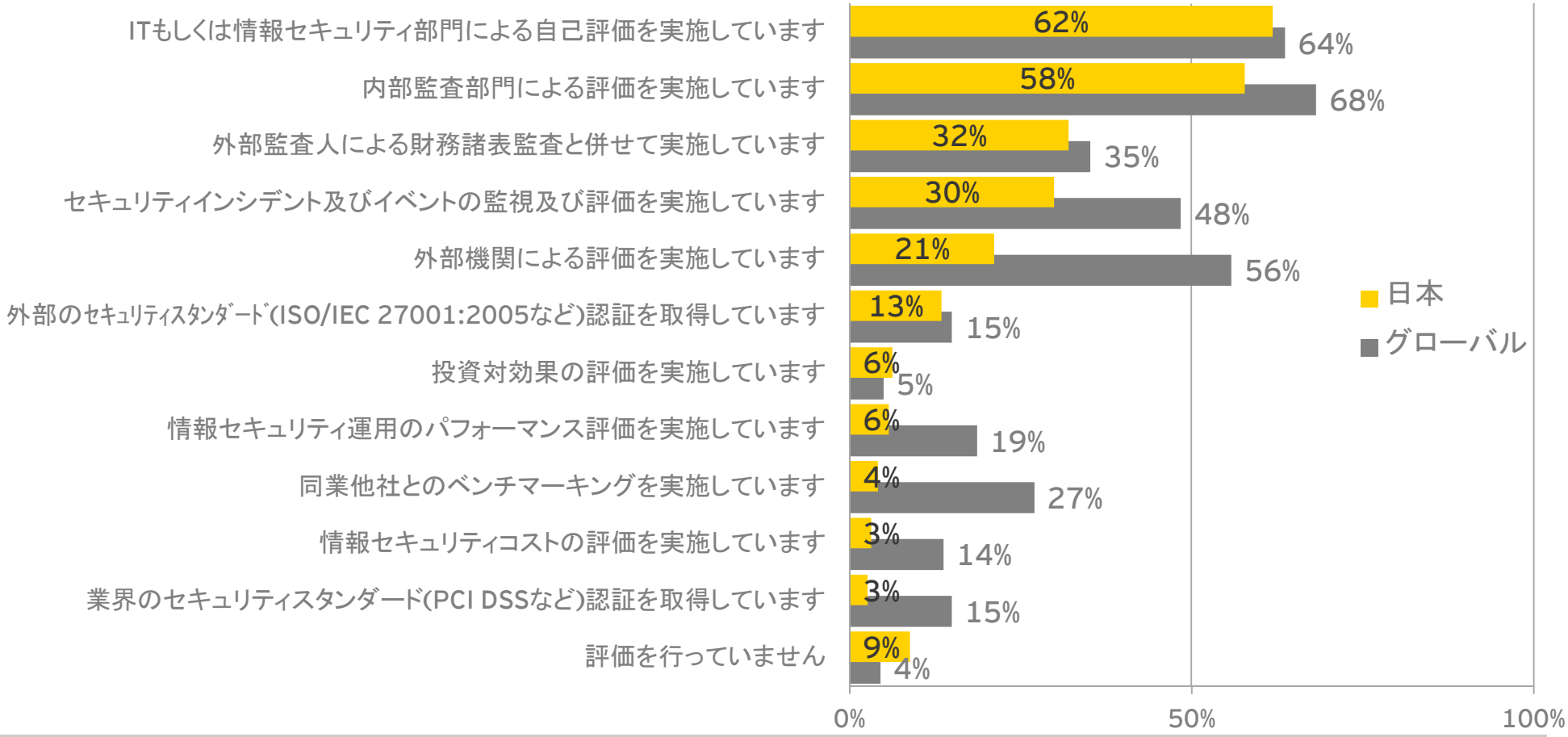
Q18. 貴社において、情報セキュリティ運用の貢献に関する課題及び組織の価値に関する障害、原因はなんですか?
該当するものをすべて選択してください。



- 日本では「スキルを有する人材の不足」「予算の制限」が、情報セキュリティ運用に関する課題として認識されている傾向があります

3.3.情報セキュリティ品質や有効性の評価方法

Q19. 貴社は情報セキュリティの品質や有効性をどのように評価していますか？ 該当するものをすべて選択してください。



- 日本では、「外部機関による評価」の活用がグローバルの3分の1程度である21%にとどまります

調査結果

4.脅威、リスク及びインシデント

4.脅威、リスク及びインシデント

調査結果の概要と私たちの見解

損失額を最大で2,000万円程度と評価している情報セキュリティリスクは、組織内部と外部の両方に存在します

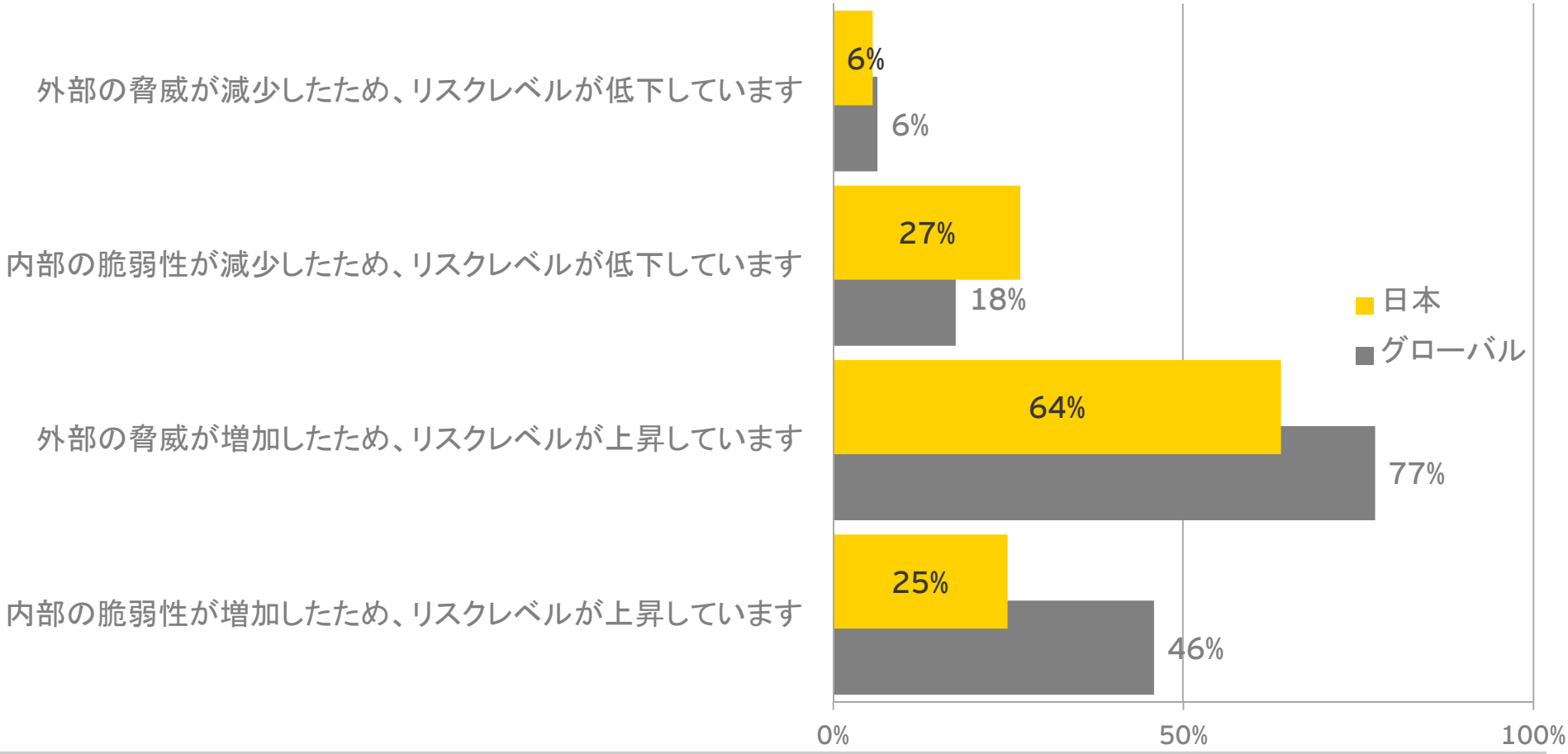
- 約9割の企業が、情報セキュリティリスクによる損失額を2,000万未満と想定、もしくは把握していません
- 日本では、リスクへの影響度を増加させた脅威及び脆弱性（T&V）として、「財務情報の窃盗を目的とするサイバー攻撃」「不注意な従業員」などが認識されています
- セキュリティインシデント件数は変化がありません

日本では、情報セキュリティ関連リスクの把握と対応をより充実させることが期待されます

- 日本では、内部の脆弱性によるリスクへの認識が、グローバルの2分の1程度である25%にとどまります
- 日本では、外部からの攻撃によって脅威が増加したと回答した企業が、グローバルより19ポイント低い21%にとどまります
- 日本では、脆弱性テスト（攻撃、侵入）を実施していない、または把握していないと回答した企業の割合が、グローバルより38ポイント高い62%となっています
- 日本では、発生したセキュリティインシデント件数が「年間5件未満」と回答した企業が、グローバルより14ポイント低い48%となっています。その理由の一つとして、把握できていないセキュリティインシデントが存在する可能性があります

4.1.リスク環境の変化

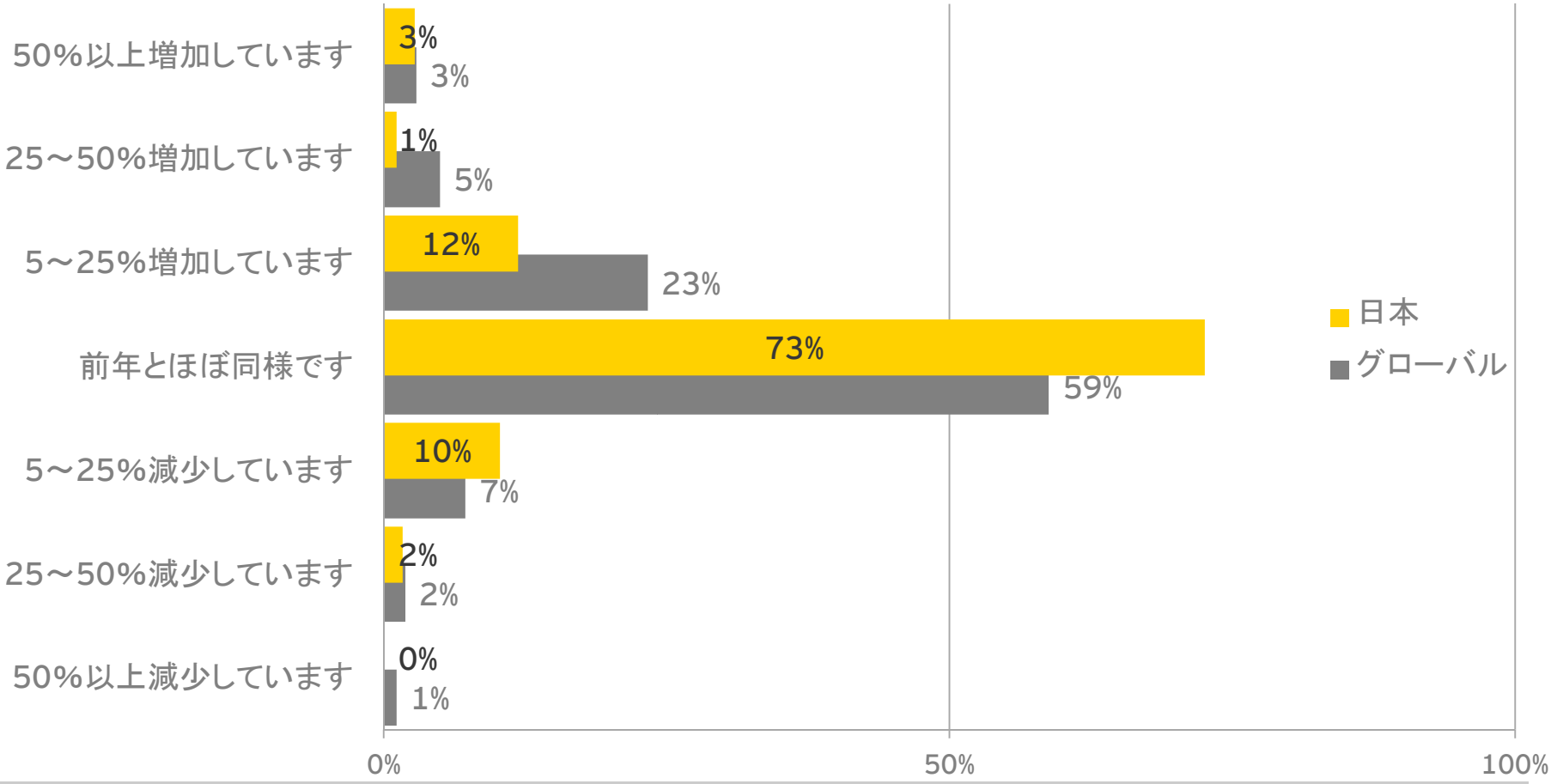
Q20. 過去12か月間に起こったリスク環境の変化について、貴社に該当するものをすべて選択してください。



- 日本では「内部の脆弱性が増加したため、リスクレベルが上昇した」と回答した企業が、グローバルの46%の2分の1程度である25%にとどまります
- 多くの企業が、外部の脅威が増加したため、リスクレベルが上昇したと考えています

4.2.セキュリティインシデント件数の変化

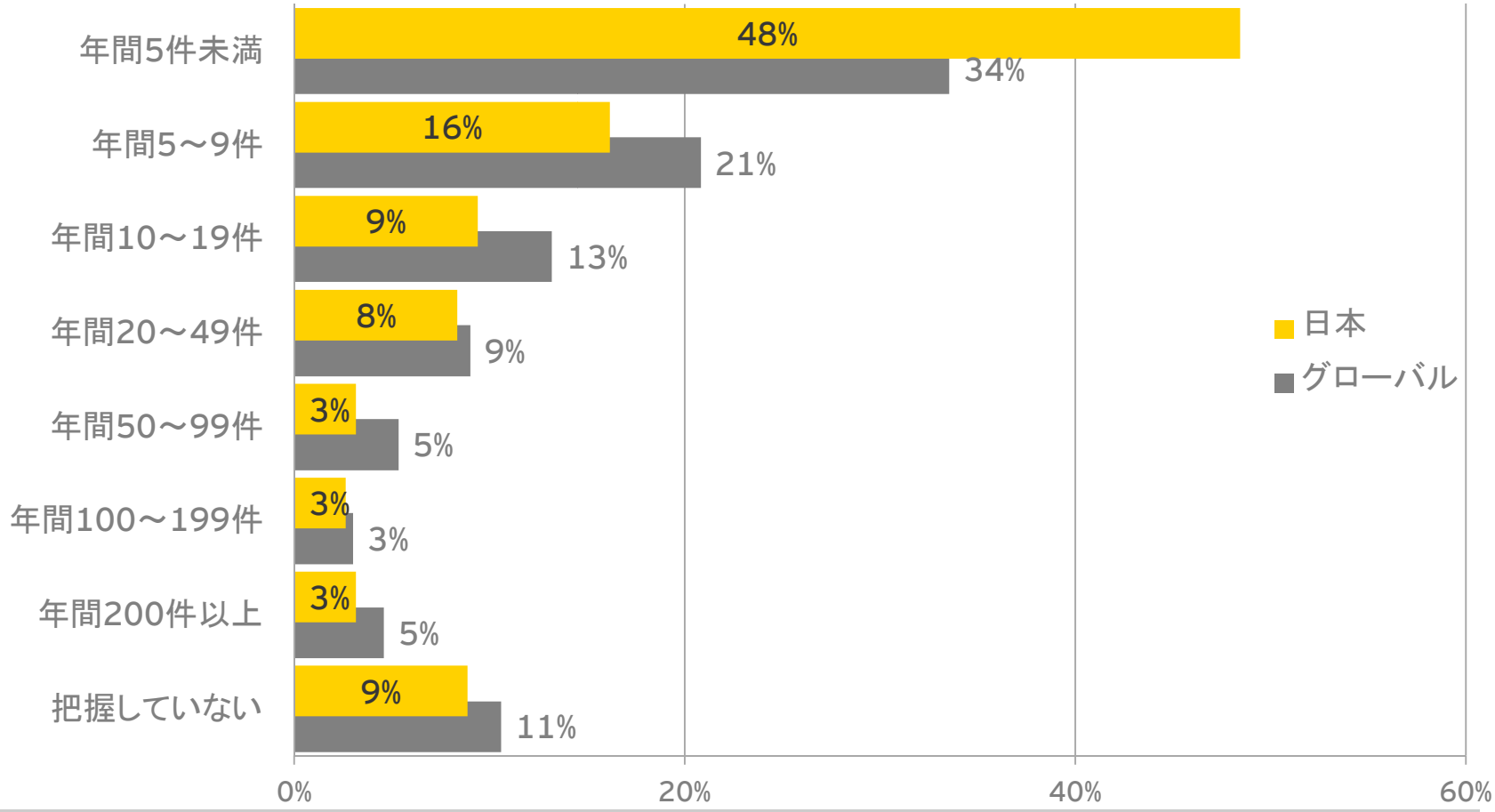
Q21. 前年度と比較したセキュリティインシデント件数の変化について、貴社に該当するものを1つ選択してください。



- 日本では、多くの企業がセキュリティインシデント件数は前年度とほぼ同様と回答しています
- 一方で、グローバルでは、セキュリティインシデント件数が前年度より増えたと回答した企業の割合が多くなっています

4.3.発生したセキュリティインシデント件数

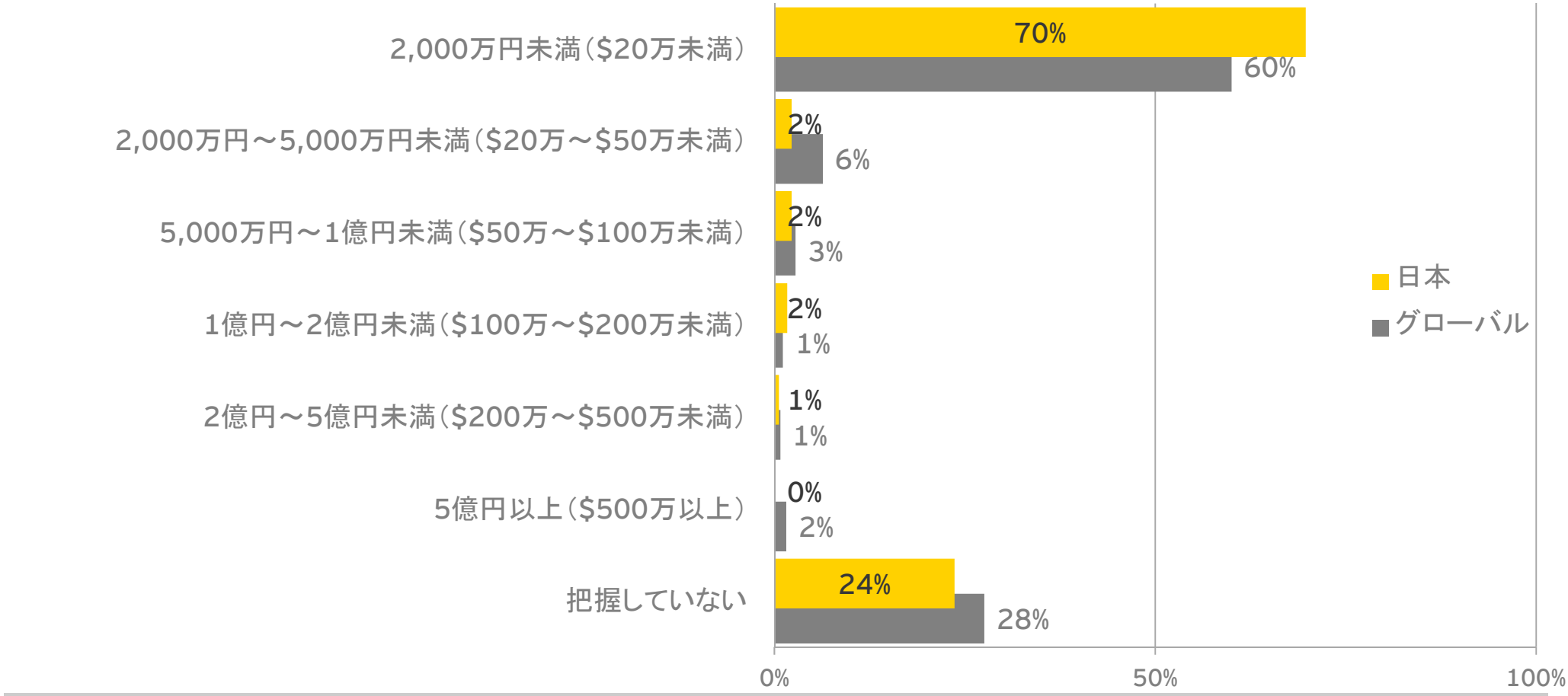
Q22. 前年度に発生した情報セキュリティインシデント件数（合計）について、貴社に該当するものを1つ選択してください。



- 日本では、発生したセキュリティインシデント件数が「年間5件未満」と回答した企業が、グローバルより14ポイント高い48%となっています
- 理由の一つとして、把握できていないセキュリティインシデントが存在する可能性があります

4.4.セキュリティインシデントに関する損失額

Q23. 前年度に発生した情報セキュリティインシデントに関する損失額について、貴社に該当するものを1つ選択してください。
（損失額には、対応コスト、生産性の低下、法規制上の罰金、損害賠償、様々な責任（クレジットカードの交換コスト、民事上の罰金等）を含む。ただし、ブランドイメージの低下による費用もしくは収入の損失は含まない）



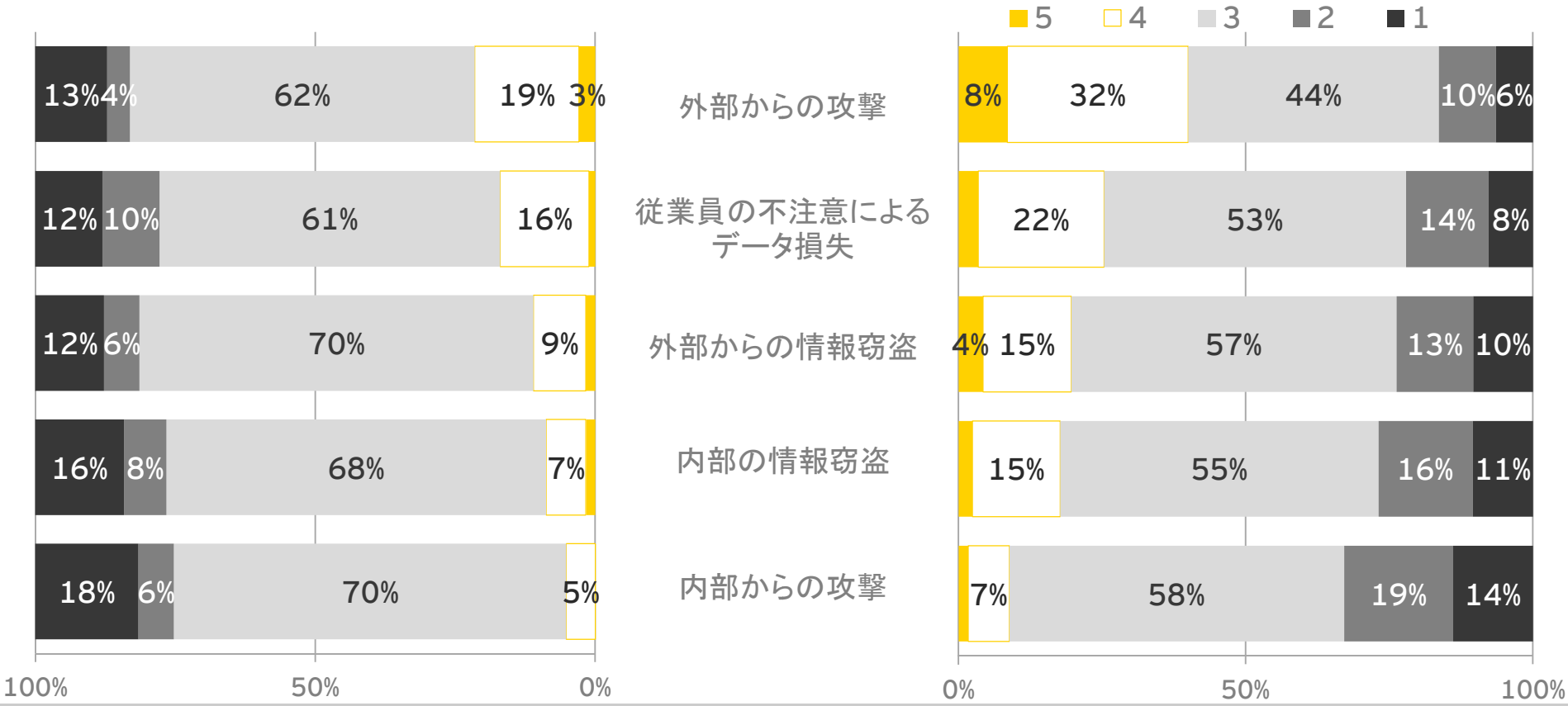
- 日本では、約90%以上の企業が、情報セキュリティリスクによる損失額を「2,000万未満」もしくは「把握していない」と回答しています
- グローバルでは、約0.1%の企業が、情報セキュリティインシデントに関する損失額が1,000億円以上（$10億以上）と回答しています

4.5.セキュリティインシデントの脅威の変化

Q24. 貴社で実際に発生したインシデントについて、以下の脅威はどの程度変化したか、その変化度について、5段階評価で1～5から該当するものを1つ選択してください。（1:非常に減少、5:非常に増加）

日本

グローバル

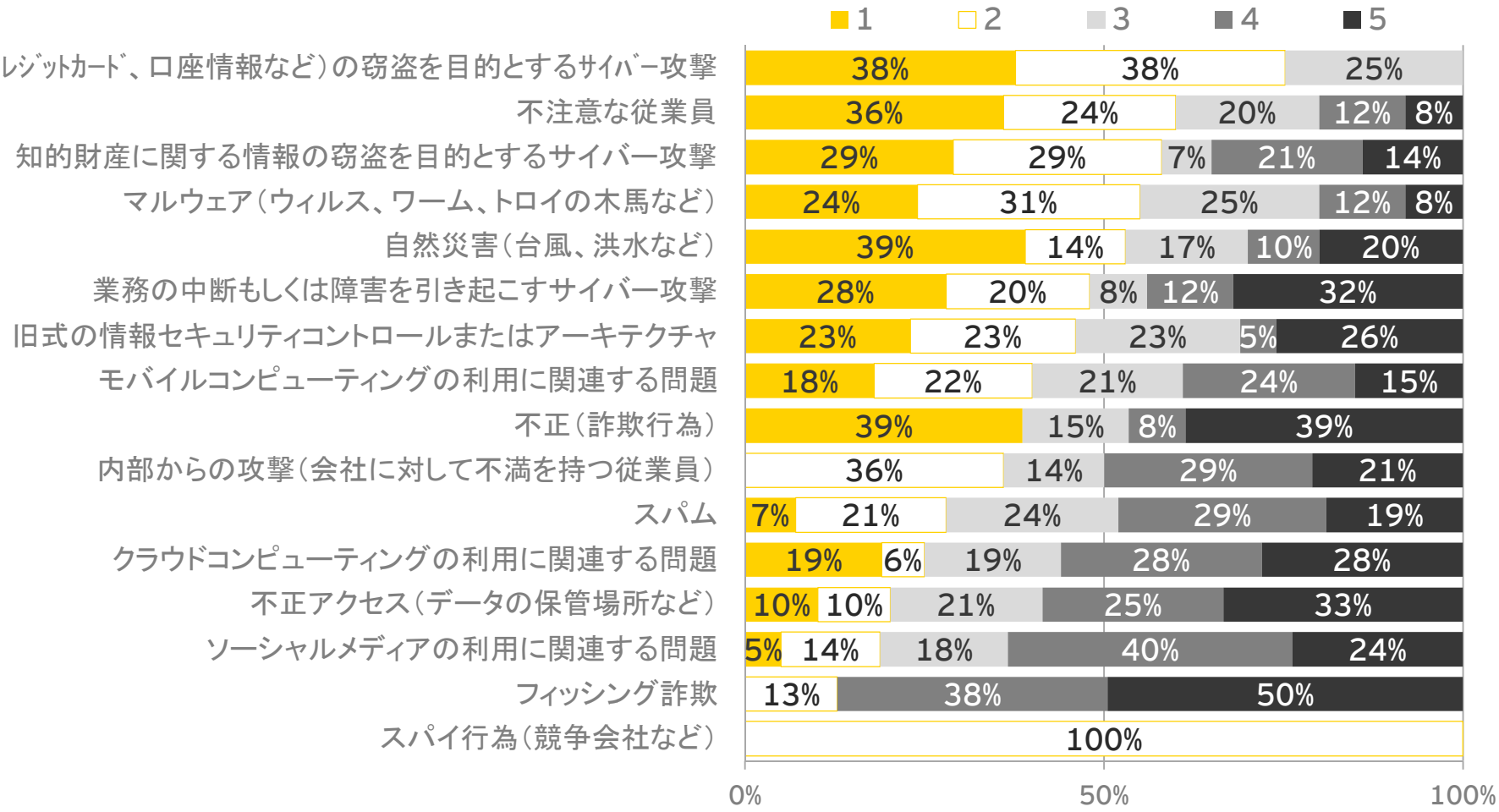


- 日本では、外部からの攻撃によって脅威が増加したと回答した企業が、グローバルより18ポイント低い22%にとどまります

日本

4.6.リスクへの影響度を増加させた脅威および脆弱性

Q25. 過去12か月間に、貴社のリスクへの影響度を最も増加させた脅威および脆弱性（T&V）について、下記より5つ選択し、影響度が高いものから順に1、2、3、4、5と番号を記入してください。

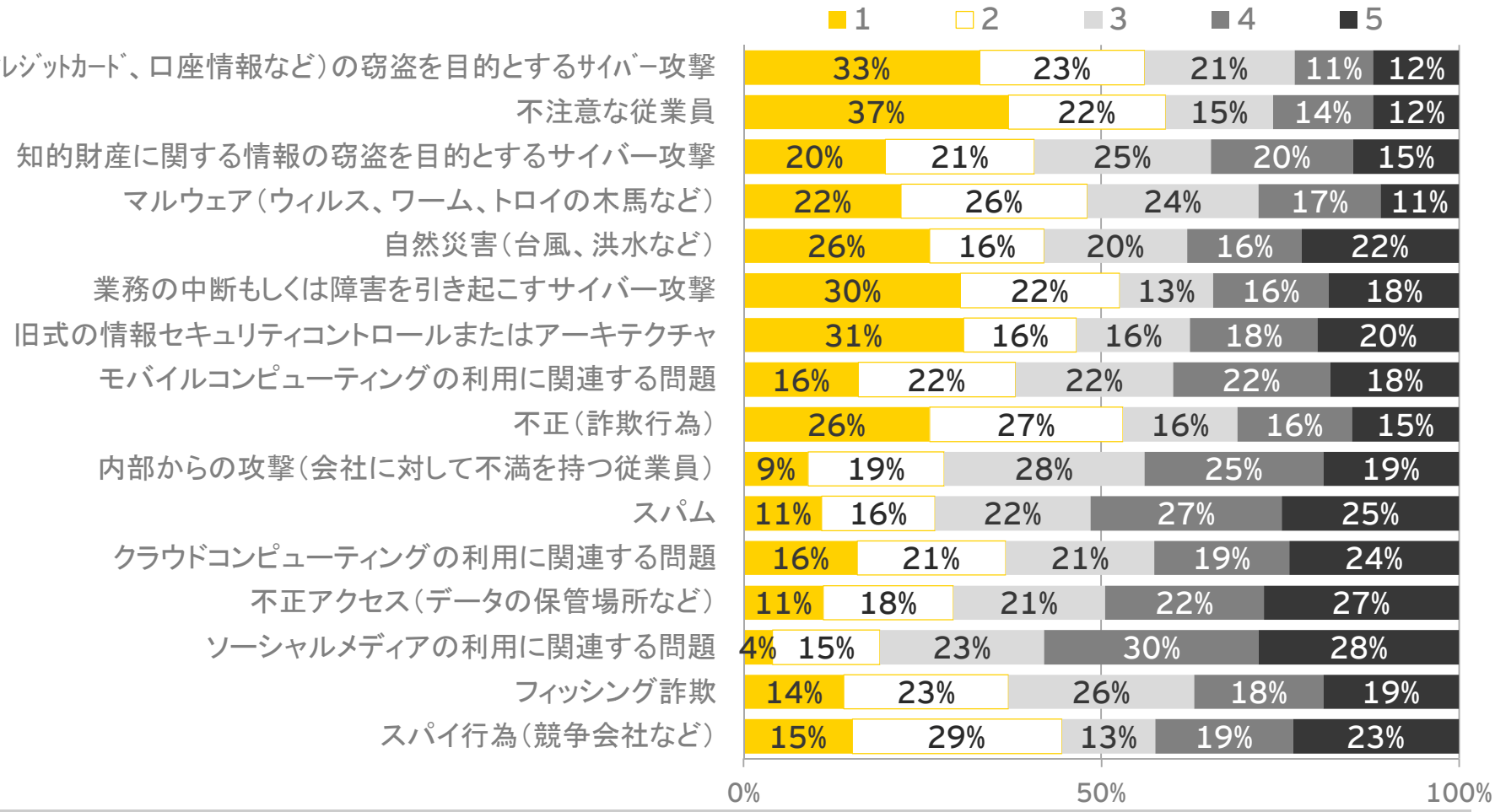


- 日本では、リスクへの影響度を増加させた脅威及び脆弱性（T&V）として、「財務情報の窃盗を目的とするサイバー攻撃」「不注意な従業員」「知的財産に関する情報の窃盗を目的とするサイバー攻撃」の影響度が高い傾向にあります

グローバル

4.6.リスクへの影響度を増加させた脅威および脆弱性

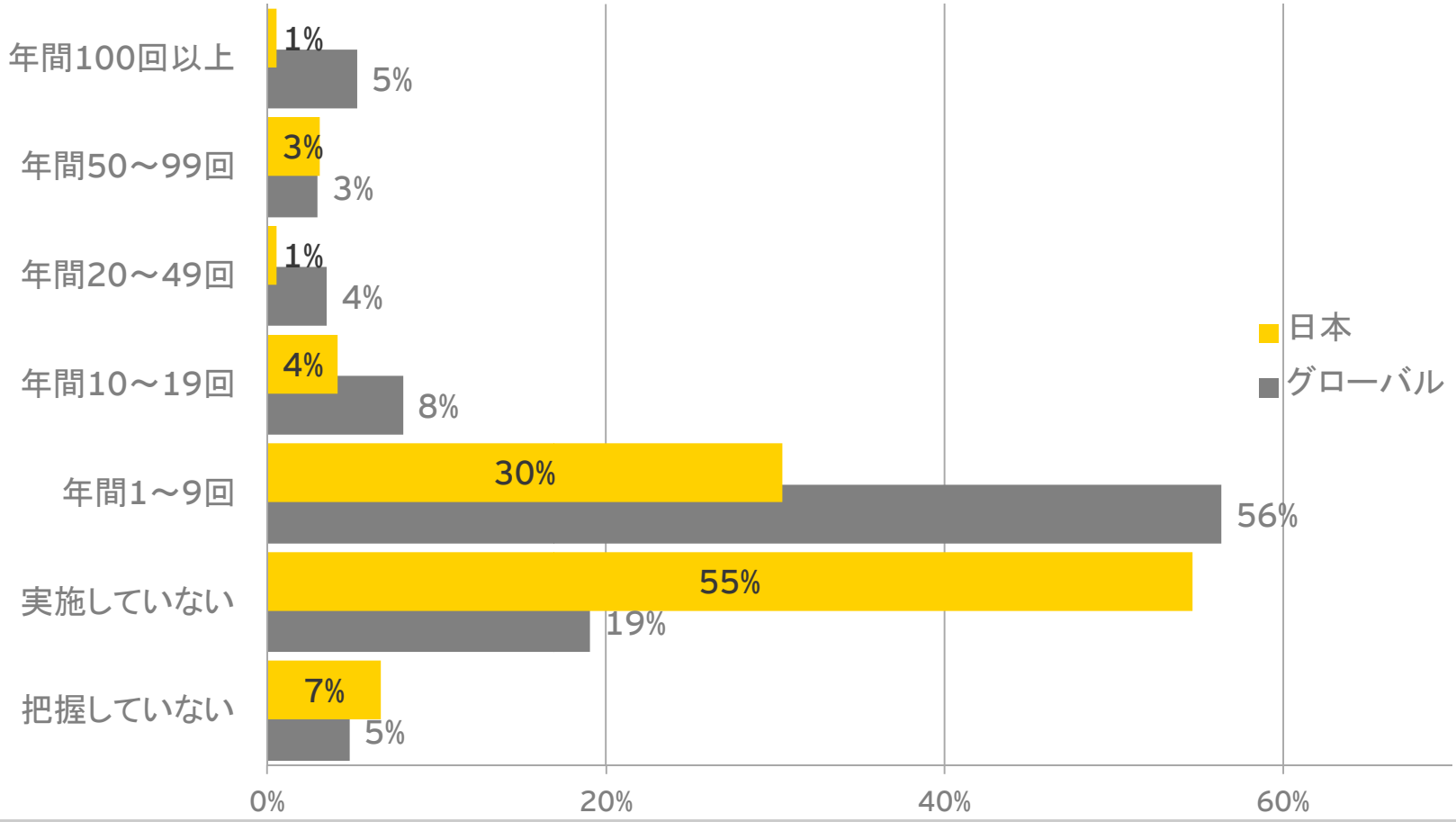
Q25. 過去12か月間に、貴社のリスクへの影響度を最も増加させた脅威および脆弱性(T&V)について、下記より5つ選択し、影響度が高いものから順に1、2、3、4、5と番号を記入してください。



- グローバルでは、リスクへの影響度を増加させた脅威及び脆弱性(T&V)として、「不注意な従業員」「財務情報の窃盗を目的とするサイバー攻撃」「不正(詐欺行為)」の影響度が高い傾向にあります

4.7.脆弱性テスト(攻撃、侵入)の実施状況

Q26. 年次での脆弱性テスト(攻撃、侵入)の実施について、貴社に該当するものを1つ選択してください。



- 日本では、脆弱性テスト(攻撃、侵入)を実施していない、または把握していないと回答した企業の割合が、グローバルより38ポイント高い62%となっています

調査結果

5.モバイルコンピューティング

5.モバイルコンピューティング

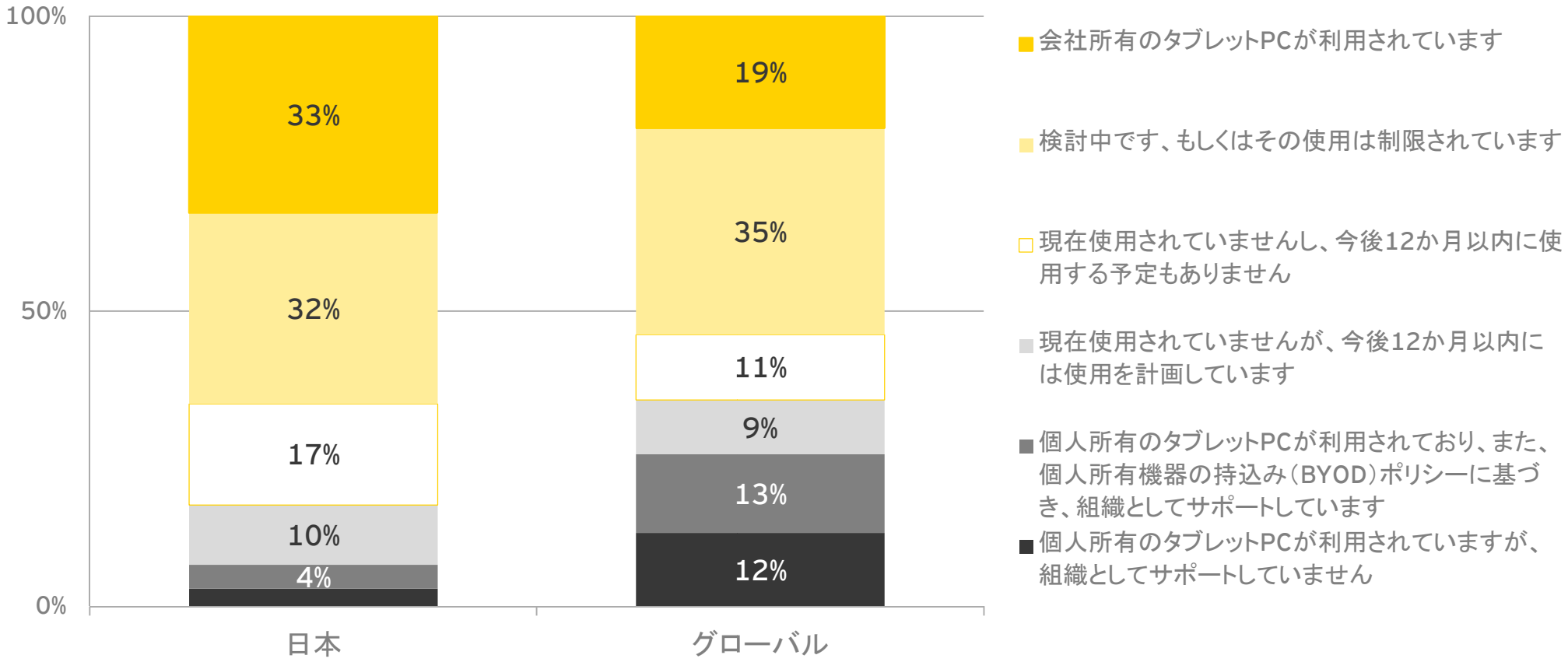
調査結果の概要と私たちの見解

急速に進んでいるモバイルコンピュータの活用に、セキュリティ対策が追い付いていない状況です

- 日本・グローバルともに、多くの企業が業務目的でのタブレットコンピュータ（タブレットPC）を使用している、または利用することを計画していると回答しています
- 日本では、「セキュリティ意識向上活動の強化」に注力している一方で、意識向上に必要な要素である「ポリシの一改訂」はグローバルより17ポイント低い35%にとどまります

5.1.タブレットコンピュータの使用状況

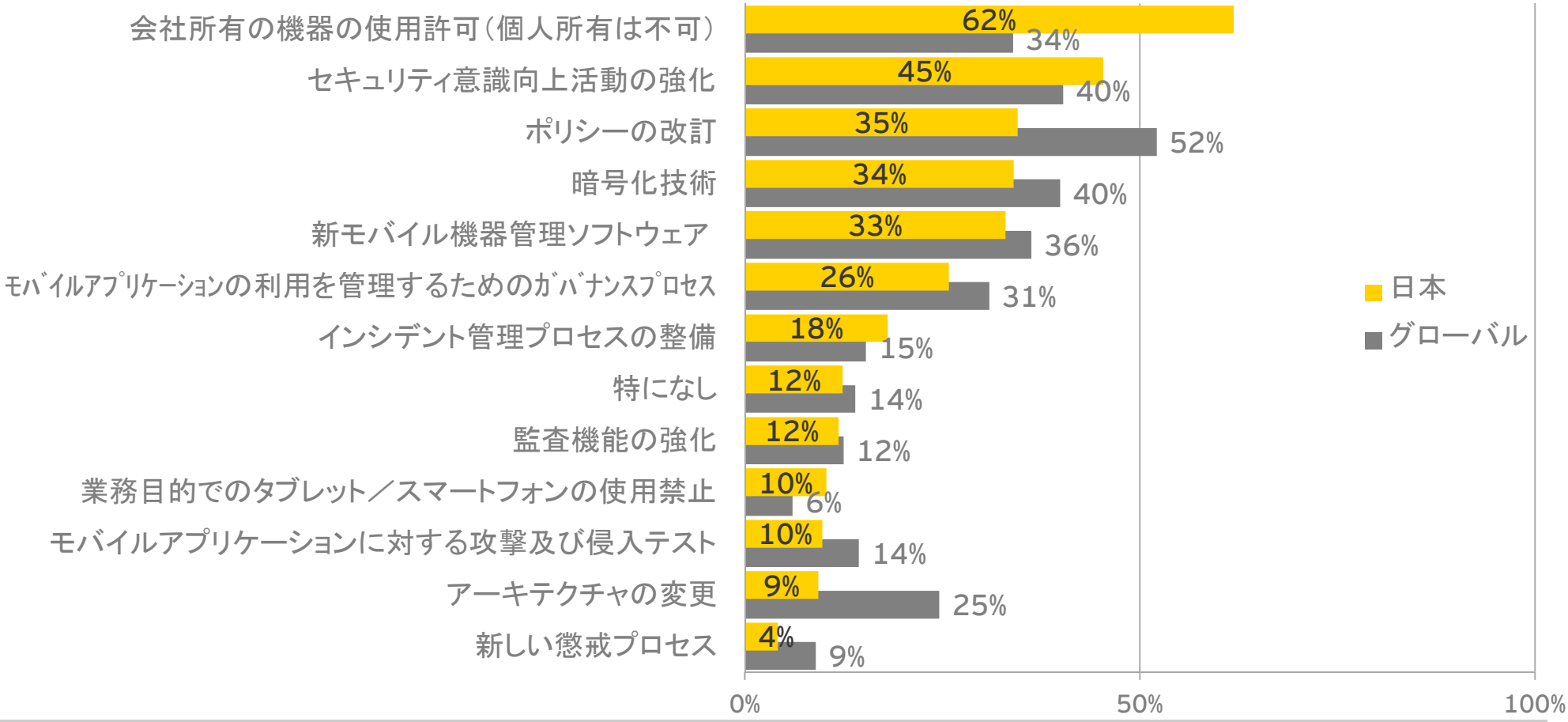
Q27. 現在、貴社では業務目的でのタブレットコンピュータ（タブレットPC）の使用を許可していますか？該当するものを1つ選択してください。



- 日本・グローバルともに、多くの企業が業務目的でのタブレットコンピュータ（タブレットPC）を使用している、または利用することを計画していると回答しています

5.2.モバイルコンピューティングに関するコントロール

Q28. モバイルコンピューティング（タブレットPCやスマートフォンを含む）を利用する際、「新たな」または「増加する」リスクを低減するために実施しているコントロールについて、該当するものをすべて選択してください。



- 日本では、「セキュリティ意識向上活動の強化」に注力している一方で、意識向上に必要な要素である「ポリシの一改訂」はグローバルより17ポイント低い35%にとどまります

調査結果

6.クラウドコンピューティング

6.クラウドコンピューティング

調査結果の概要と私たちの見解

クラウドサービスは、既に多くの企業で利用されています

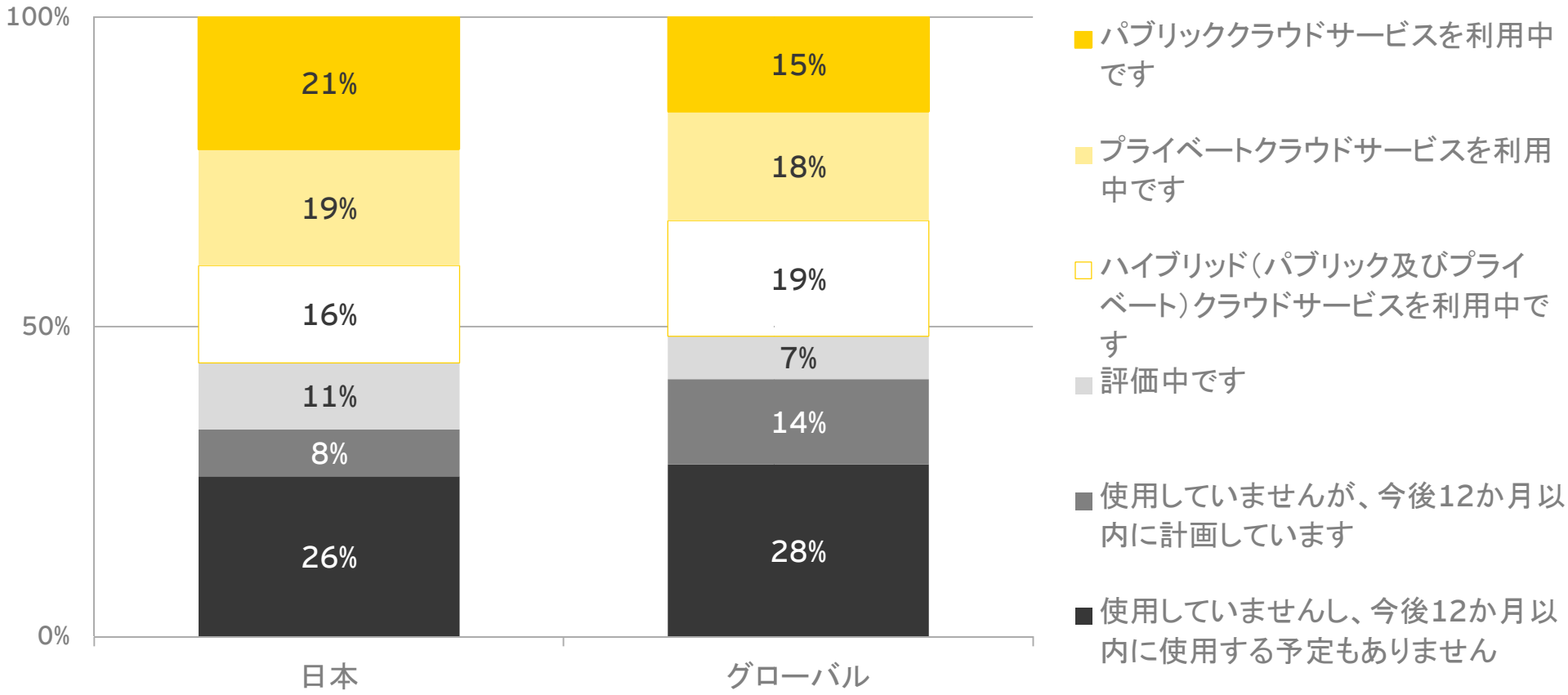
- 日本・グローバルともに、70%以上の企業が、クラウドサービスを利用している、または評価・計画中と回答しています
- 日本・グローバルともに、SaaS型クラウドサービスの利用を中心として、IaaS型、PaaS型を組み合わせてクラウドサービスを利用、または計画している傾向があります

クラウドサービスに関連するリスクに対応したコントロールは、まだ十分に実施されていません

- 外部認証や証明書を取得することで、クラウドを提供するプロバイダの信頼が高まります
- グローバルでは、約30%の企業が、クラウドを利用した自社データの所在（国または地域）を認識していません
- 日本では、約49%の企業が、クラウドコンピューティングに関するリスクを低減するためのコントロールを実施していないと回答しています

6.1.クラウドサービスの利用状況

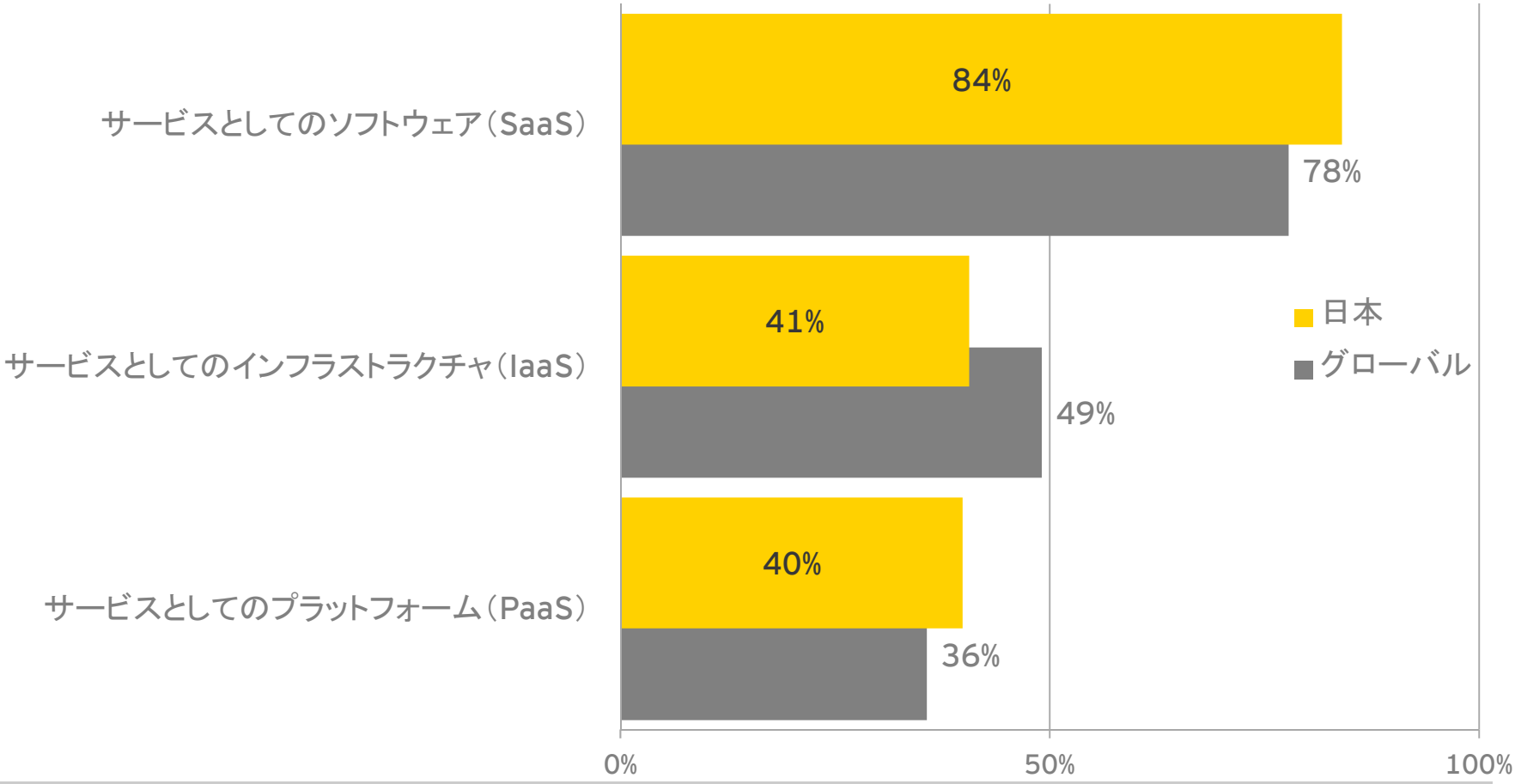
Q29. 現在クラウドコンピューティングベースのサービスを使用していますか?該当するものを1つ選択してください。



- 日本・グローバルともに、70%以上の企業が、クラウドサービスを利用している、または評価・計画中と回答しています

6.2.利用しているクラウドサービスの種類

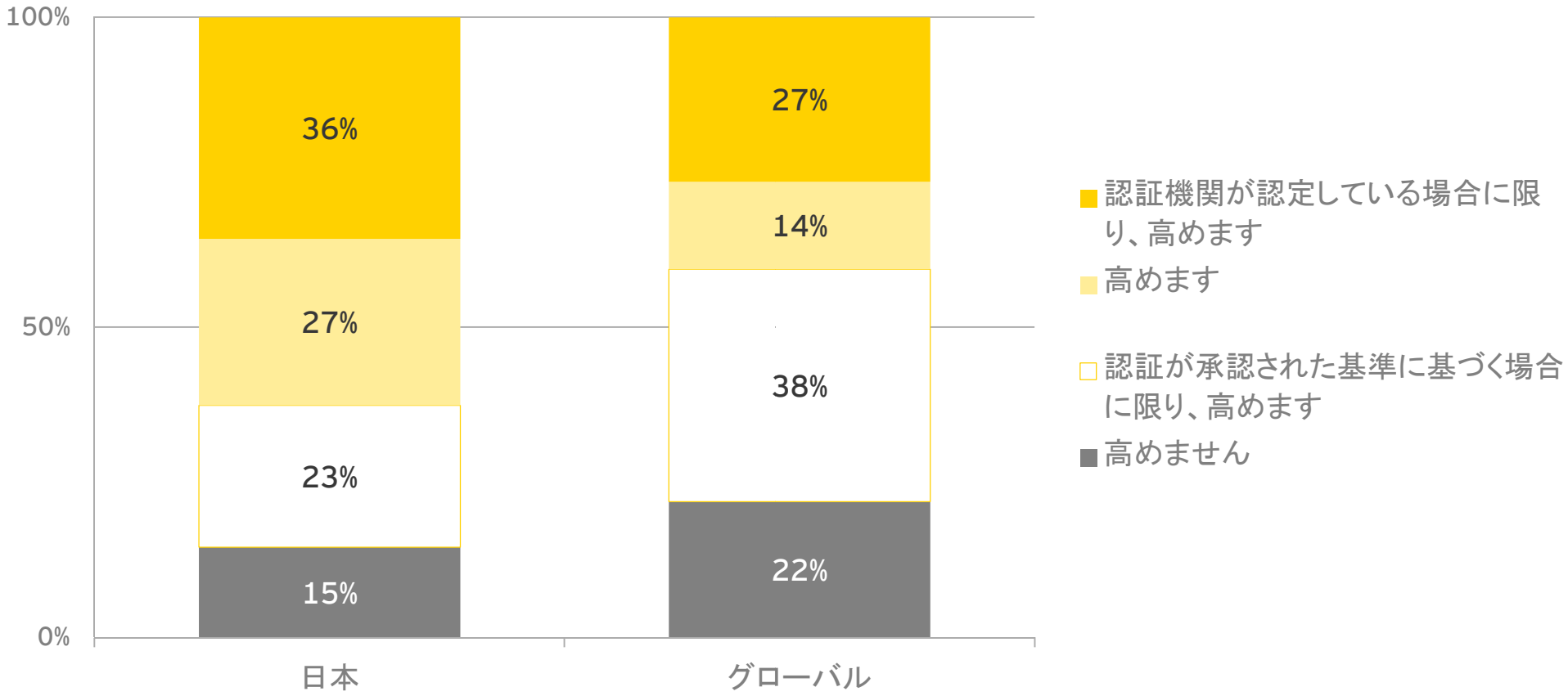
Q30. 現在利用中、または計画中のクラウドサービスの種類について、該当するものをすべて選択してください。



- 日本・グローバルともに、SaaS型クラウドサービスの利用を中心として、IaaS型、PaaS型を組み合わせてクラウドサービスを利用している傾向があります

6.3.クラウドサービスプロバイダの外部認証の信頼性

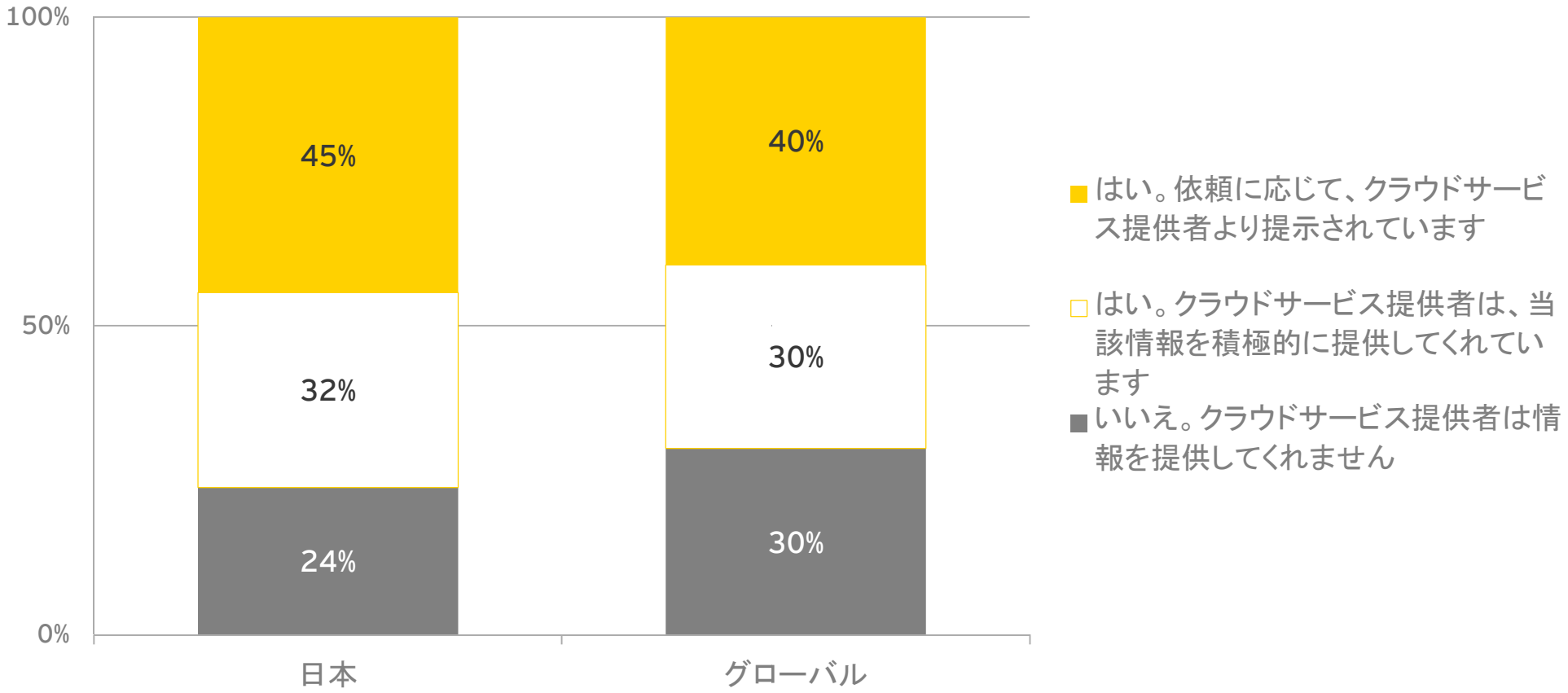
Q31. クラウドのサービスプロバイダが取得した外部認証や証明書は、クラウドコンピューティングに対する信頼を高めますか？
該当するものを1つ選択してください。



- 多くの企業が、クラウドのサービスプロバイダが取得した外部認証や証明書は、クラウドコンピューティングに対する信頼を高めると回答しています

6.4.クラウドサービスを利用している場合の自社データの所在

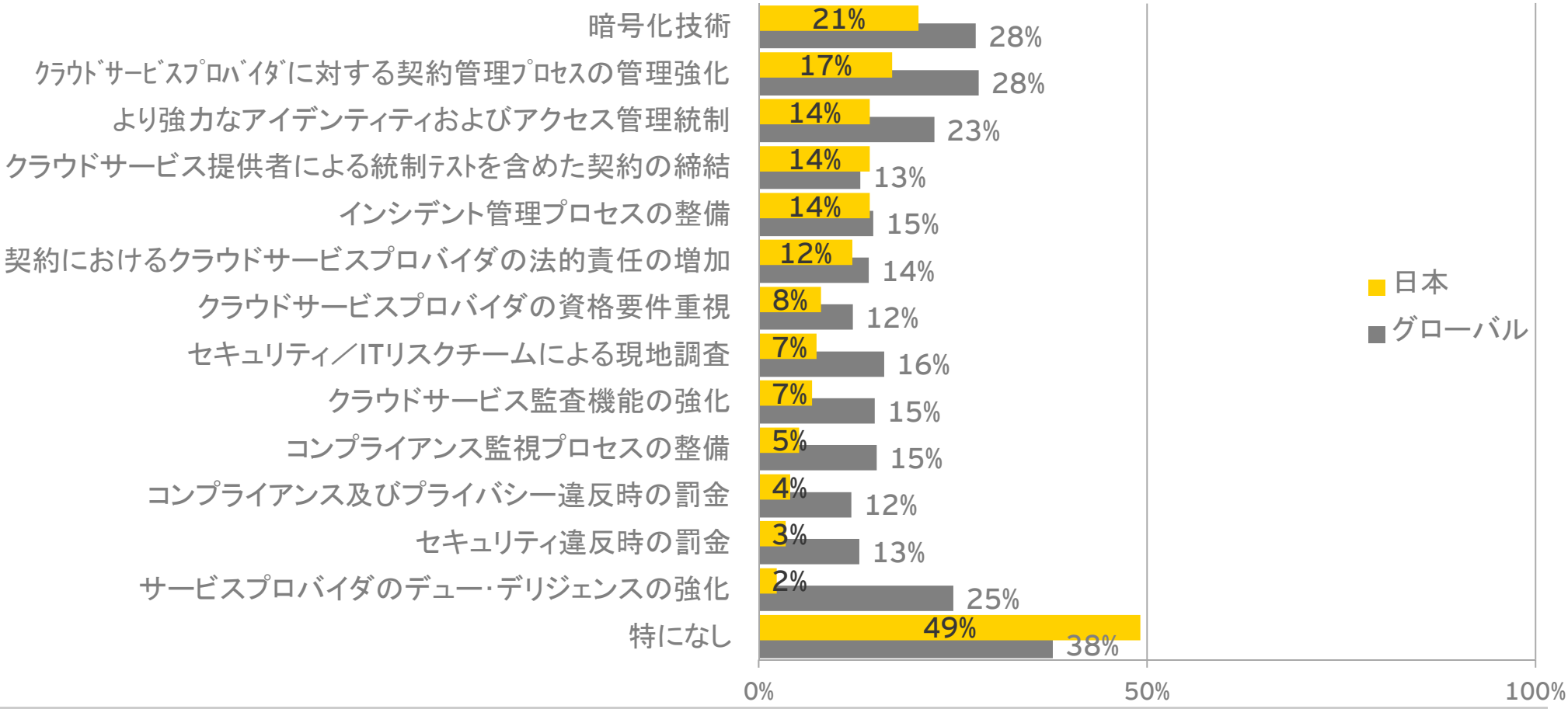
Q32. クラウドを利用している場合、自社のデータがどこ(国または地域)にあるか認識していますか?該当するものを1つ選択してください。



- グローバルでは、約30%の企業が、クラウドを利用した自社データの所在(国または地域)を認識していません

6.5.クラウドサービスに関するコントロール

Q33. クラウドコンピューティングを利用する際、「新たな」または「増加する」リスクを低減するために実施しているコントロールについて、該当するものをすべて選択してください。該当しない場合は「特になし」としてください。



- 日本では、約49%の企業が、クラウドコンピューティングに関するリスクを低減するためのコントロールを実施していないと回答しています
- 日本では、クラウドコンピューティングに関するリスクを低減するためのコントロールを、全体的に実施していない傾向があります

調査結果

7.ソーシャルメディア

7.ソーシャルメディア

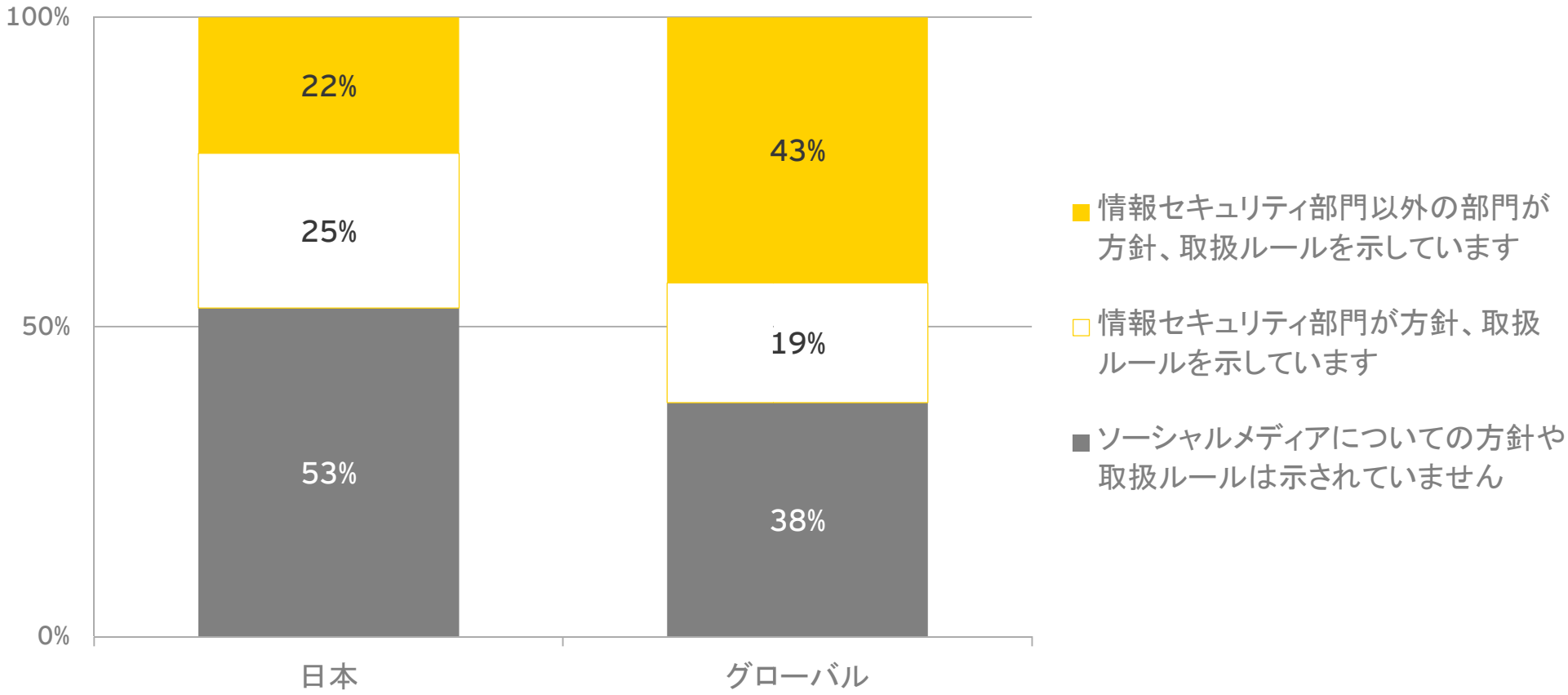
調査結果の概要と私たちの見解

急速に普及するソーシャルメディアの活用に対応して、企業は情報セキュリティ面でのコントロールに取組み始めています

- 日本では、約53%の企業が、ソーシャルメディアについての方針や取扱ルールを示していません
- 日本では、約48%の企業が、ソーシャルメディアに関するリスクを低減するためのコントロールを実施していないと回答しています
- ソーシャルメディア利用に関するコントロールにおいて、技術面に加えて、「セキュリティおよびソーシャルメディアについての意識向上プログラム」、「ポリシーの改訂」が重要です

7.1.ソーシャルメディアの取り扱い

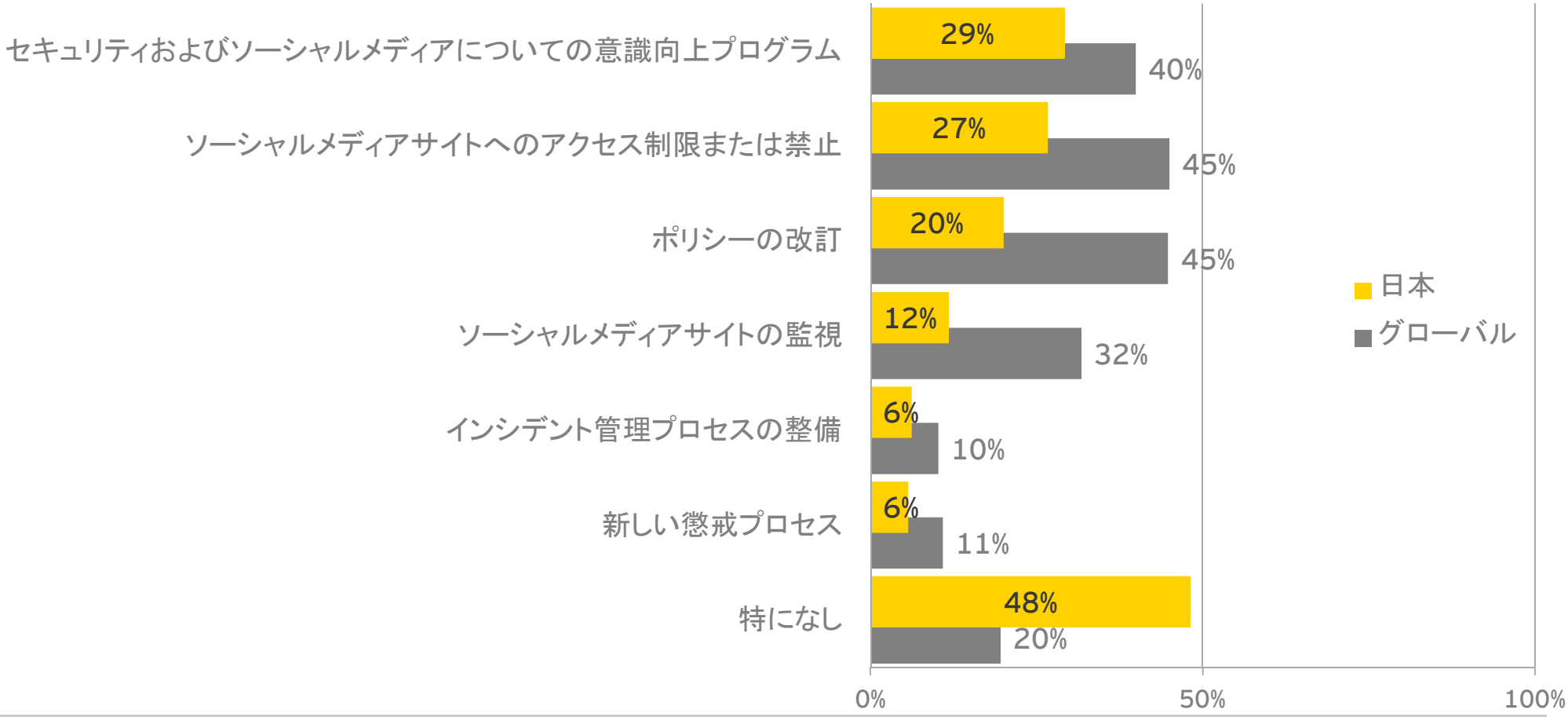
Q34. 貴社におけるソーシャルメディアの取扱いについて、該当するものを1つ選択してください。



- 日本では、約53%の企業が、ソーシャルメディアについての方針や取扱ルールを示していません

7.2.ソーシャルメディアに関するコントロール

Q35. ソーシャルメディアを利用する際、「新たな」または「増加する」リスクを低減するために貴社が実施しているコントロールについて、該当するものをすべて選択してください。該当しない場合は「特になし」としてください。



- 日本では、約48%の企業が、ソーシャルメディアに関するリスクを低減するためのコントロールを実施していないと回答しています

調査結果

8.情報セキュリティ技術

8.情報セキュリティ技術

調査結果の概要と私たちの見解

情報セキュリティに関する既存製品を十分に活用できていません

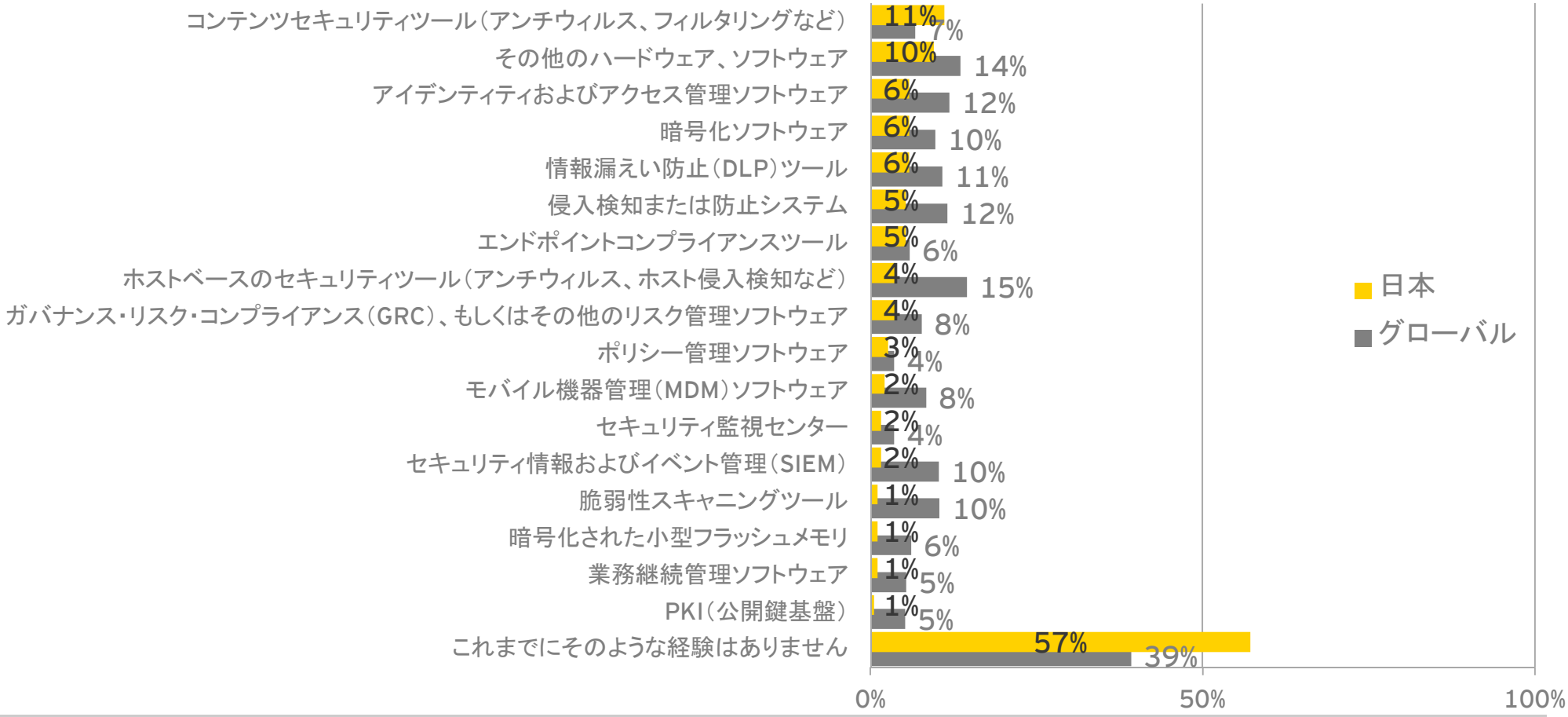
- 日本では、「既存ツールの十分な利用」「技術の活用およびその結果生成される情報をサポートするための運用プロセスの開発」などが、新しいツールや技術に関する課題として認識されている傾向があります

グローバルではデータ利用ポリシーについて、技術的・網羅的に実際の状況を評価し、遵守させることができるDLPツールの活用が始まっています

- 日本・グローバルともに、多くの企業で、機密情報の分類と取扱いに関するポリシーが策定されています
- グローバルでは、データが組織の意図通りに利用されているかをDLPツールで確認し始めています

8.1.情報セキュリティをサポートする製品の導入

Q36. 情報セキュリティをサポートするソフトウェアまたはハードウェアに関して、失敗した、もしくは期待にそぐわなかったと感じたことがありますか？感じたことがある場合、それはどのような製品ですか？該当するものをすべて選択してください。

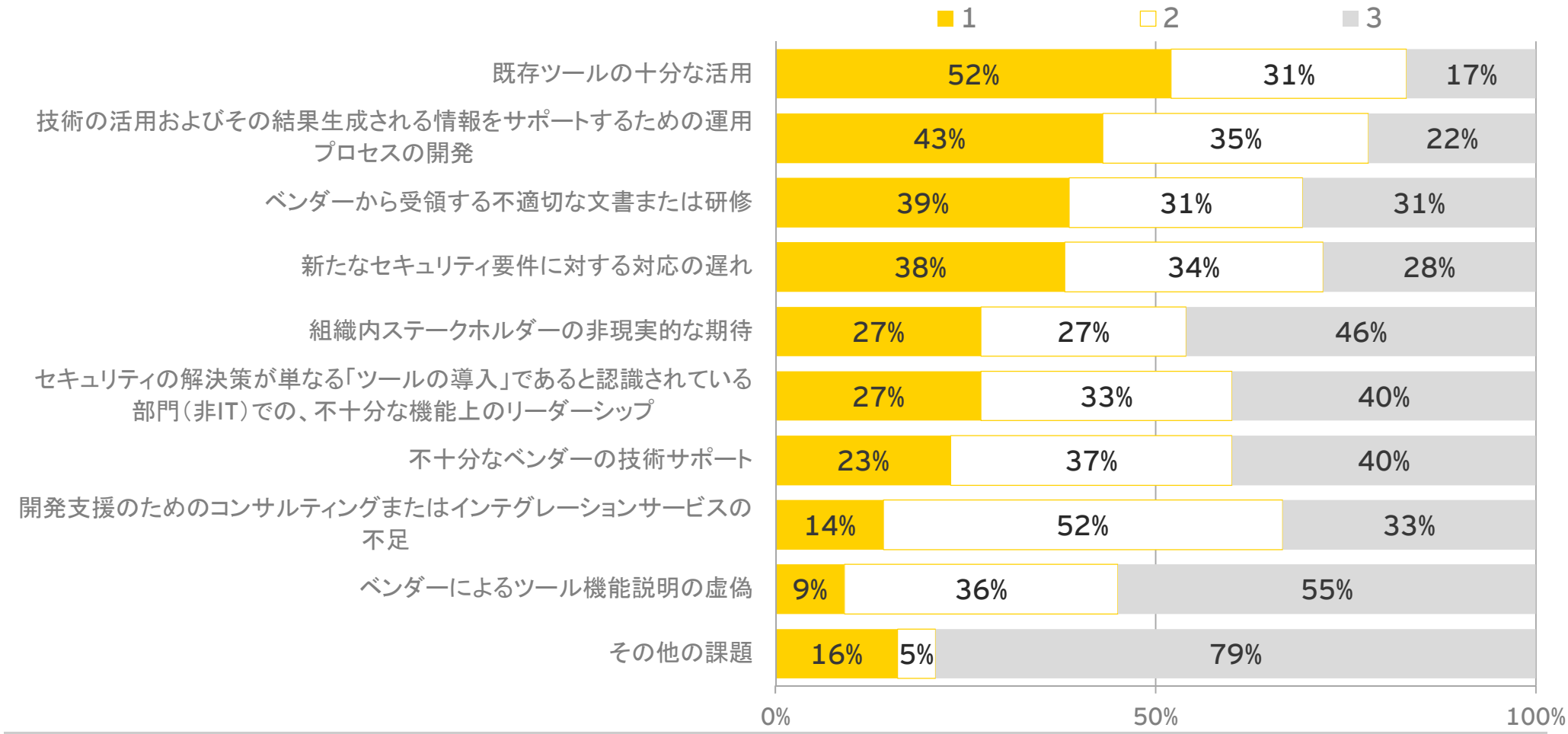


- 日本では、43%の企業が情報セキュリティをサポートするソフトウェアまたはハードウェアに関して、失敗した、もしくは期待にそぐわなかったと感じたことがあると回答しています

日本

8.2.新しいツールや技術に関する課題

Q37. 新しいツールや技術に関する課題について、下記より3つ選択し、大きい課題から順に1、2、3と番号を記入ください。

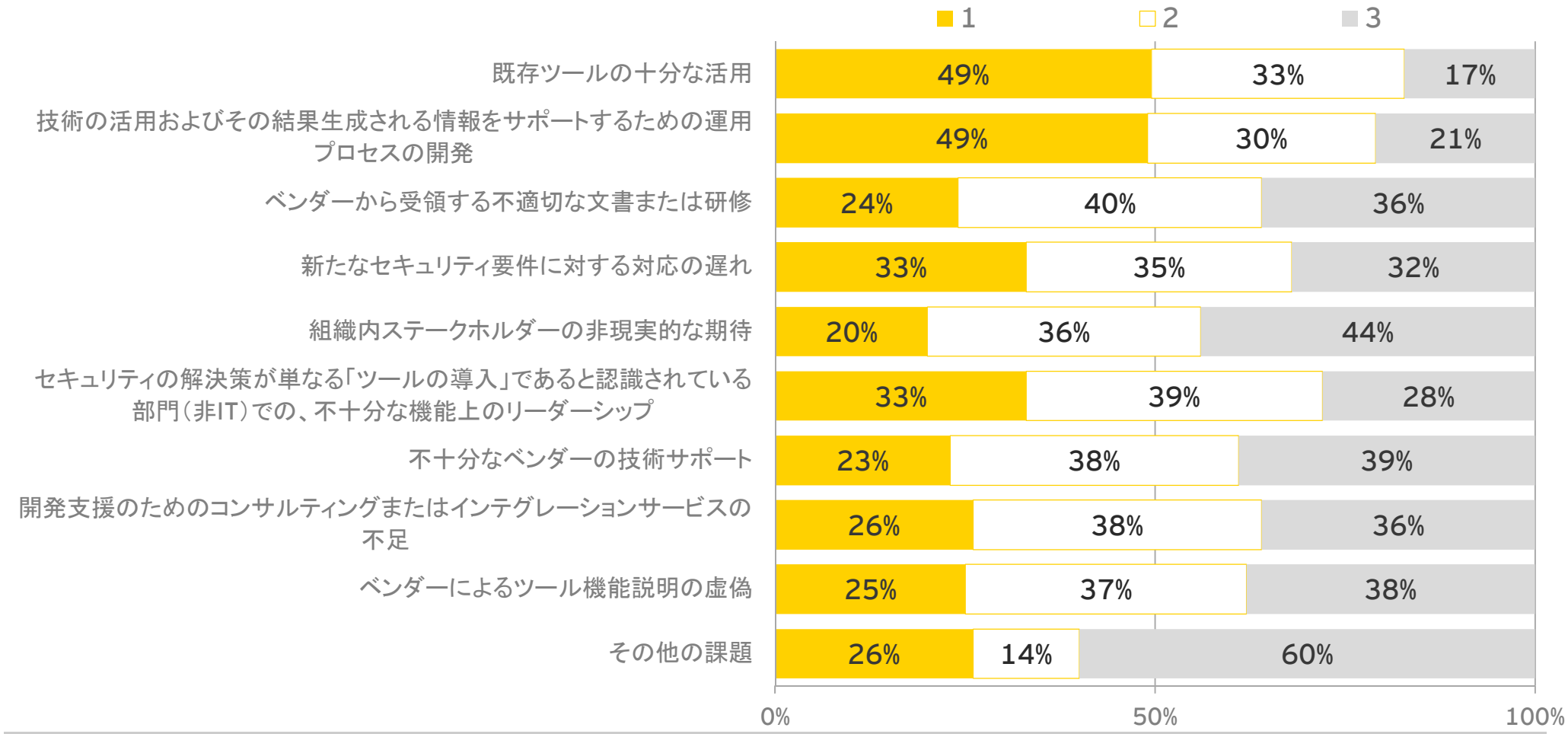


- 日本では、「既存ツールの十分な利用」「技術の活用およびその結果生成される情報をサポートするための運用プロセスの開発」などが、新しいツールや技術に関する課題として認識されている傾向があります

グローバル

8.2.新しいツールや技術に関する課題

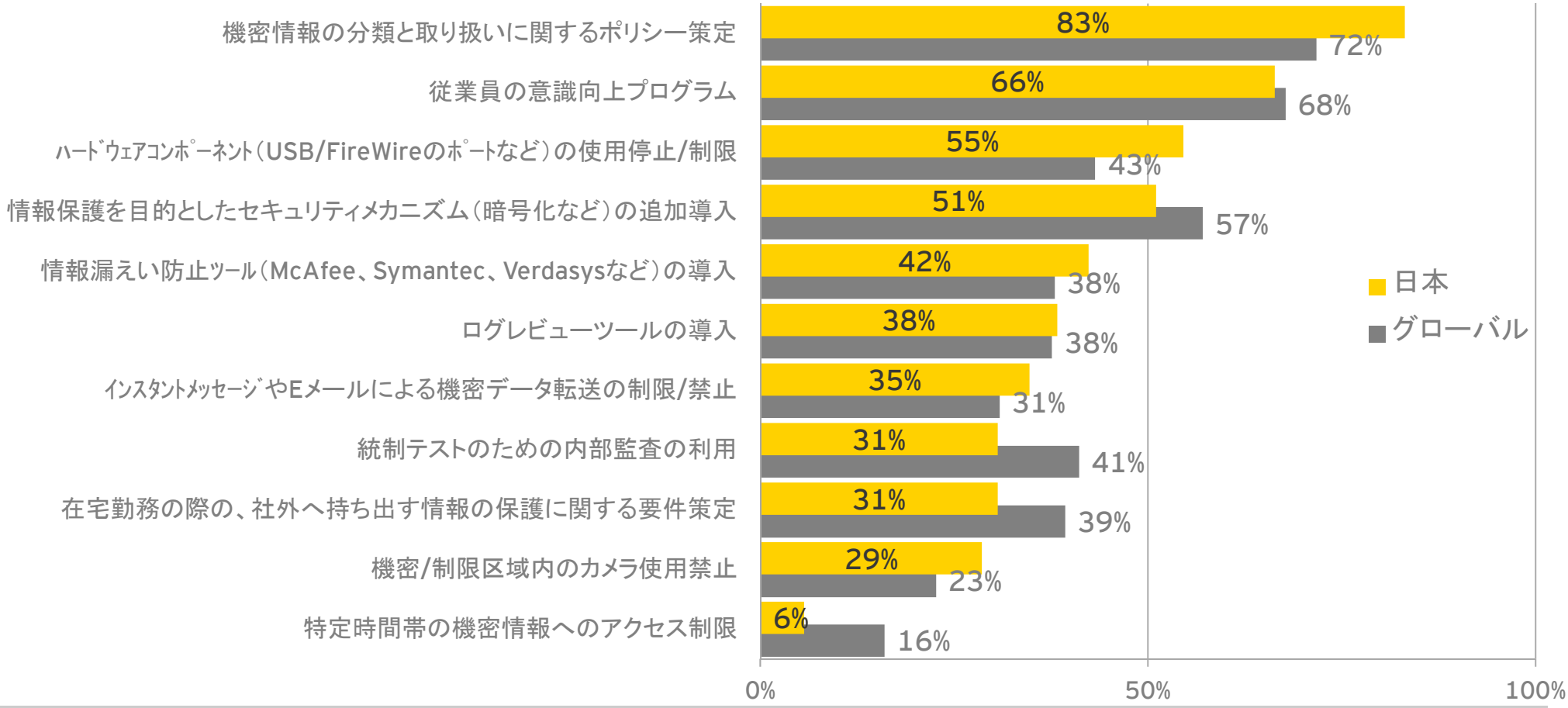
Q37. 新しいツールや技術に関する課題について、下記より3つ選択し、大きい課題から順に1、2、3と番号を記入ください。



- グローバルでも同様に、「既存ツールの十分な利用」「技術の活用およびその結果生成される情報をサポートするための運用プロセスの開発」などが、新しいツールや技術に関する課題として認識されている傾向があります

8.3.機密情報漏えい防止対策

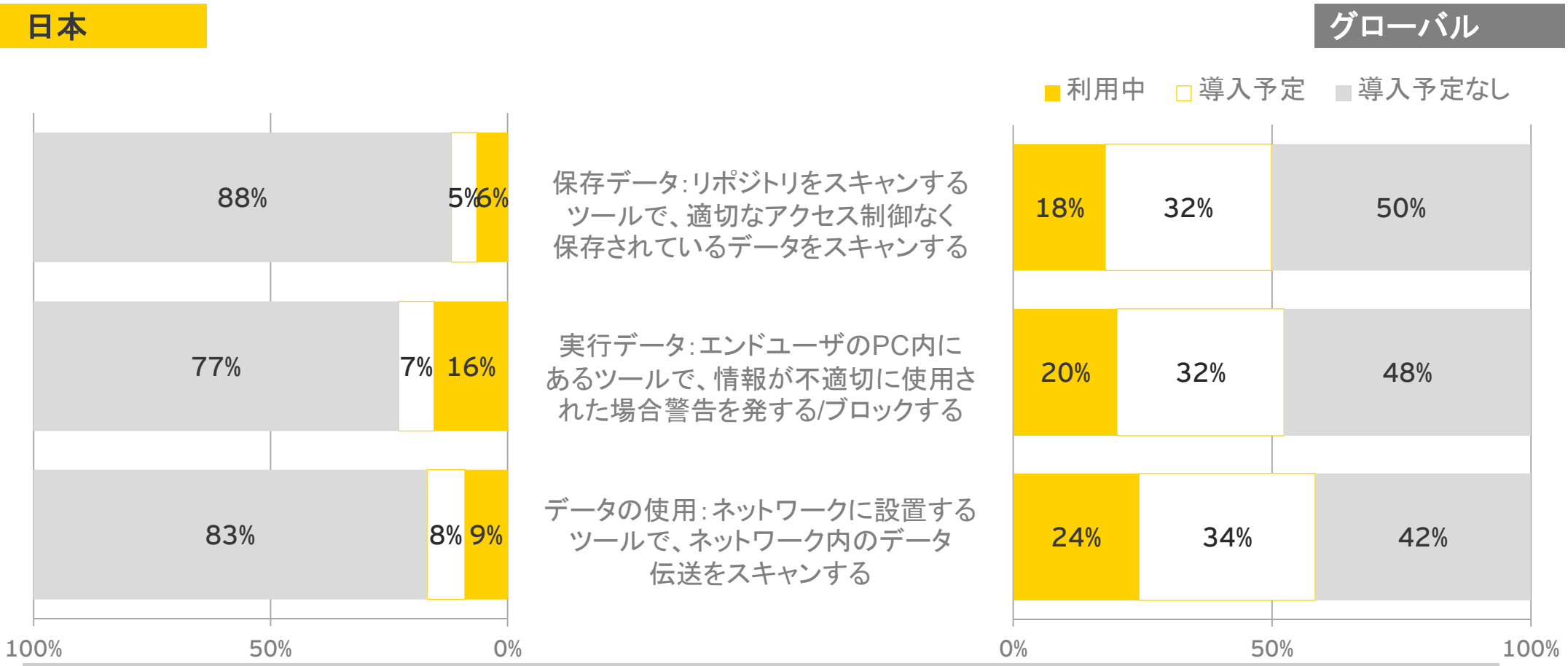
Q38. 貴社の機密情報漏えい防止対策について、該当するものをすべて選択してください。



- 日本・グローバルともに、多くの企業で、機密情報の分類と取扱いに関するポリシーが策定されています

8.4.DLPツールの導入状況

Q39.「情報漏えい防止（DLP）」とは、情報がどのように使用（場合によっては悪用）されているかを検出することができるツールの名称で、McAfee、Symantec、Verdasys、RSAといったベンダーから製品が提供されています。下記のDLPツールに関し貴社に該当するものをすべて選択してください。



- グローバルでは、データが組織の意図通りに利用されているかをDLPツールを利用して確認し始めています

Ernst & Young

アーンスト・アンド・ヤングについて
アーンスト・アンド・ヤングは、アシュアランス、税務、トランザクションおよびアドバイザリーサービスの分野における世界的なリーダーです。全世界の16万7千人の構成員は、共通のバリュー（価値観）に基づいて、品質において徹底した責任を果します。私どもは、クライアント、構成員、そして社会の可能性の実現に向けて、プラスの変化をもたらすよう支援します。

「アーンスト・アンド・ヤング」とは、アーンスト・アンド・ヤング・グローバル・リミテッドのメンバーファームで構成されるグローバル・ネットワークを指し、各メンバーファームは法的に独立した組織です。アーンスト・アンド・ヤング・グローバル・リミテッドは、英国の保証有限責任会社であり、顧客サービスは提供していません。詳しくは、www.ey.com にて紹介しています。

新日本有限責任監査法人について
新日本有限責任監査法人は、アーンスト・アンド・ヤングのメンバーファームです。全国に拠点を持ち、日本最大級の人員を擁する監査法人業界のリーダーです。品質を最優先に、監査および保証業務をはじめ、各種財務関連アドバイザリーサービスなどを提供しています。アーンスト・アンド・ヤングのグローバル・ネットワークを通じて、日本を取り巻く世界経済、社会における資本市場への信任を確保し、その機能を向上するため、可能性の実現を追求します。詳しくは、www.shinnihon.or.jp にて紹介しています。