Ernst & Young's 2011
情報セキュリティグローバルサーベイ

2011/12

新日本有限責任監査法人

ERNST & YOUNG

Quality In Everything We Do

Ernst & Young
情報セキュリティ グローバルサーベイ

今年で14年目を迎えるErnst & Youngの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ーの問題による影響を他社と比較し、重要な意思決定をする際の情報としてお役立て頂けるものとなっております。
本年度のサーベイは、2011年6月から2011年8月の期間、全主要産業において、52カ国、1,683社（日本では124社）のお客様にご参加頂きました。

Contents

調査要領

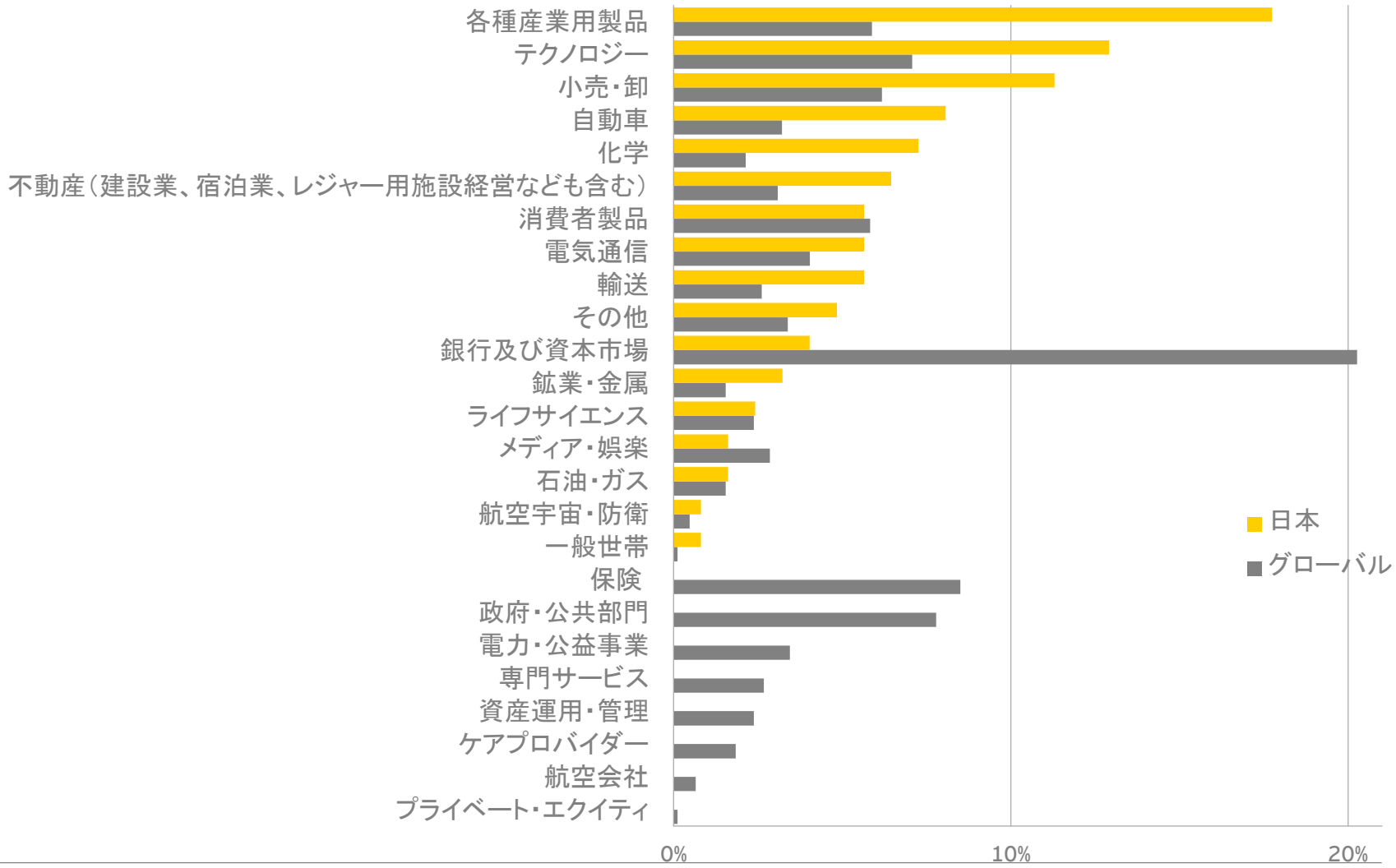
調査要領

1. 調査期間
   - 2011年6月から2011年8月

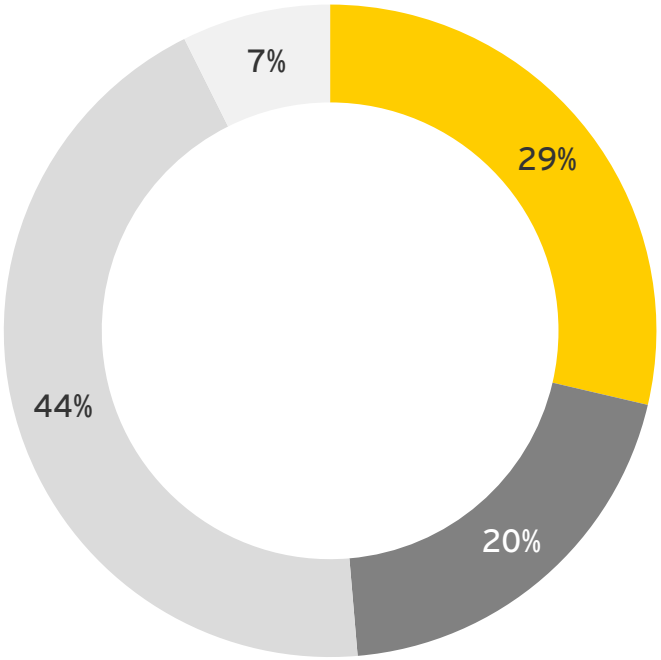
2. 回答総数
   - グローバル52カ国、1,683社（内日本では124社）

3. 調査方法
   - 本調査は、誰もが参加できるオンライン調査とは異なり、CIO（最高情報責任者）、CISO（最高情報セキュリティ責任者）、CFO（最高財務責任者）、CEO（最高経営責任者）、その他の情報セキュリティ担当役員の方々に参加をお願いして実施しています。

回答者属性
産業セクター別



回答者属性
地域別内訳（52カ国から1,683名の回答者）



アメリカズ	%
米国	17.47
メキシコ	5.11
ブラジル	3.39
カナダ	1.43
アルゼンチン	0.77
チリ	0.18
バミューダ	0.12
ウルグアイ	0.12
バルバドス	0.06
	28.65

アジア太平洋	%
オーストラリア	9.8
中国	4.93
フィリピン	2.67
ニュージーランド	1.25
シンガポール	0.71
台湾	0.59
マレーシア	0.06
	20.01

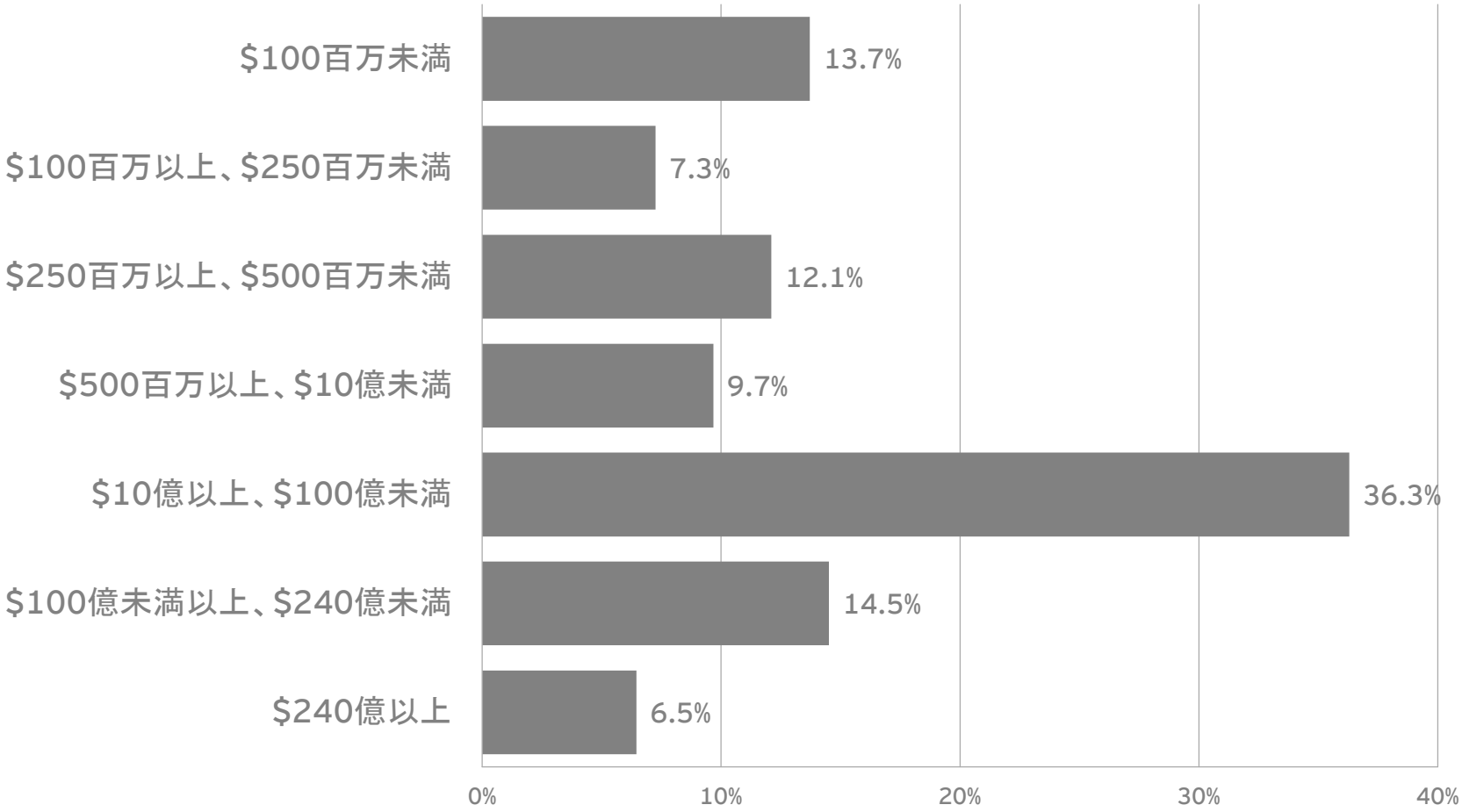
日本	%
日本	7.37
	7.37

ヨーロッパ、中東、インド及びアフリカ	%
インド	4.52
イタリア	3.21
フィンランド	3.15
スイス	3.09
オランダ	2.61
ジンバブエ	2.61
ベルギー	2.44

ヨーロッパ、中東、インド及びアフリカ	%
ルクセンブルク	2.20
フランス	2.02
ベラルーシ	1.96
英国	1.90
チュニジア	1.72
トルコ	1.43
ドイツ	1.25
ロシア連邦	1.25
ラトビア	1.19
オーストリア	0.83
アイルランド	0.83
クロアチア	0.77
ウクライナ	0.77
ノルウェー	0.65
アラブ首長国連邦	0.65
ポーランド	0.53
ギリシャ	0.48
チェコ共和国	0.36
スペイン	0.30
ルーマニア	0.24
スウェーデン	0.24
グルジア	0.18
カザフスタン	0.18
バーレーン	0.12
エジプト	0.12
マルタ	0.06
デンマーク	0.06
サウジアラビア	0.06
	43.98

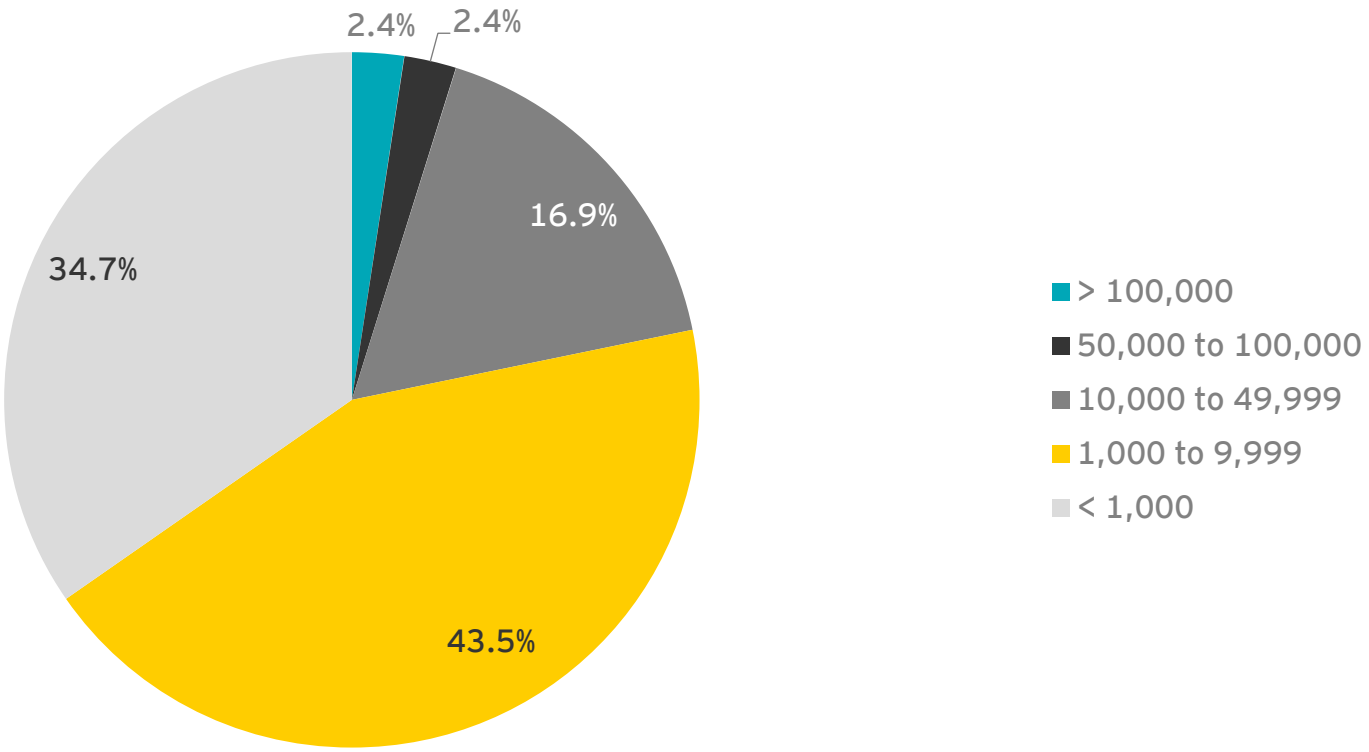
回答者属性
収益別内訳（年間）

日本の状況



回答者属性
従業員人数別内訳

日本の状況



アンケート概要

1.投資と課題

- 情報セキュリティ関連予算は増加傾向
- 情報セキュリティ予算の第1位はBCP
- 情報セキュリティの役割の第1位はERM
- 情報セキュリティの課題は優れた人材の確保

2.脅威、リスクと対策

- 新しい脅威は外部からの攻撃
- 外部からの攻撃に対するリスク環境の変化
- 日本の脅威は自然災害
- モバイルコンピューティングのコントロールについて
- クラウドコンピューティングのコントロールについて
- ソーシャルメディアのコントロールについて

3.ツールとテクノロジー

- グローバルではGRCツールを活用
- タブレットコンピュータの使用は限定的
- クラウドコンピューティングの利用状況
- グローバルで拡大するアクセス管理技術
- グローバルでの情報セキュリティツールの失敗
- 情報セキュリティツールの内訳
- 情報セキュリティツールの課題は運用プロセス
- 情報の漏えい防止技術の導入状況
- 日本は技術的セキュリティテストが少ない

4.戦略・ガバナンスとコントロール

- 新しい脅威に対する情報セキュリティ戦略の見直しの必要性
- 情報セキュリティマネジメントシステムの導入状況
- ITリスク管理プログラムの導入状況
- セキュリティ基準・フレームワークの導入状況
- セキュリティ・アーキテクチャの導入状況
- グローバルは情報セキュリティ評価に外部機関を利用
- 情報取り扱いの管理対策としての外部評価の利用
- 日本は事業継続管理のテストや訓練が少ない
- 日本は第三者機関による事業継続管理の評価が少ない

1.投資と課題

- 情報セキュリティ関連予算は増加傾向
- 情報セキュリティ予算の第1位はBCP
- 情報セキュリティの役割の第1位はERM
- 情報セキュリティの課題は優れた人材の確保

1.投資と課題
調査結果の概要

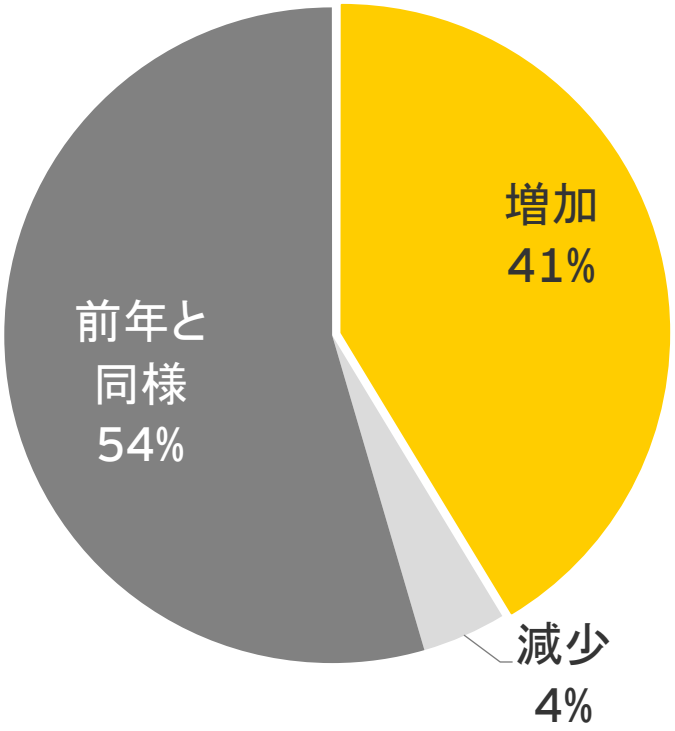
1. 情報セキュリティ関連予算は増加傾向
   - 9割の企業が予算を維持または増加、日本以上にグローバルで増加傾向
2. セキュリティ予算の第1位はBCP
   - 「情報漏洩/損失防止技術及びプロセス」の予算も重視
3. 情報セキュリティの役割の第1位はERM（全社的リスク管理）
   - グローバルは、「企業方針の順守」「評判とブランドの保護」も重視
4. 情報セキュリティの課題は優れた人材の確保
   - 日本は、「優れた人材の確保」を課題と考える企業の割合がグローバルよりも高い
   - グローバルは、「タブレット、スマートフォン及びその他のモバイル機器の導入」も課題と認識

1.投資と課題
1.1.情報セキュリティ関連予算の状況

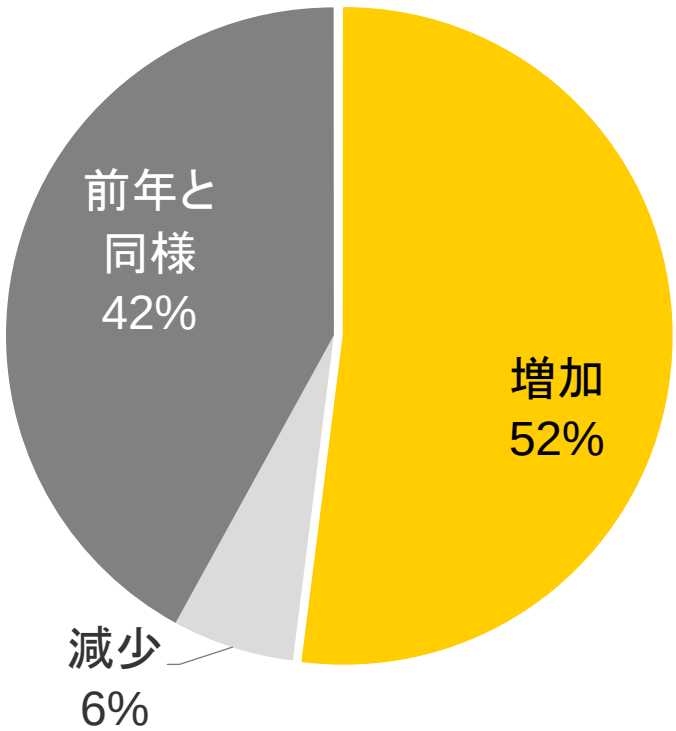
- 日本でもグローバルにおいても、情報セキュリティ予算は9割以上が現状維持、または、増加傾向にある

Q1.過去12ヶ月間の情報セキュリティ予算について、貴社に該当するものを1つ選択してください。

日本



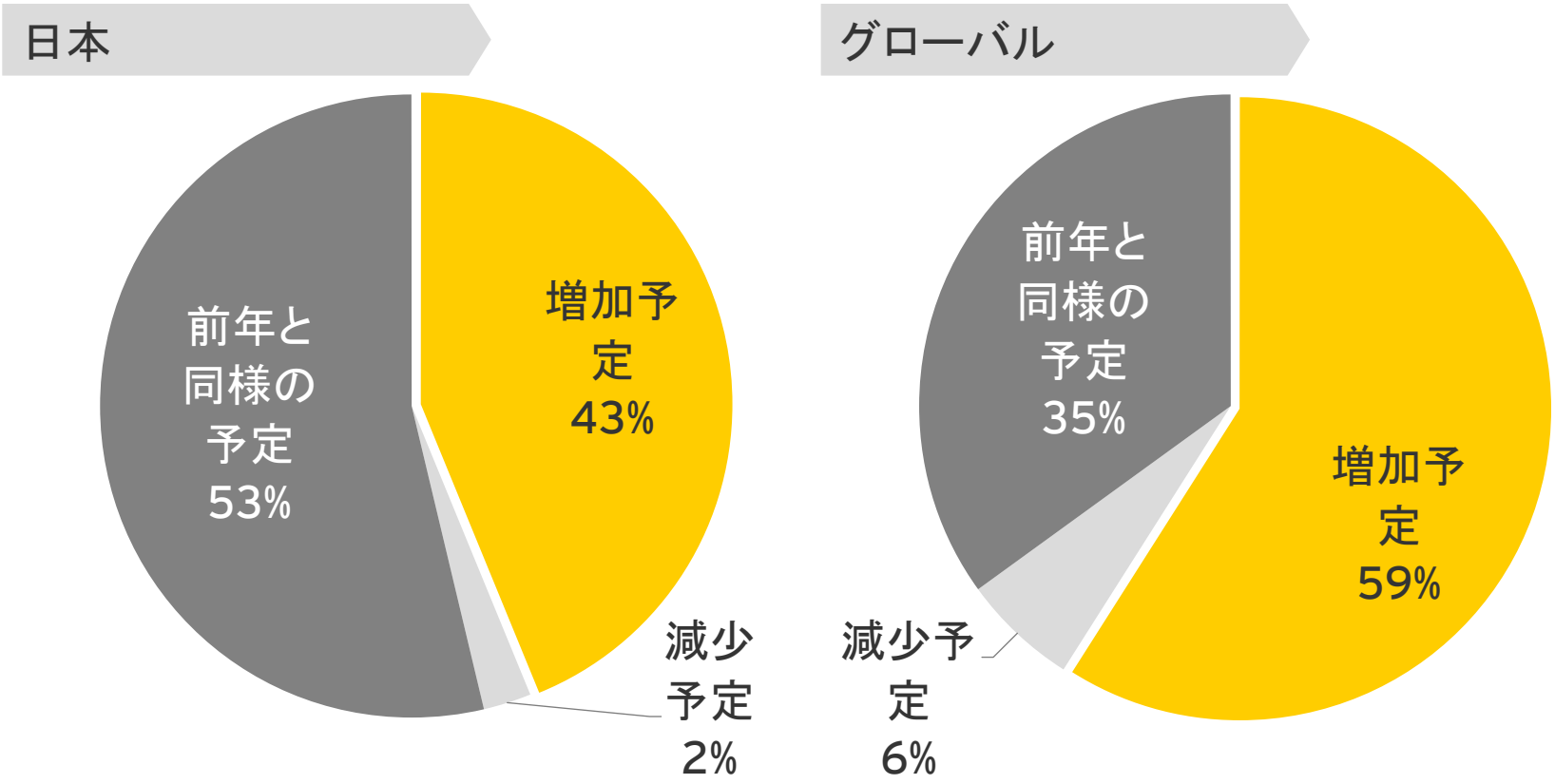
グローバル



1.投資と課題
1.1.a.情報セキュリティ予算計画

- 今後の予算の見通しについては、日本の4割に対し、グローバルでは6割が予算増を予定している

Q1a.今後12ヶ月間の情報セキュリティ予算計画について、貴社に該当するものを1つ選択してください。

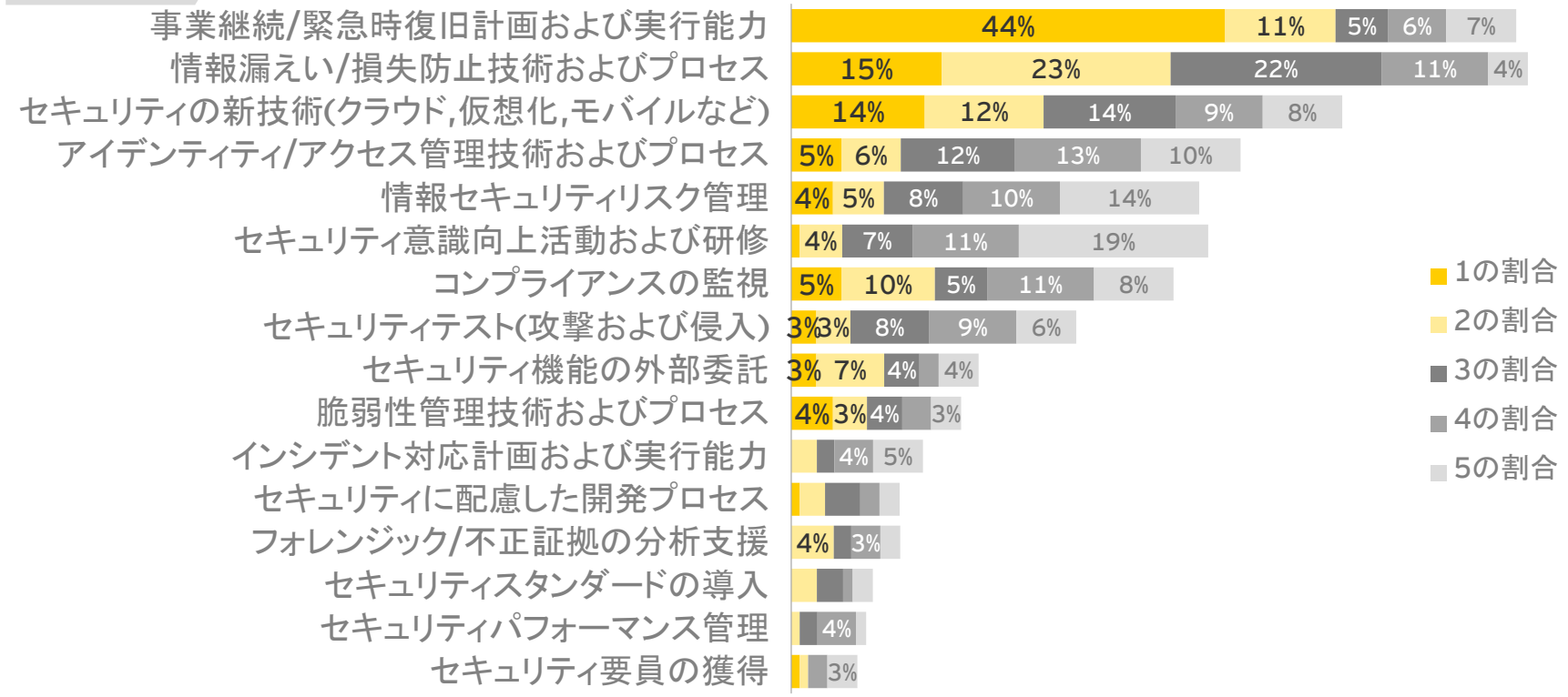


1.投資と課題
1.1.b.情報セキュリティ関連予算の内訳1

- 日本もグローバルも共に、セキュリティ予算の金額が最も大きいものは、「事業継続/緊急時復旧計画及び実行能力」である
- 「情報漏洩/損失防止技術及びプロセス」は2番目に大きい
- 日本は、東日本大震災の影響により「事業継続/緊急時復旧計画及び実行能力」に関連する予算を増額させている割合がグローバルよりも高い

Q1b.今後12ヶ月間で支出予定のあるセキュリティ項目を下記より5つ選択し、金額が高いものから順に1,2,3,4,5と番号を記入ください（1:高⇔5:低）

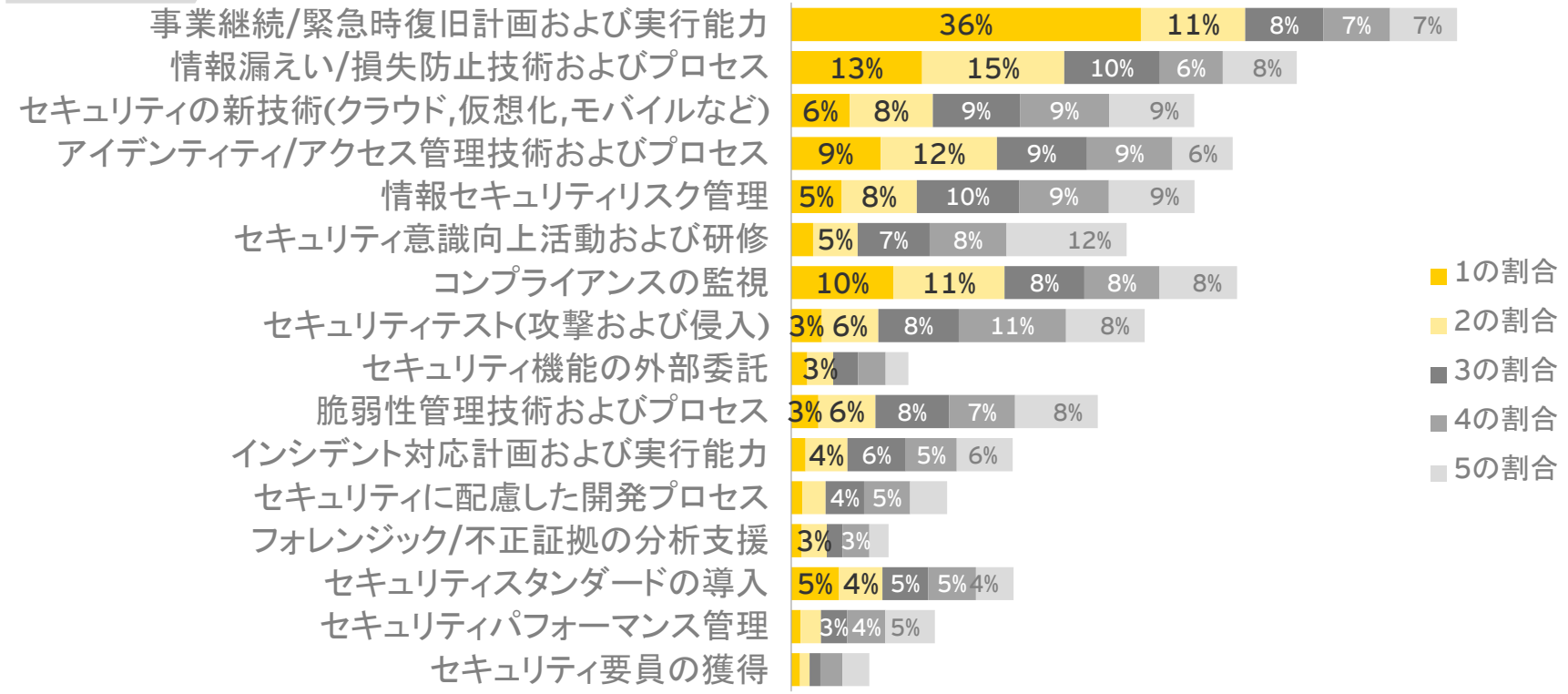
日本



1.投資と課題
1.1.b.情報セキュリティ関連予算の内訳2

Q1b.今後12ヶ月間で支出予定のあるセキュリティ項目を下記より5つ選択し、金額が高いものから順に1,2,3,4,5と番号を記入ください（1:高⇔5:低）

グローバル

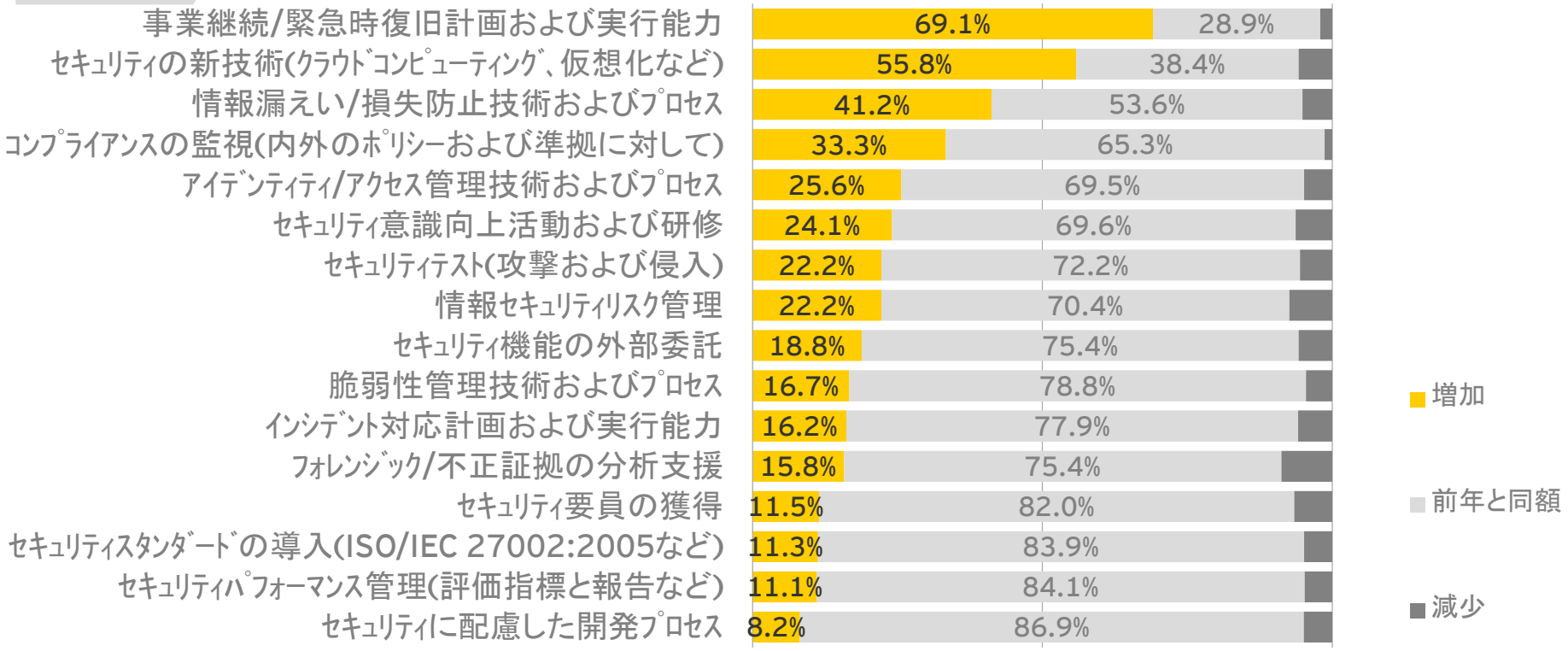


1.投資と課題
1.1.c.情報セキュリティ関連予算の内訳増減1

- 日本もグローバルも伴に、当年度の情報セキュリティの予算を前年度から増やしているのは、1位「事業継続/緊急時復旧計画及び実行能力」、2位「セキュリティの新技術（クラウド、仮想化、モバイル）」、3位「情報漏洩/損失防止技術及びプロセス」である

Q1c.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1つを選択してください。

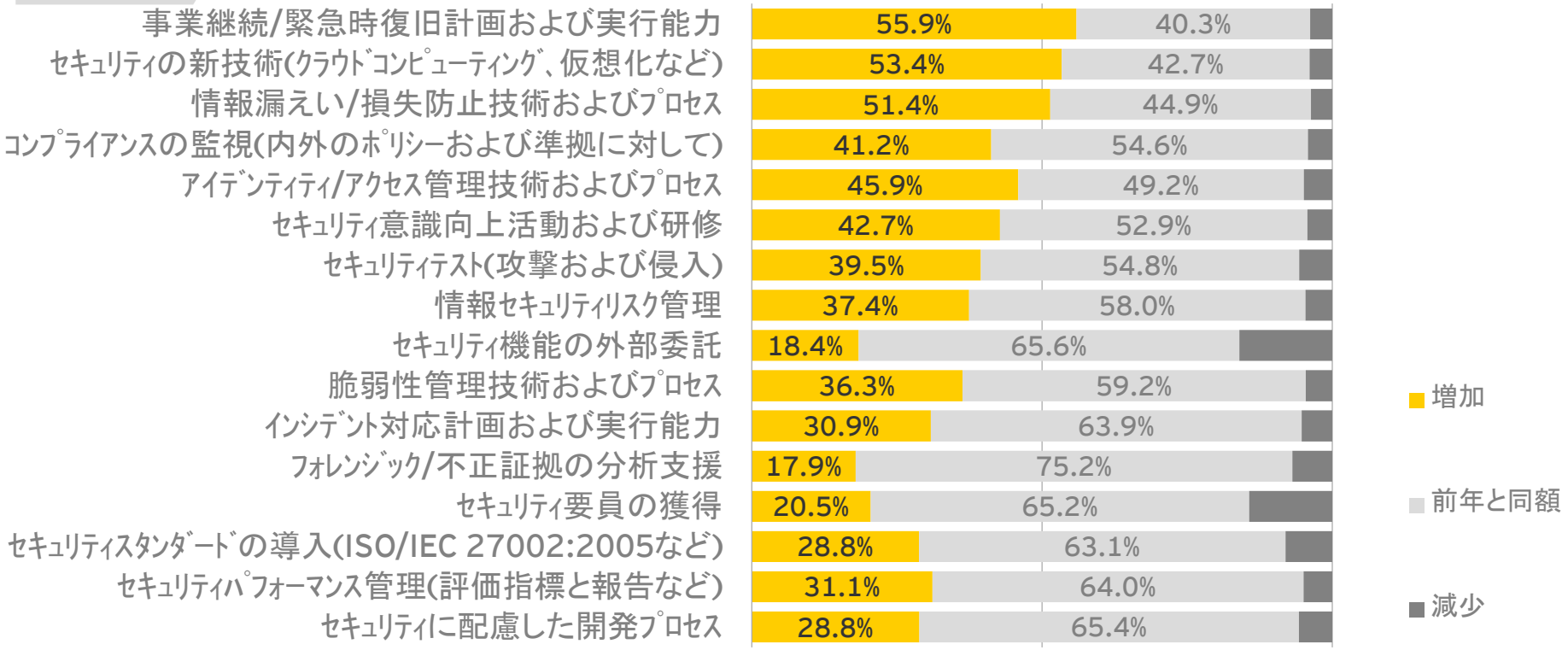
日本



1.投資と課題
1.1.c.情報セキュリティ関連予算の内訳増減2

Q1c.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1つを選択してください。

グローバル

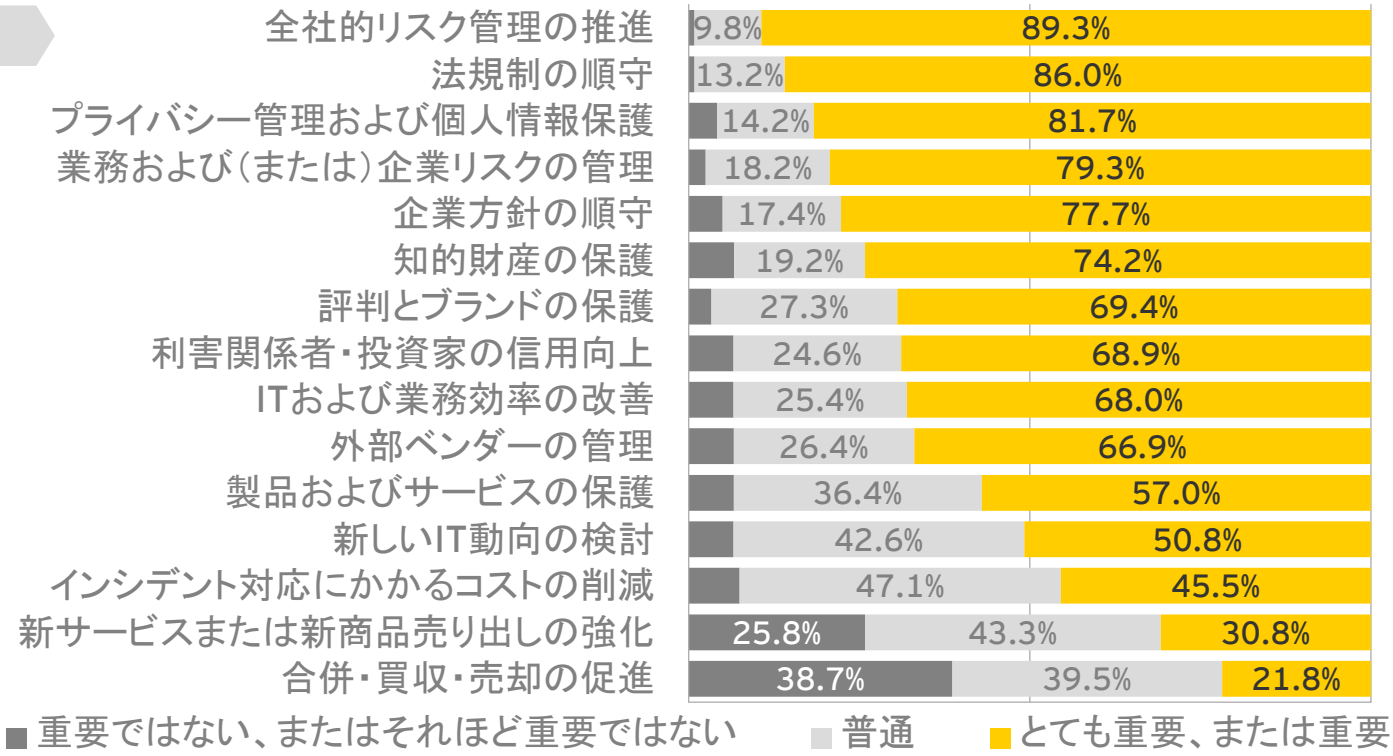


1.投資と課題
1.2.情報セキュリティの役割の重要性1

- 情報セキュリティの役割について、日本は1位「全社的リスク管理」（第1位）ととらえている
- グローバルでは「全社的リスク管理」の割合が低く、むしろ「法規制の順守」「プライバシー管理及び個人情報保護」「企業方針の順守」「評判とブランドの保護」が同程度に高い。

Q2.下記の活動において、情報セキュリティの役割はどれくらい重要ですか?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。

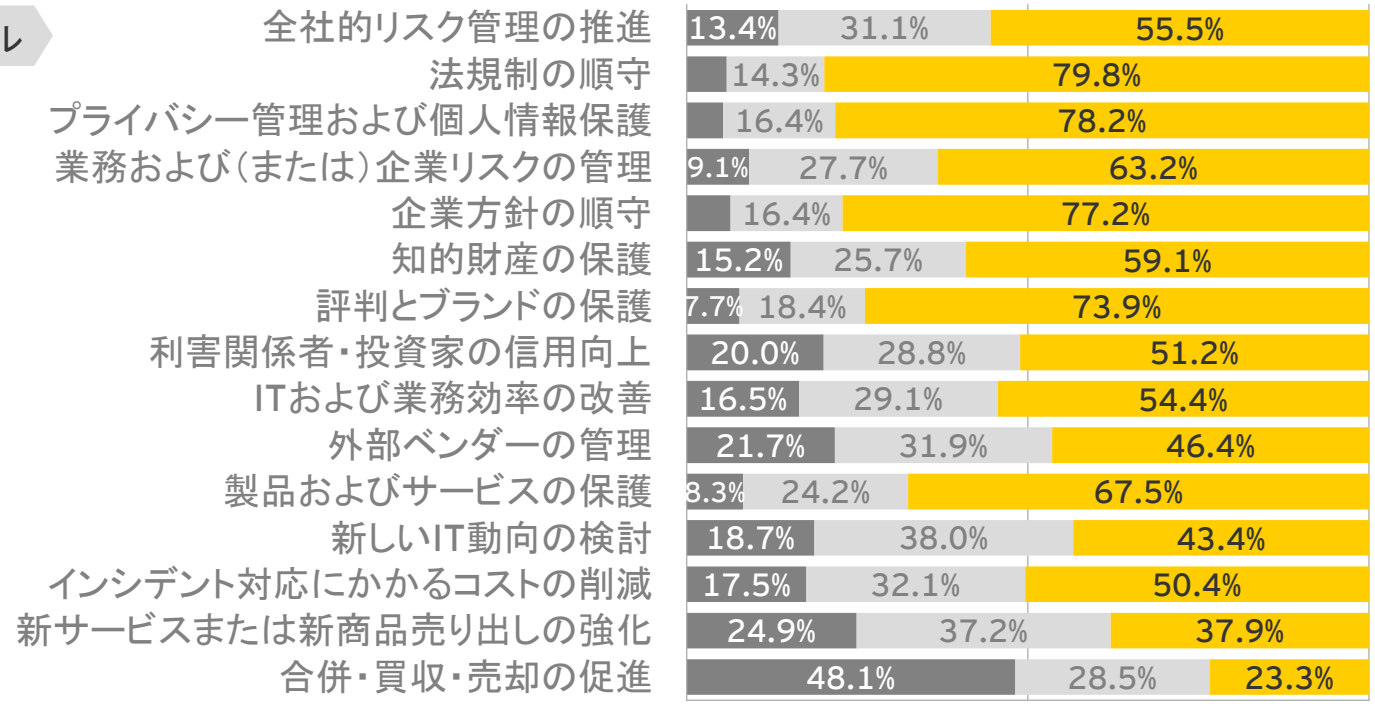
日本



1.投資と課題
1.2.情報セキュリティの役割の重要性2

Q2.下記の活動において、情報セキュリティの役割はどれくらい重要ですか?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。

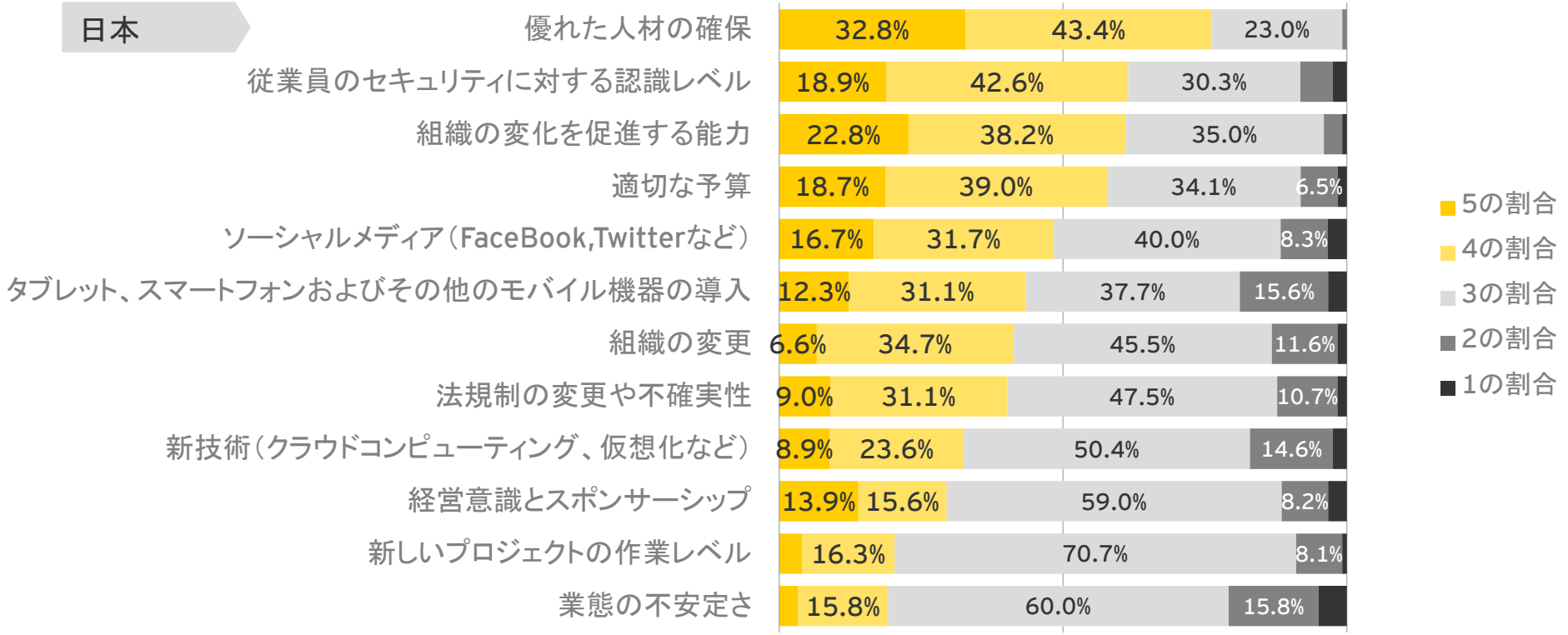
グローバル



1.投資と課題
1.3.情報セキュリティ課題の難易度1

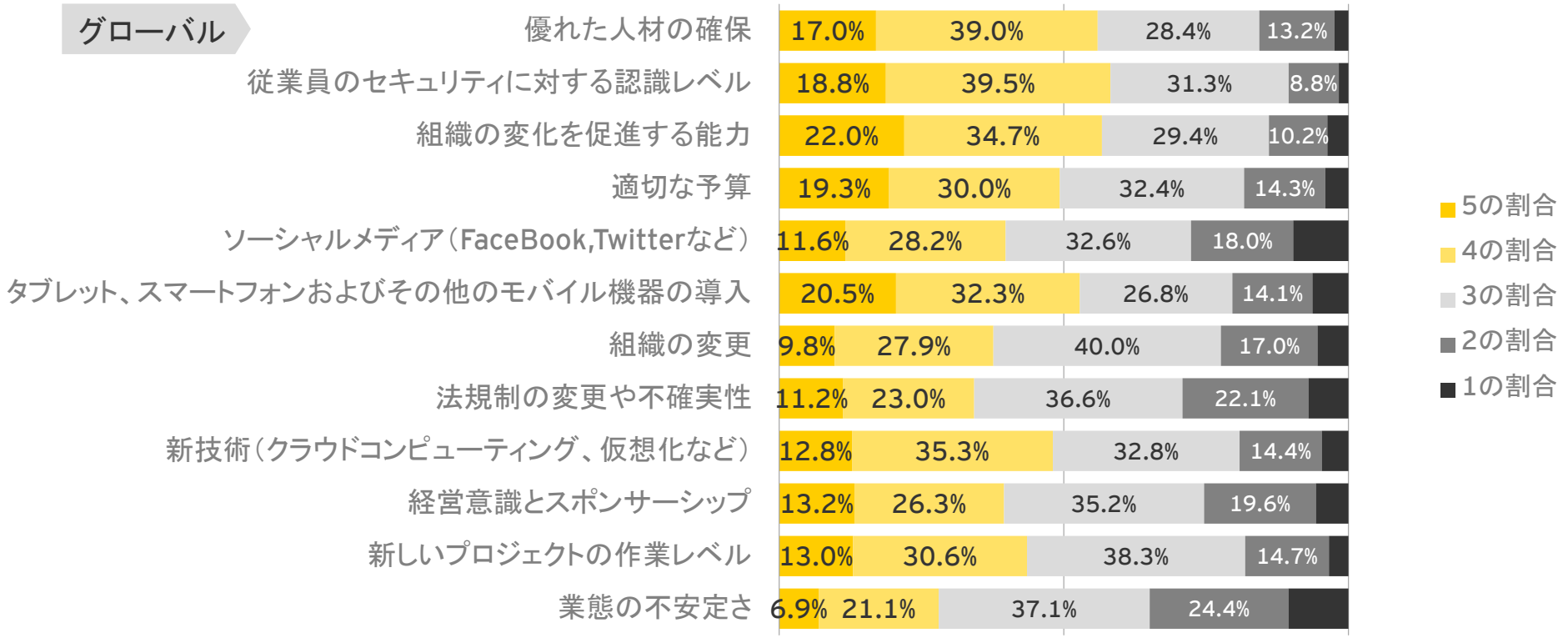
- 情報セキュリティの課題は、日本もグローバルも共に、「優れた人材の確保」、「従業員のセキュリティに対する認識レベル」、「組織の変化を促進する能力」である
- 日本は、「優れた人材の確保」が難しいと考えている
- グローバルは、「タブレット、スマートフォン及びその他のモバイル機器の導入」について課題と認識している

Q3.情報セキュリティへの取り組みを行う際に直面する課題の難易度について、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。(5:困難⇔1:容易)



1.投資と課題
1.3.情報セキュリティ課題の難易度2

Q3.情報セキュリティへの取り組みを行う際に直面する課題の難易度について、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。(5:困難⇔1:容易)



2.脅威、リスクと対策

- 新しい脅威は外部からの攻撃
- 外部からの攻撃に対するリスク環境の変化
- 日本の脅威は自然災害
- モバイルコンピューティングのコントロールについて
- クラウドコンピューティングのコントロールについて
- ソーシャルメディアのコントロールについて

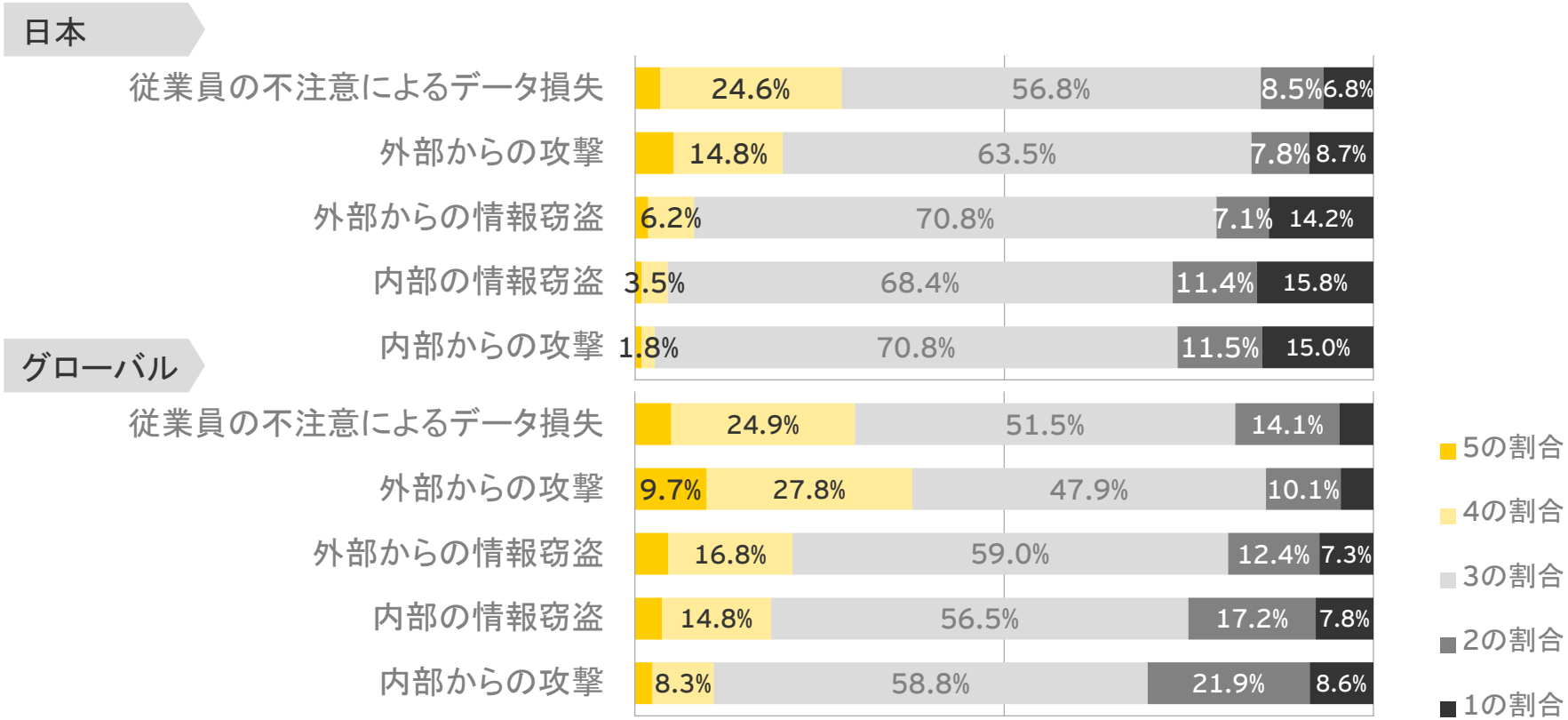
2.脅威、リスクと対策 調査結果の概要

1. 新しい脅威は外部からの攻撃
   - 最近の外部からのサイバー攻撃による事件を反映して、外部からの攻撃に対するリスクへの関心が世界的に高まっている。
2. 外部からの攻撃に対するリスク環境の変化
   - 外部からの攻撃のリスク認識は、日本が57%に対して、グローバルは72%とグローバルの方が高い
3. 日本の脅威は自然災害
   - グローバルでは、「ソーシャルメディア（LinkedIn, Facebook）」、「フィッシング」なども脅威と考える
4. モバイルコンピューティングのコントロールについて
   - 日本は「ポリシーの改定」、「新モバイル管理ソフトウェア」、「アーキテクチャの変更」などの実施が少ない
5. クラウドコンピューティングのコントロールについて
   - 日本は、「暗号化技術」、「クラウドサービスプロバイダの資格要件」を重視し、グローバルは、「クラウドサービスプロバイダに対する契約管理プロセスの管理強化」、「より強力なアイデンティティ及びアクセス管理統制」、「サービスプロバイダのデュー・デリジェンスの強化」を重視している
6. ソーシャルメディアのコントロールについて
   - 日本は、「ソーシャルメディアサイトへのアクセスの制限または禁止」、「インターネット使用状況のモニタリングの強化」、「セキュリティ及びソーシャルメディアについての意識向上プログラム」の対策が弱い

2.脅威、リスクと対策
2.1.脅威の変化

- 日本もグローバルも共に、「外部からの攻撃により発生したインシデント」が増加している
- 逆に、「内部からの情報窃盗」、「内部からの攻撃によるインシデント」が減少している
- グローバルでは、「内部からの情報窃盗」、「内部からの攻撃によるインシデント」の増加が日本よりも高い

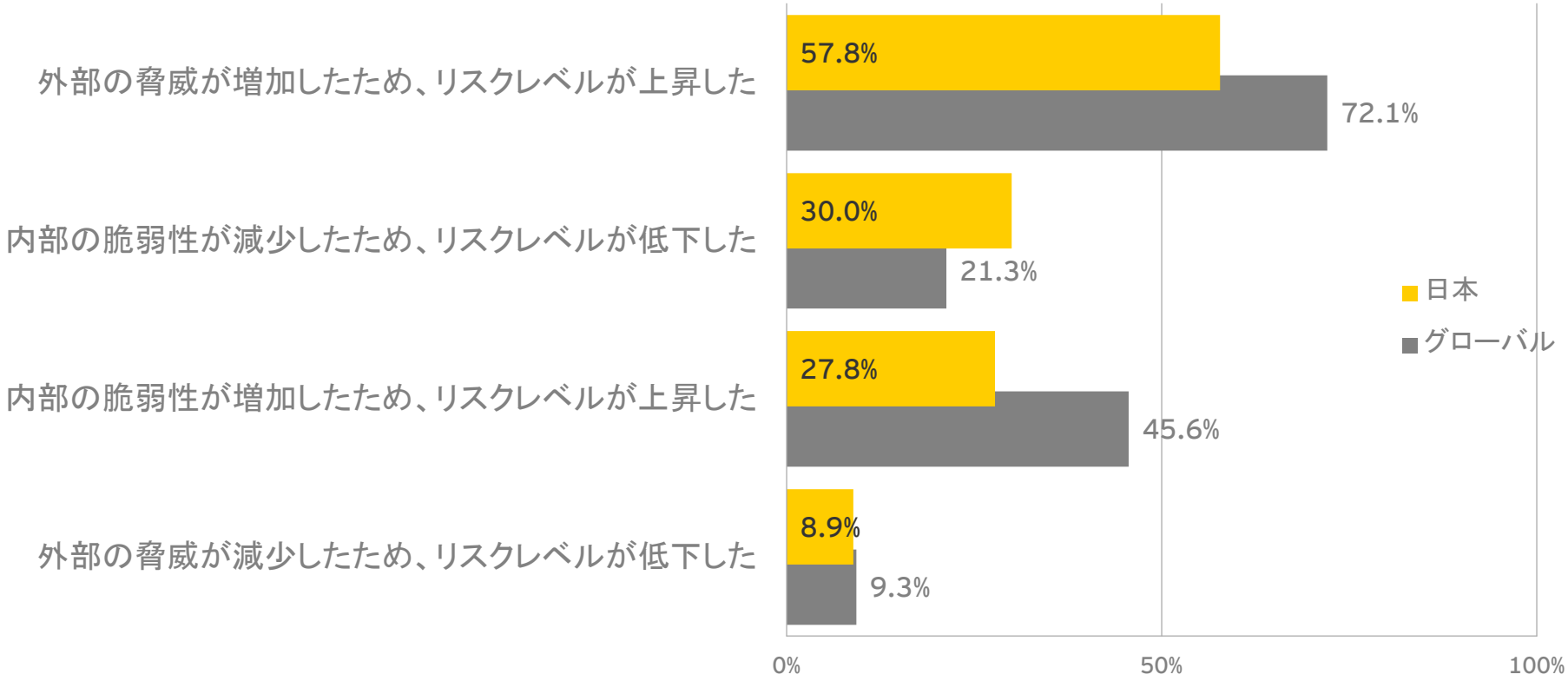
Q4.貴社で実際に発生したインシデントにおける、下記脅威の変化度について、5段階評価で1～5から該当するものを1つ選択してください。(5:非常に増加⇔1:非常に減少)



2.脅威、リスクと対策
2.2.リスク環境の変化

- 日本もグローバルも共に、「外部の脅威が増加したことによりリスクレベルが増加した」と考えている
- その割合は、日本57%よりもグローバル72%の方が高い
- グローバルでは、「内部の脆弱性が増加したため、リスクレベルが上昇した」と回答する企業の割合が日本よりも高い

Q5.過去12ヶ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。

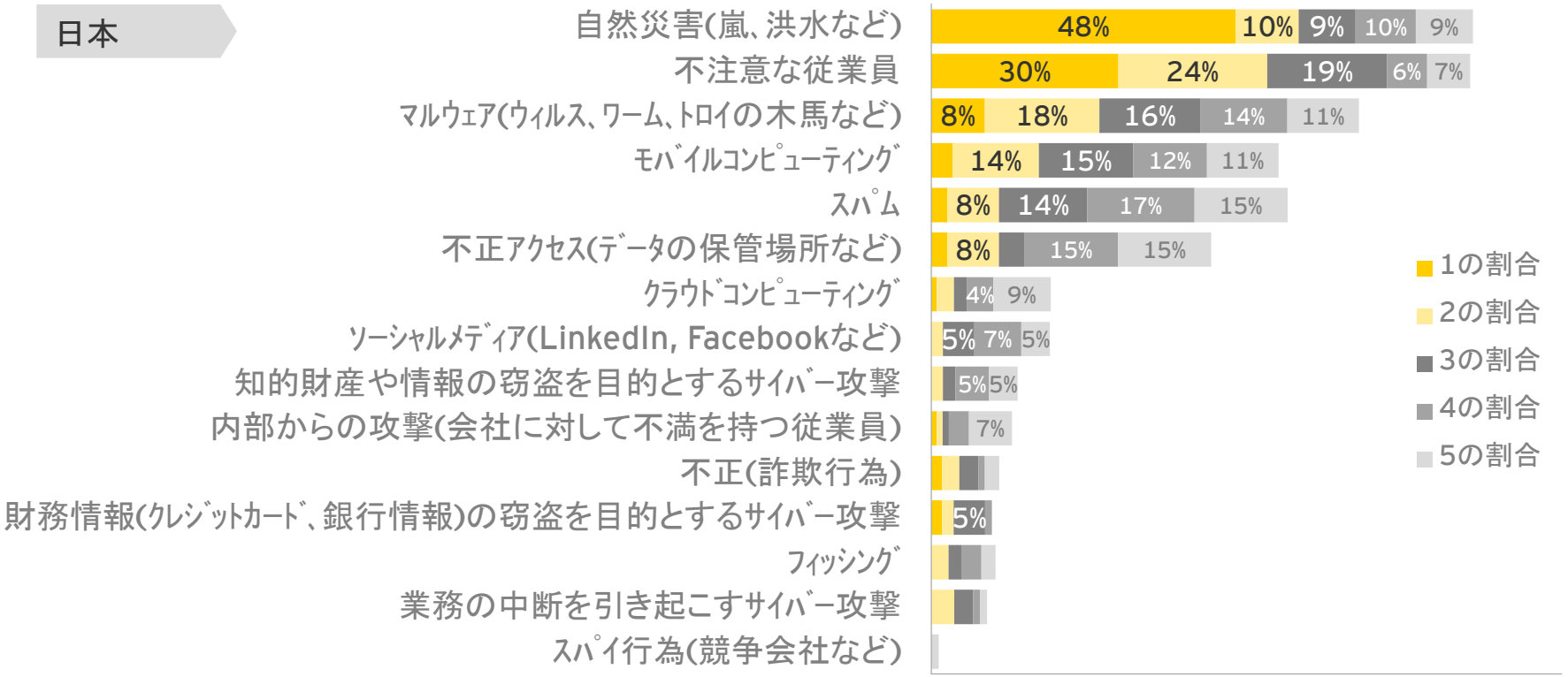


2.脅威、リスクと対策
2.2.a.脅威および脆弱性の影響度の傾向1

- 日本においては、多くの企業が自然災害のリスクが増大したと考えている
- 日本もグローバルも共に、不注意な従業員、マルウェア、モバイルコンピューティング、スパム、不正アクセスを脅威と認識している
- グローバルでは、「ソーシャルメディア（LinkedIn, Facebook）」、「フィッシング」などを脅威と考える企業が多い

Q5a.過去12ヵ月間に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と番号を記入ください。

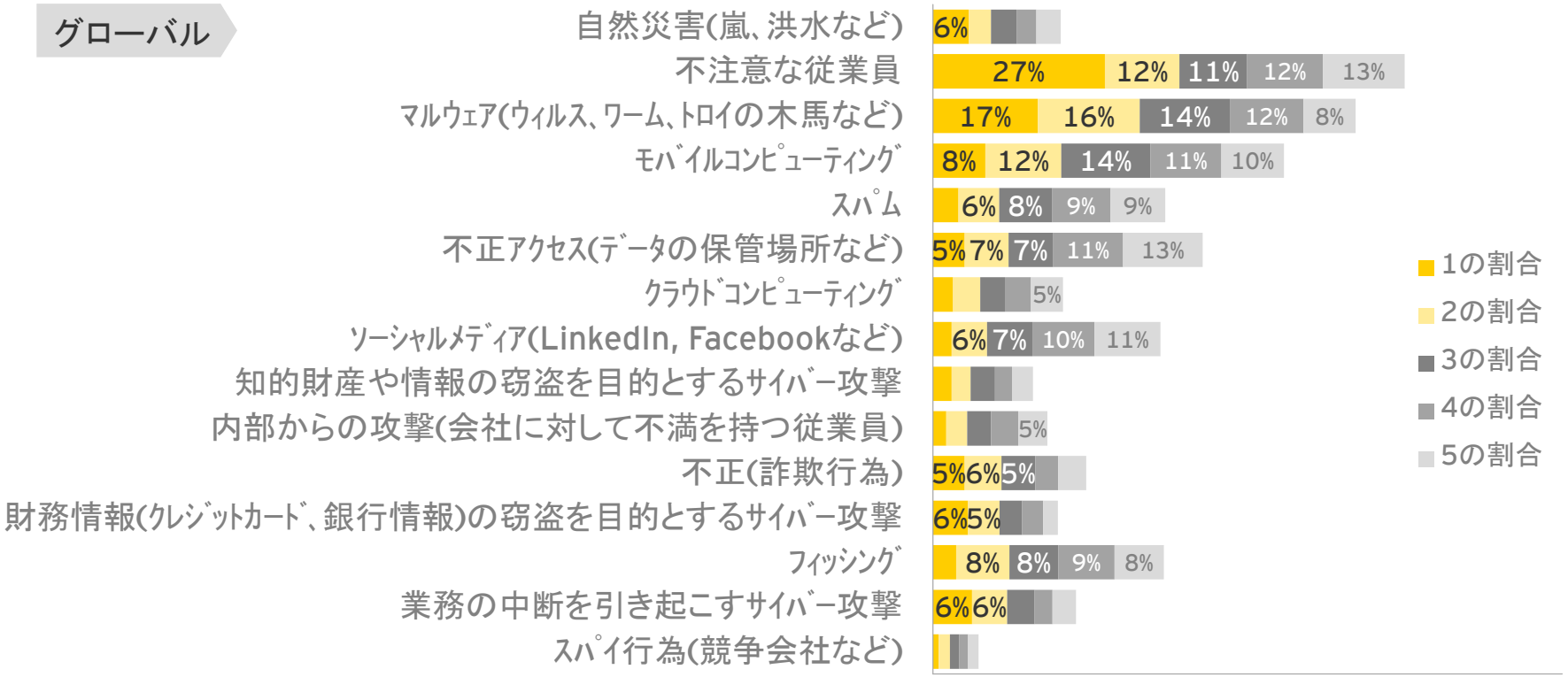
日本



2.脅威、リスクと対策
2.2.a.脅威および脆弱性の影響度の傾向2

Q5a.過去12ヵ月間に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と番号を記入ください。

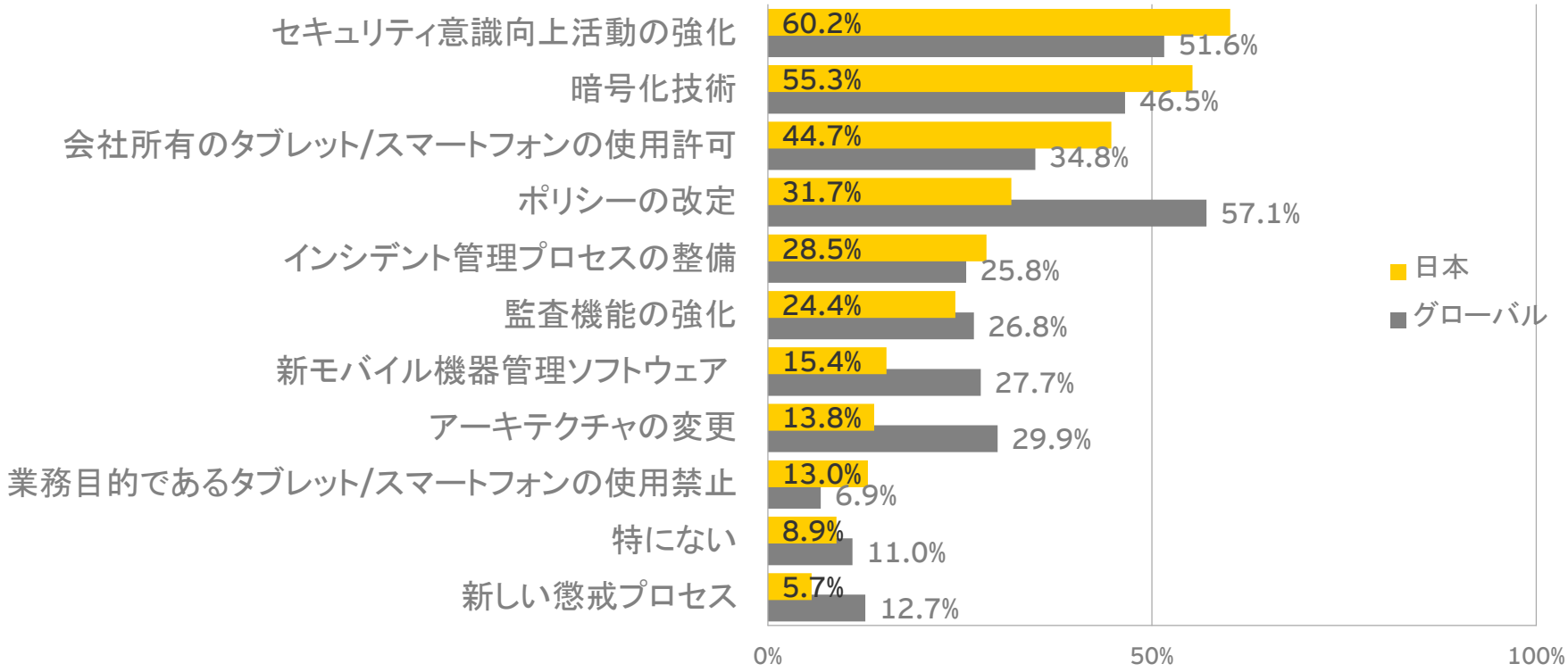
グローバル



2.脅威、リスクと対策
2.3.モバイルコンピューティングについて

- 日本もグローバルも共に、「セキュリティ意識向上活動の強化」、「暗号化技術」、「会社所有のモバイル使用許可」のコントロールを実施している。
- 日本は「ポリシーの改定」、「新モバイル管理ソフトウェア」、「アーキテクチャの変更」などの実施が少ない

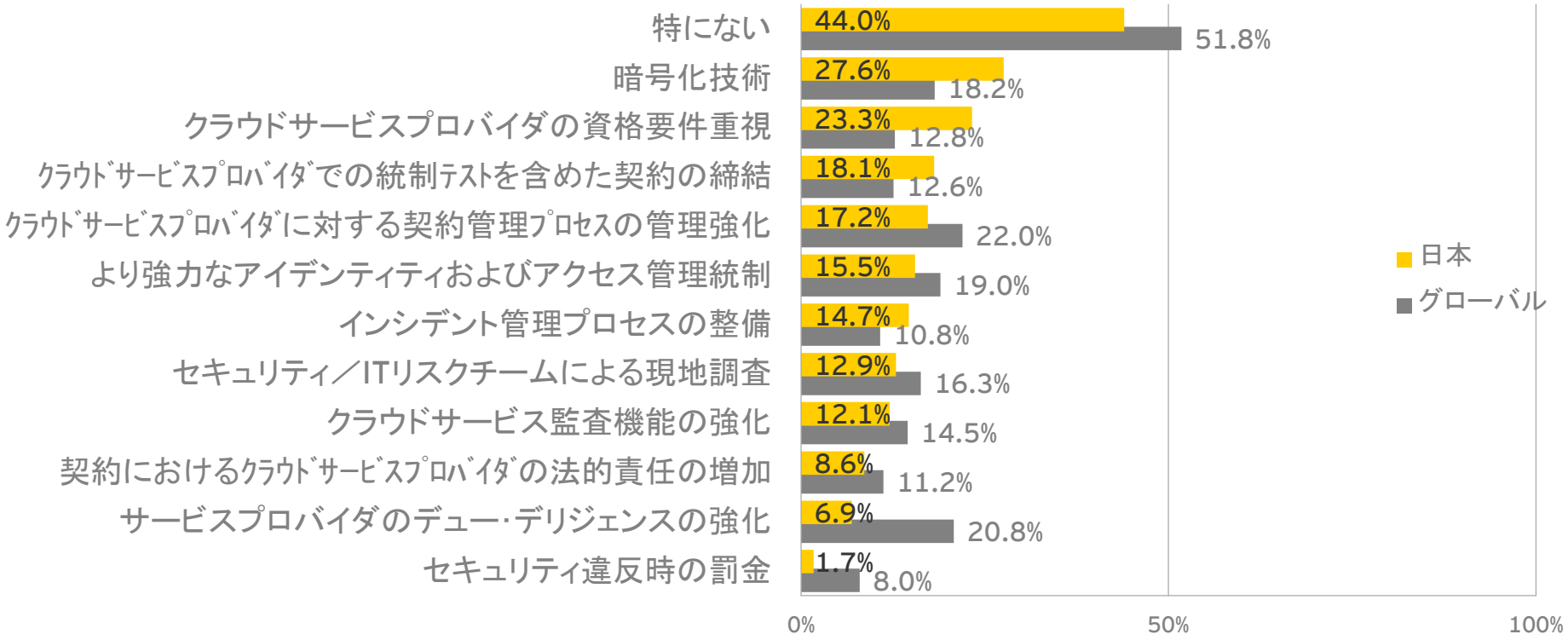
Q6.モバイルコンピューティングを利用する際、「新たな」または「増加する」リスクを低減するために実施しているコントロールについて、該当するものをすべて選択してください。



2.脅威、リスクと対策
2.3.a.クラウドコンピューティングについて

- 日本もグローバルも共に、半数程度の企業がクラウドに対するコントロールを整備していない
- 日本は、「暗号化技術」、「クラウドサービスプロバイダの資格要件」を重視している
- グローバルは、「クラウドサービスプロバイダに対する契約管理プロセスの管理強化」、「より強力なアイデンティティ及びアクセス管理統制」、「サービスプロバイダのデュー・デリジェンスの強化」を重視している

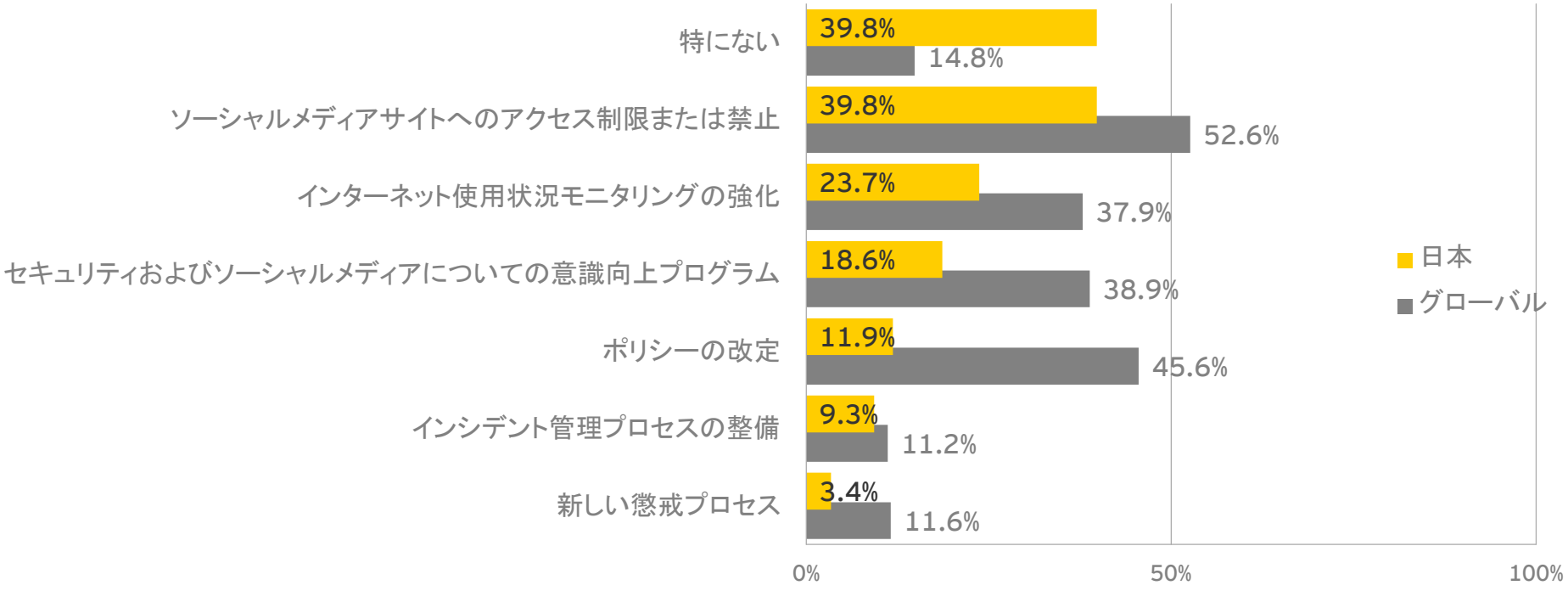
Q6a.クラウドコンピューティングを利用する際、「新たな」または「増加する」リスクを低減するために実施しているコントロールについて、該当するものをすべて選択してください。



2.脅威、リスクと対策
2.3.b.ソーシャルメディアについて

- 日本の40%の企業がソーシャルメディアに対するコントロールを実施していない（グローバル15%）
- グローバルでは、「ソーシャルメディアサイトへのアクセスの制限または禁止」、「インターネット使用状況のモニタリングの強化」、「セキュリティ及びソーシャルメディアについての意識向上プログラム」のすべての対策を4割から5割の企業が実施している（日本の割合はグローバルの半分程度）

Q6b.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。



3.ツールとテクノロジー

- グローバルではGRCツールを活用
- タブレットコンピュータの使用は限定的
- クラウドコンピューティングの利用状況
- グローバルで拡大するアクセス管理技術
- グローバルでの情報セキュリティツールの失敗
- 情報セキュリティツールの内訳
- 情報セキュリティツールの課題は運用プロセス
- 情報の漏えい防止技術の導入状況
- 日本は技術的セキュリティテストが少ない

3.ツールとテクノロジー 調査結果の概要

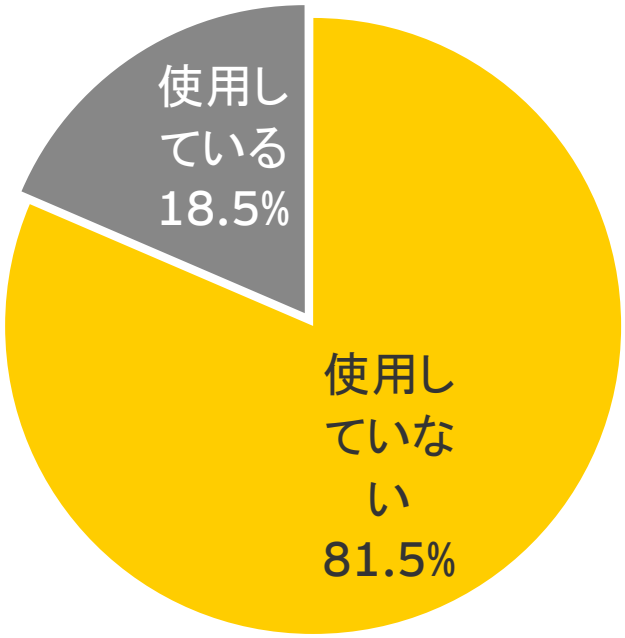
1. グローバルではGRCツールを活用
2. タブレットコンピュータの使用は限定的
   - グローバルで進むタブレットコンピュータの利用
   - 半数の企業は、タブレットコンピュータの利用について未だ検討中あるいは限定的利用
3. クラウドコンピューティングの利用状況
   - 3分の1の企業がクラウドコンピューティングを「使用中」、3分の1の企業が「検討中または計画中」、残りの3分の1の企業は「使用しない」
4. グローバルで拡大するアクセス管理技術
5. グローバルでの情報セキュリティツールの失敗
   - グローバルで高い失敗
6. 情報セキュリティツールの内訳
   - 日本もグローバルも共に、「情報セキュリティツールで失敗する内容は概ね同じであるが、グローバルは「ホストベースのセキュリティツールの失敗が多い
7. 情報セキュリティツールの課題は運用プロセス
8. 情報の漏えい防止技術の導入状況
   - グローバルのほうが、このような技術の導入に積極的
9. 日本は技術的セキュリティテストが少ない

3.ツールとテクノロジー
3.1.リスク管理プロセス支援ツールの使用状況

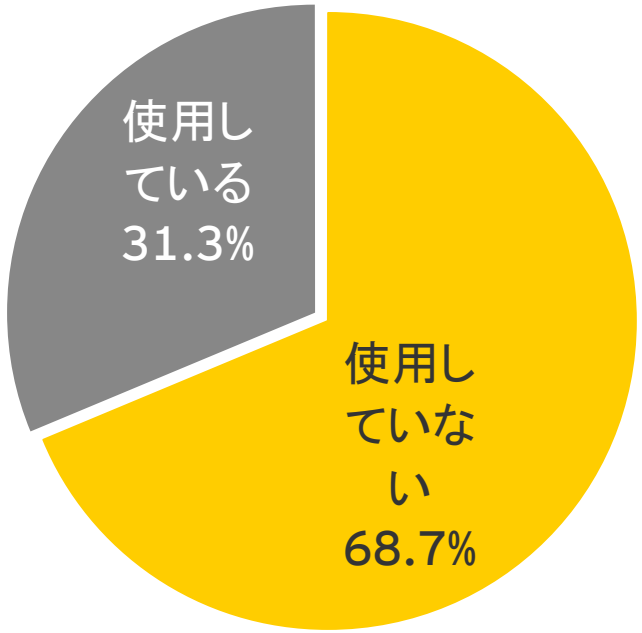
- GRCツールの活用は、グローバル3割、日本2割と、日本が遅れている

Q7.全社的リスク管理、ITリスク管理、情報セキュリティリスク管理、またはGRC（ガバナンス・リスク・コンプライアンス）といったプロセスを支援するための技術ツールを使用していますか?

日本



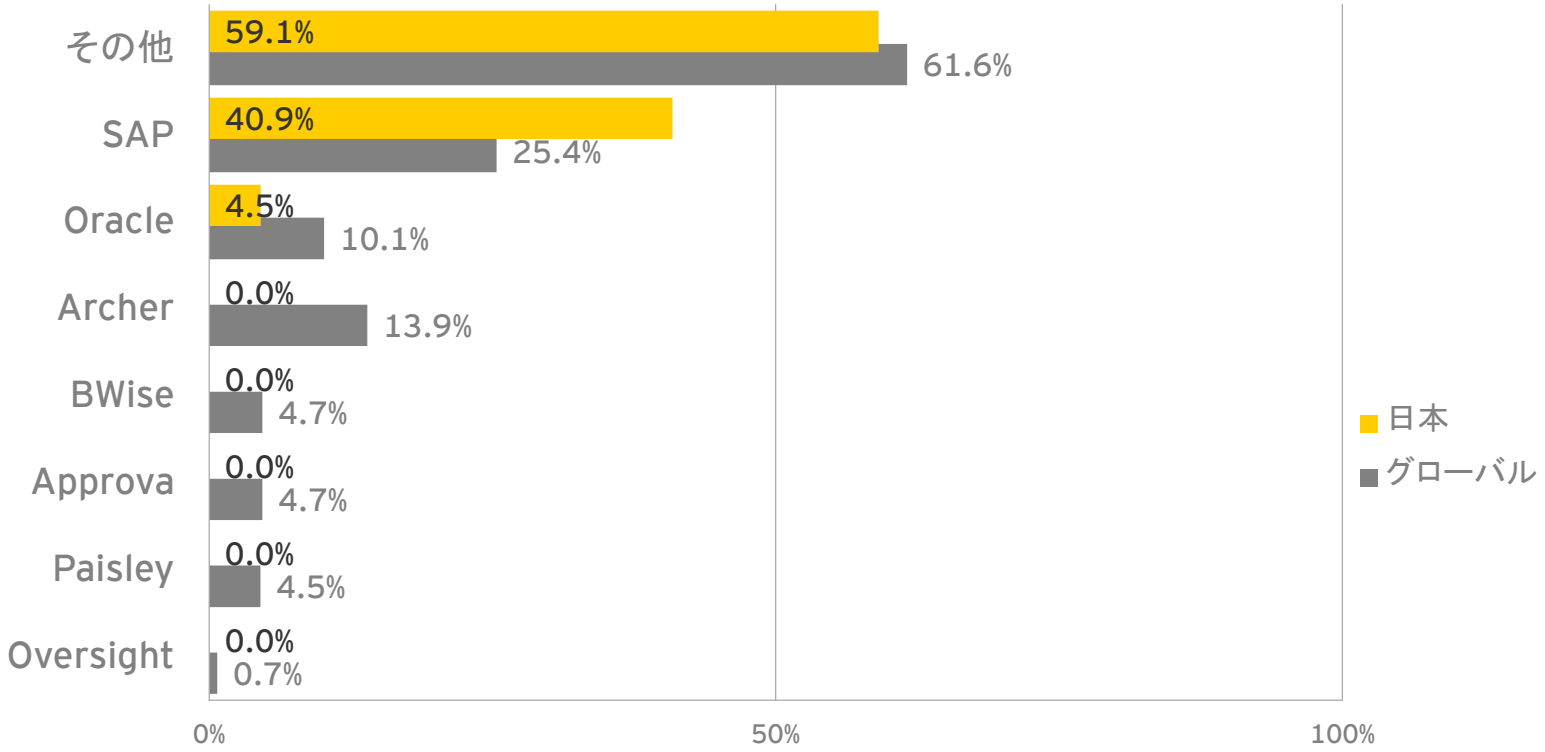
グローバル



3.ツールとテクノロジー
3.1.a.使用しているGRCツールの内訳

- 日本もグローバルも共に、GRCツールとしてSAPを利用している企業が多い

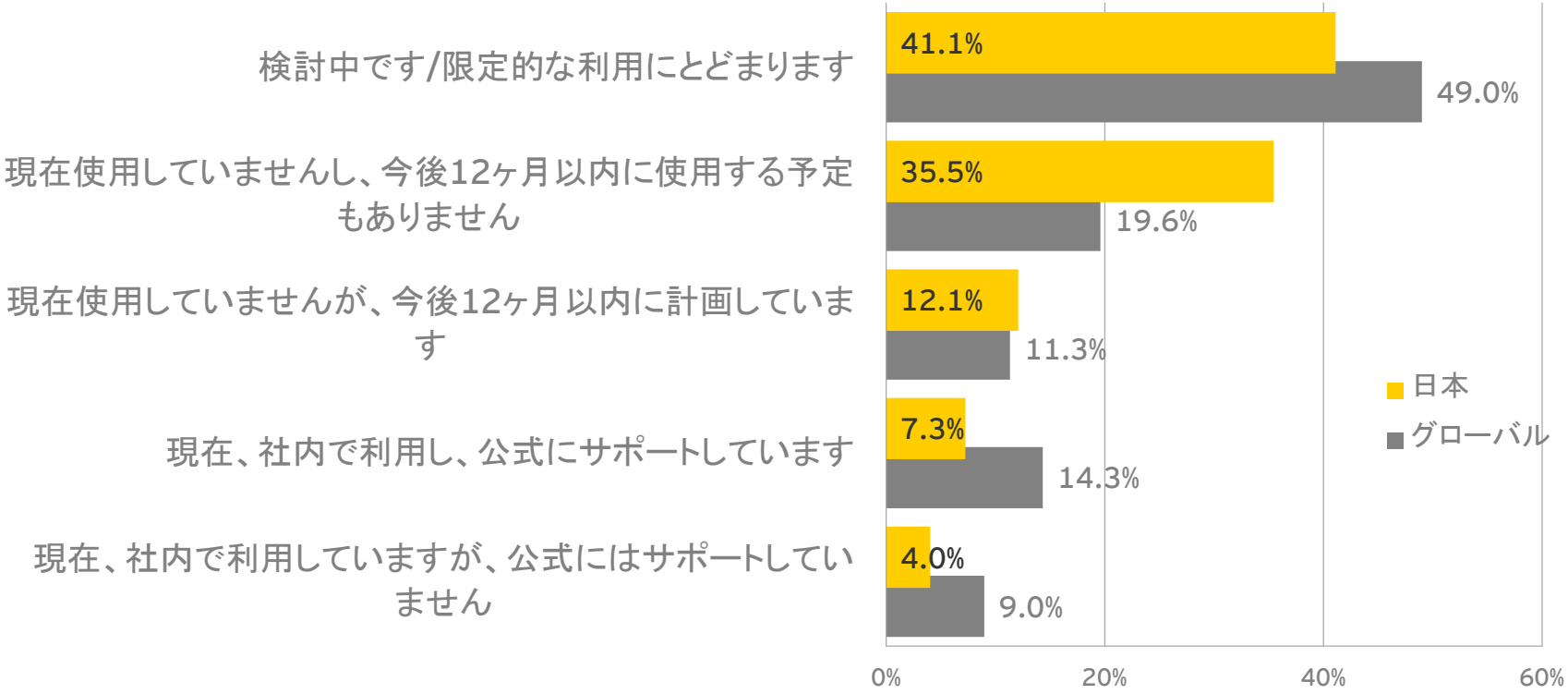
Q7a.現在貴社で使用しているGRC（ガバナンス・リスク・コンプライアンス）ツールについて、該当するものをすべて選択してください。（Q7で[GRCを利用している]と回答した方のみ回答）



3.ツールとテクノロジー
3.2.タブレットコンピュータの使用許可状況

- タブレットコンピュータの使用を検討中または限定的な利用にとどめている企業が多く、日本で4割, グローバルでは5割
- 「社内で利用し、公式にサポートしている企業」は少なく、日本7%, グローバル14%

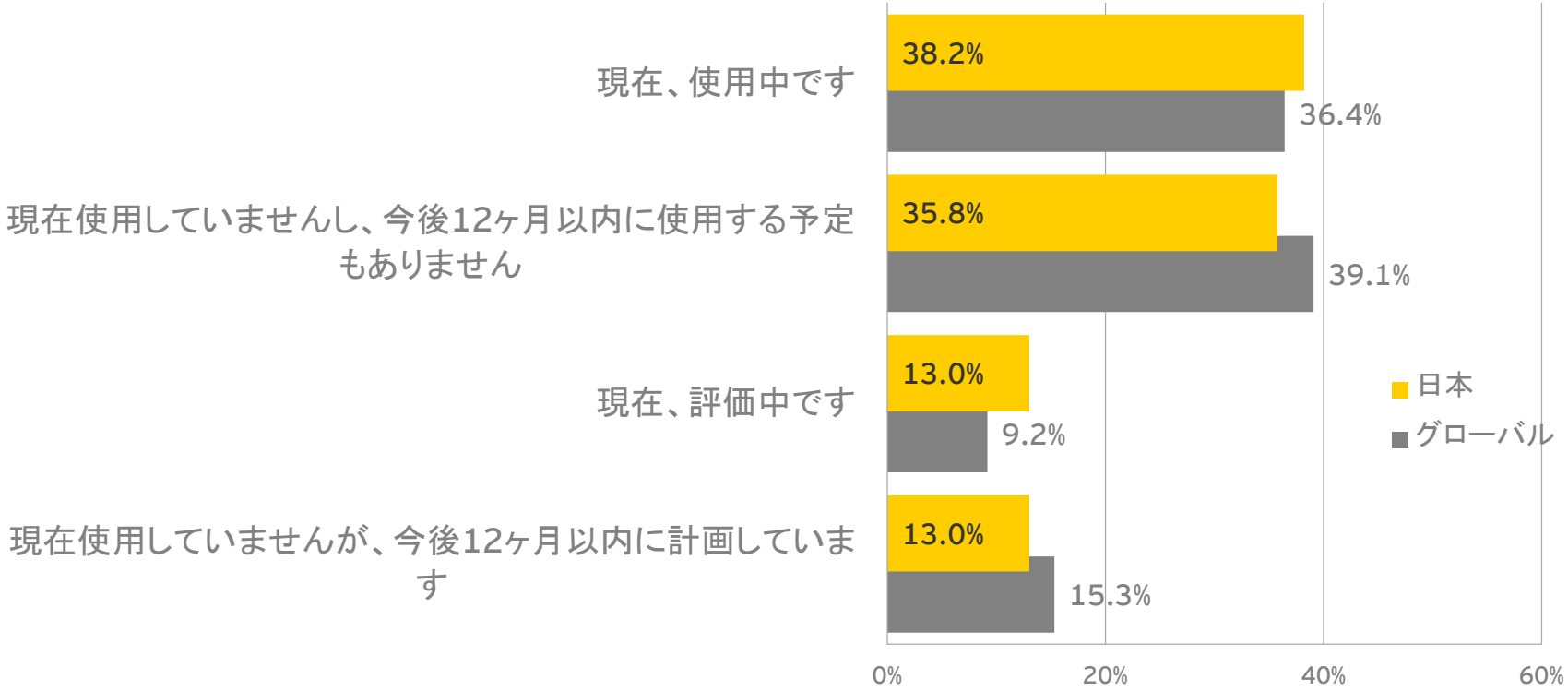
Q8.現在業務目的でタブレットコンピュータの使用を許可していますか?該当するものを1つ選択してください。



3.ツールとテクノロジー
3.3.クラウドコンピューティングの利用状況

- 日本もグローバルも共に、3分の1の企業がクラウドコンピューティングを「使用中」、3分の1の企業が「検討中または計画中」、残りの3分の1の企業は「使用しない」

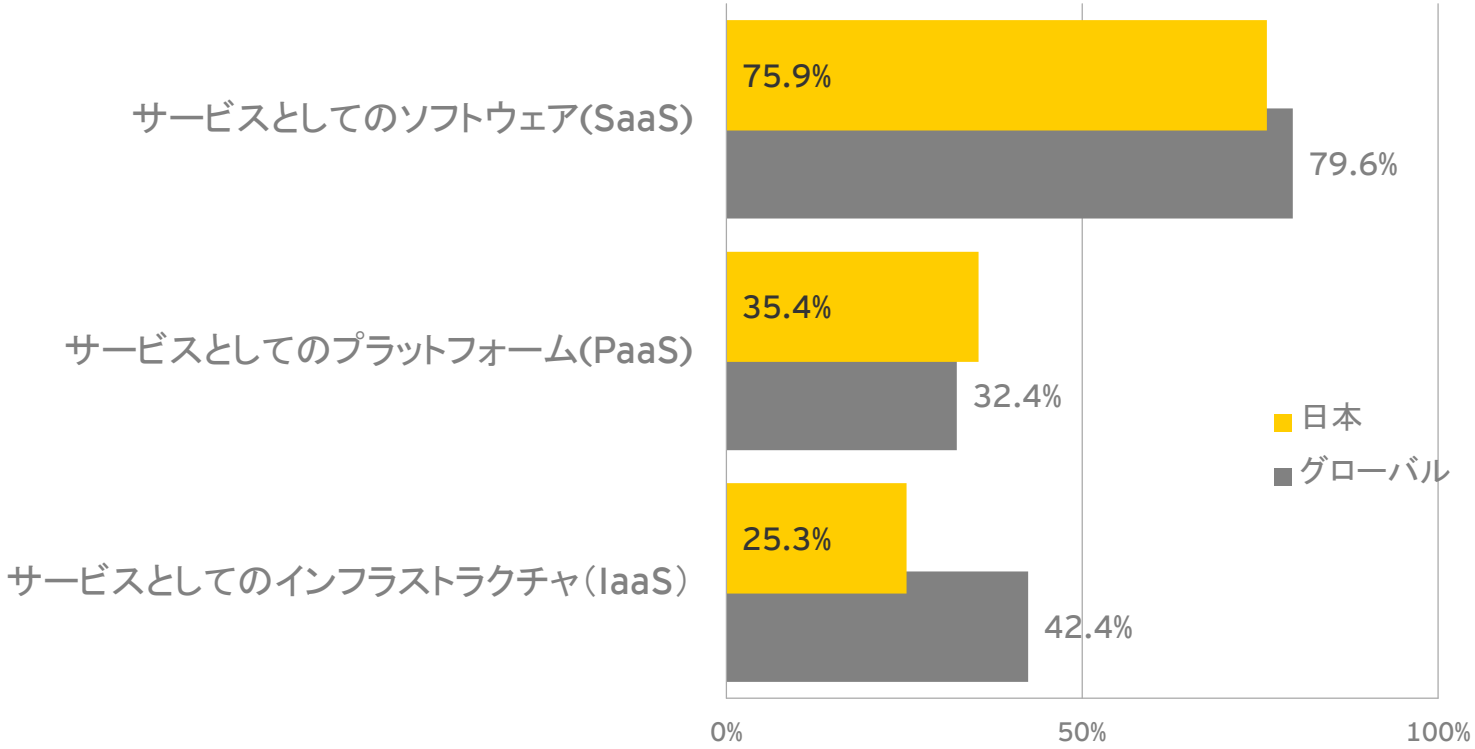
Q9.現在クラウドコンピューティングベースのサービスを使用していますか?該当するものを1つ選択してください。



3.ツールとテクノロジー
3.3.a.クラウドコンピューティングの利用状況

- クラウドサービスの利用は、SaaSが多い
- IaaSの利用は、日本25%, グローバル42%と、グローバルの方が利用が多い

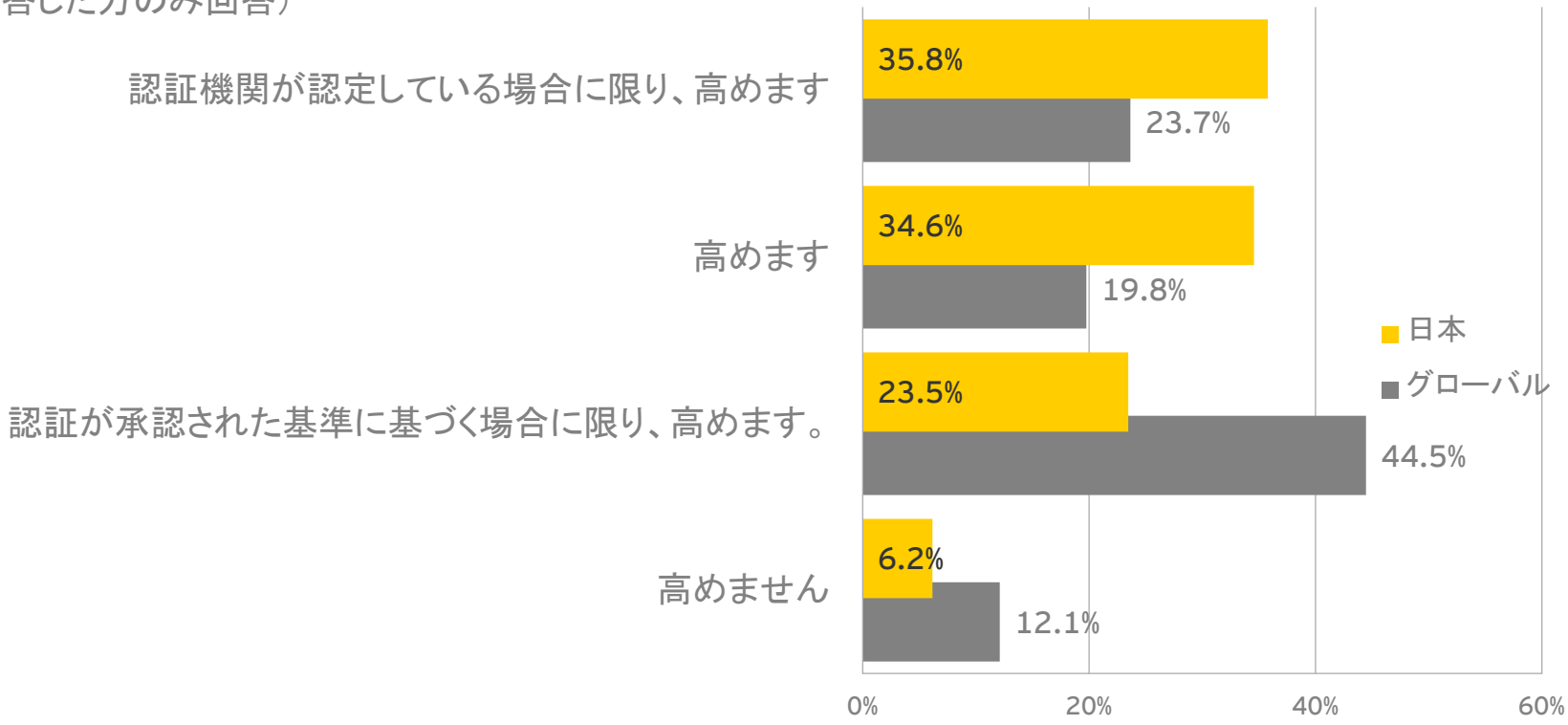
Q9a.現在利用中、または計画中のクラウドサービスの種類について、該当するものをすべて選択してください。
（Q9で[クラウドサービスを利用中/評価中/計画中]と回答した方のみ回答）



3.ツールとテクノロジー
3.3.b.クラウドサービスプロバイダの信頼性

- 日本は、認証機関の認定を重視する（日本36%, グローバル24%）
- グローバルは、「どのような基準に基づいた認証か」を重視する（日本24%, グローバル45%）

Q9b.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。（Q9で[クラウドサービスを利用中/評価中/計画中]と回答した方のみ回答）

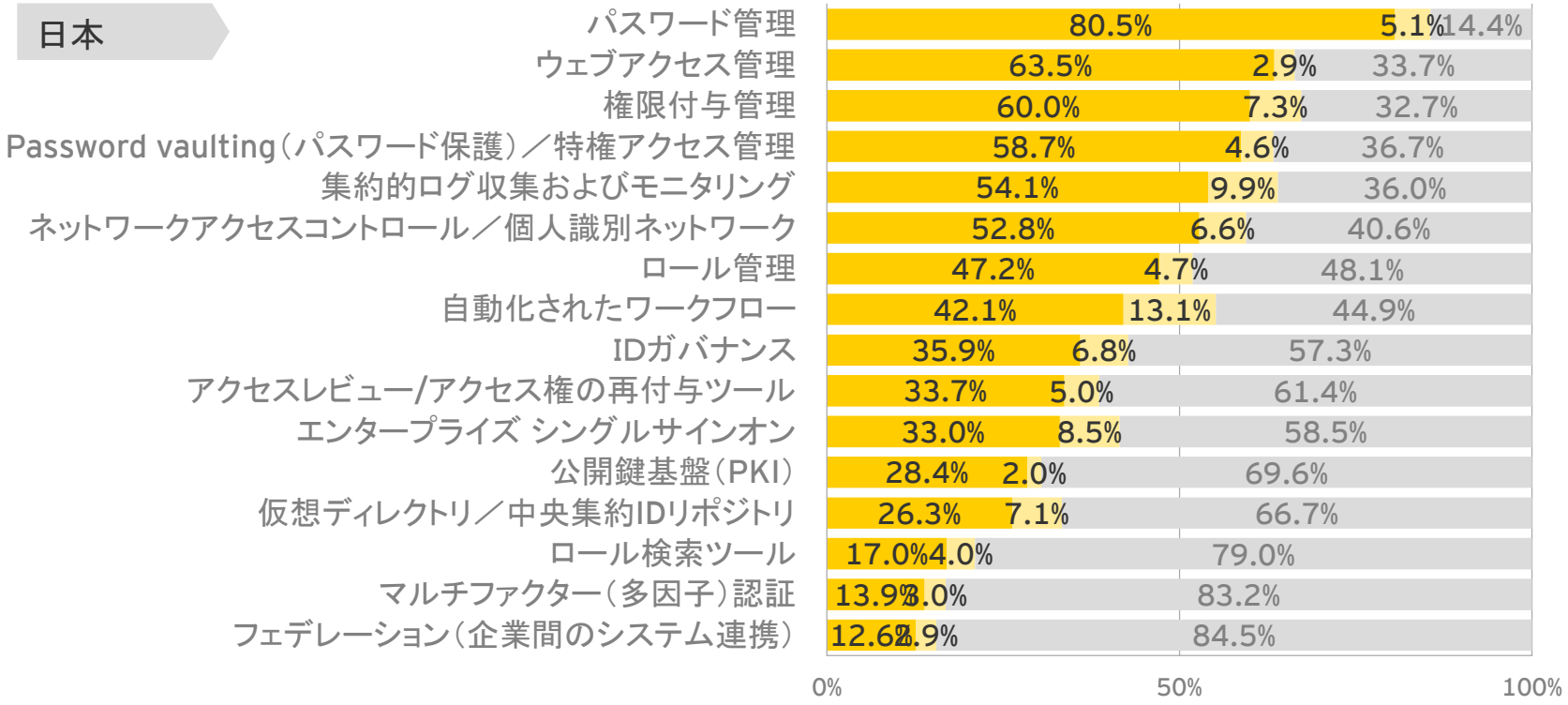


3.ツールとテクノロジー
3.4.アクセス管理技術の導入状況1

- アクセス管理技術の利用は、日本もグローバルも共に高い
- 1年以内に導入する割合は、グローバルで高く、日本はこのような技術の導入が遅れている

Q10.現在利用している、または導入予定のアイデンティティ/アクセス管理技術について、該当するものをすべて選択してください。

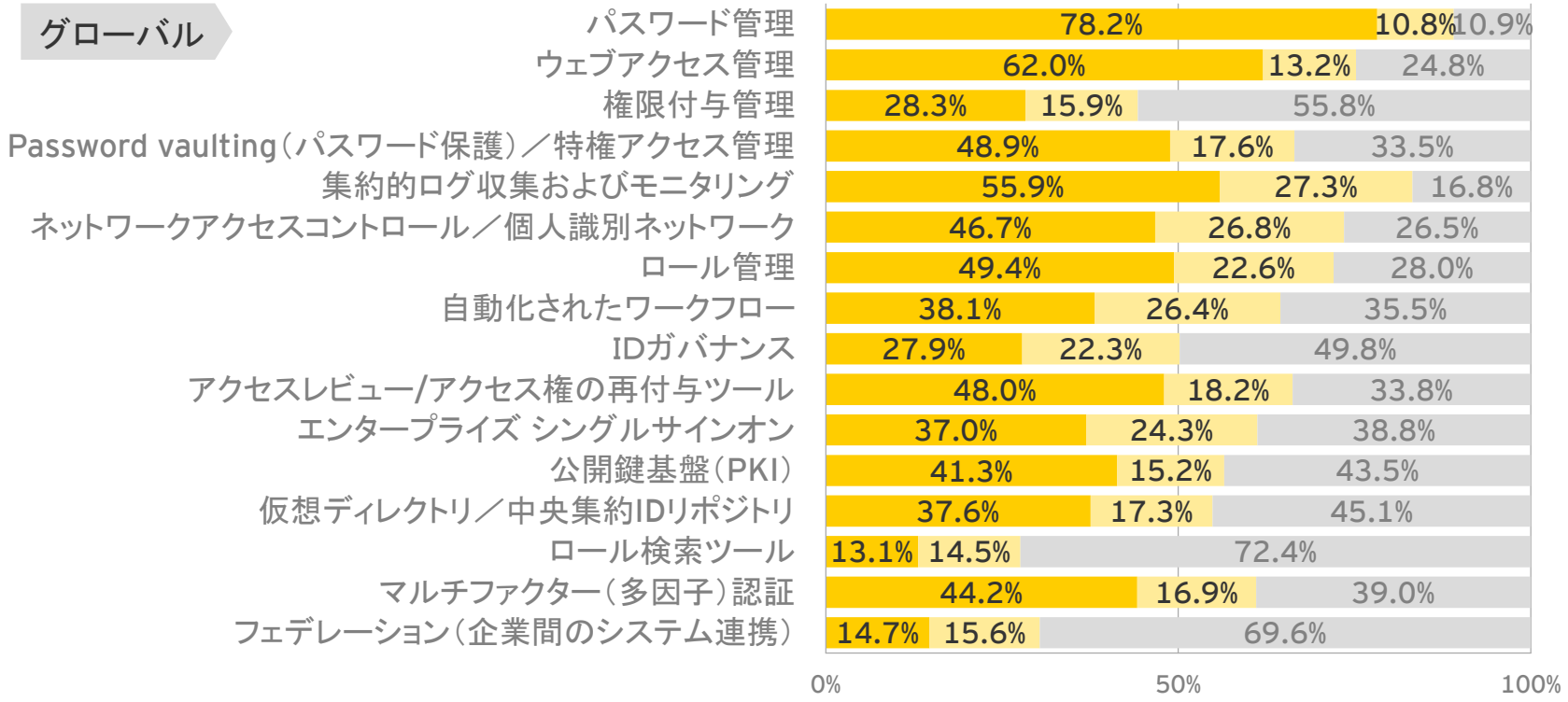
日本



3.ツールとテクノロジー
3.4.アクセス管理技術の導入状況2

Q10.現在利用している、または導入予定のアイデンティティ/アクセス管理技術について、該当するものをすべて選択してください。

グローバル

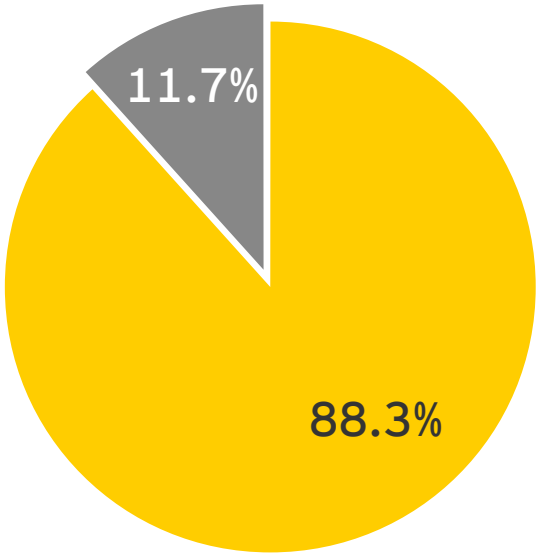


3.ツールとテクノロジー
3.5.情報セキュリティツールの導入プロセス

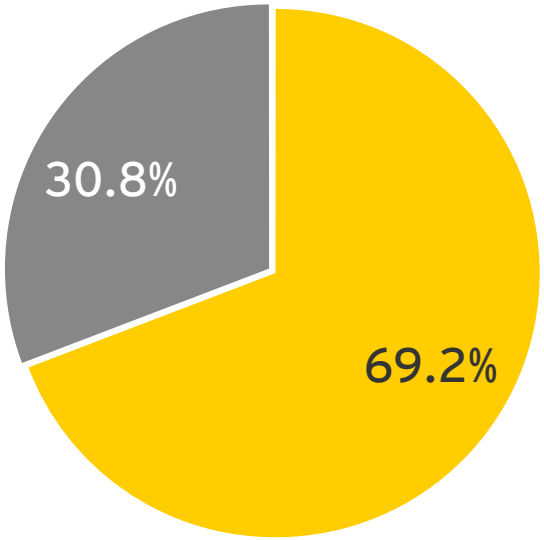
- 情報セキュリティツールの導入は、グローバルの方が失敗する割合が高い

Q11.過去18ヶ月に購入した、情報セキュリティをサポートするソフトウェアおよび/またはハードウェアで失敗したと感じたものはありましたか?該当するものを1つ選択してください。

日本



グローバル

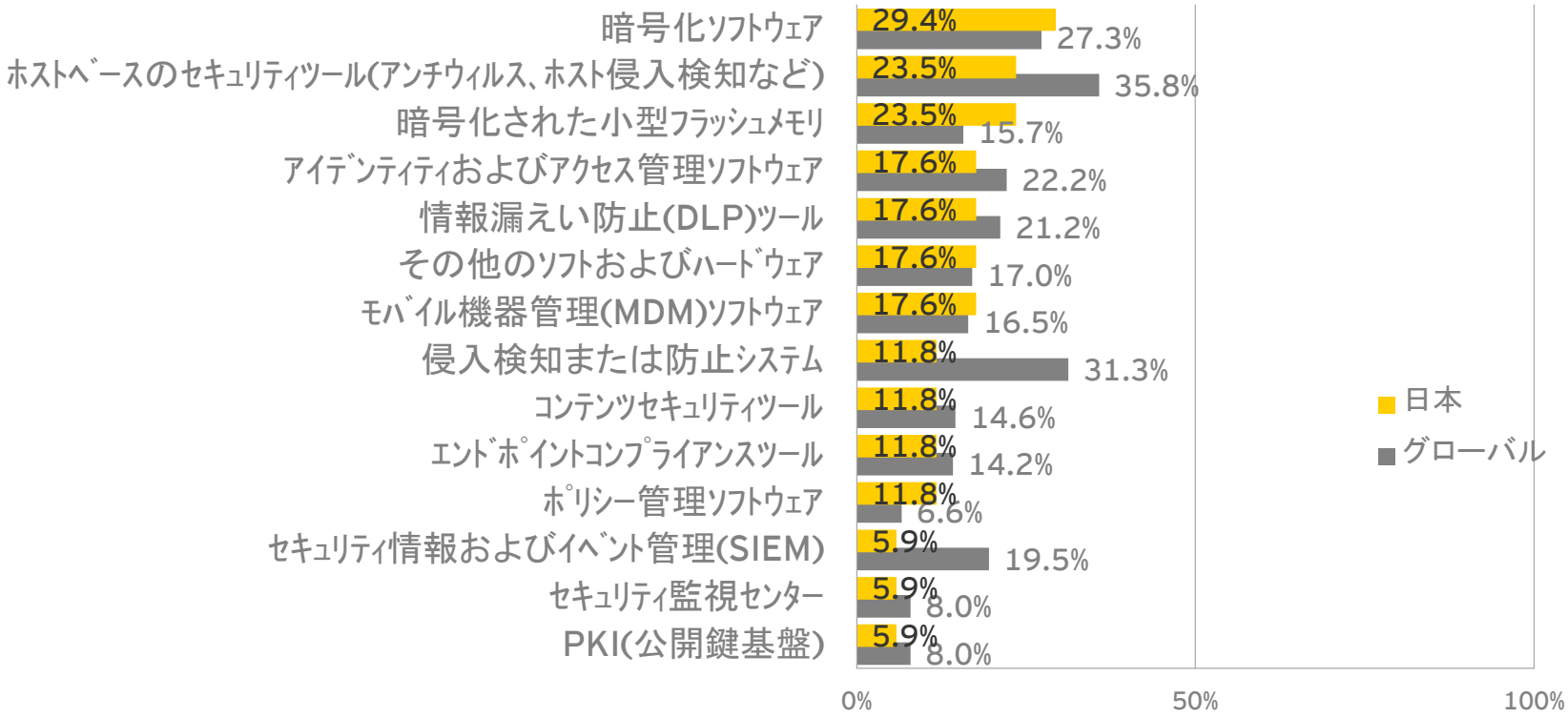


■ありません。情報セキュリティ技術はすべて適切に実装されています。 ■ありました

3.ツールとテクノロジー
3.5.a.情報セキュリティツールの内訳

- 日本もグローバルも共に、情報セキュリティツールで失敗する内容は同じ
- グローバルは、「ホストベースのセキュリティツール（アンチウィルス、ホスト侵入検知など）」や「侵入検知または防止システム」の失敗が多い

Q11a.それはどのようなソフトウェアまたはハードウェアですか？ 該当するものをすべて選択してください。（Q9で[情報セキュリティ・ソフトウェアで失敗したと感じたものがあった]と回答した方のみ回答）

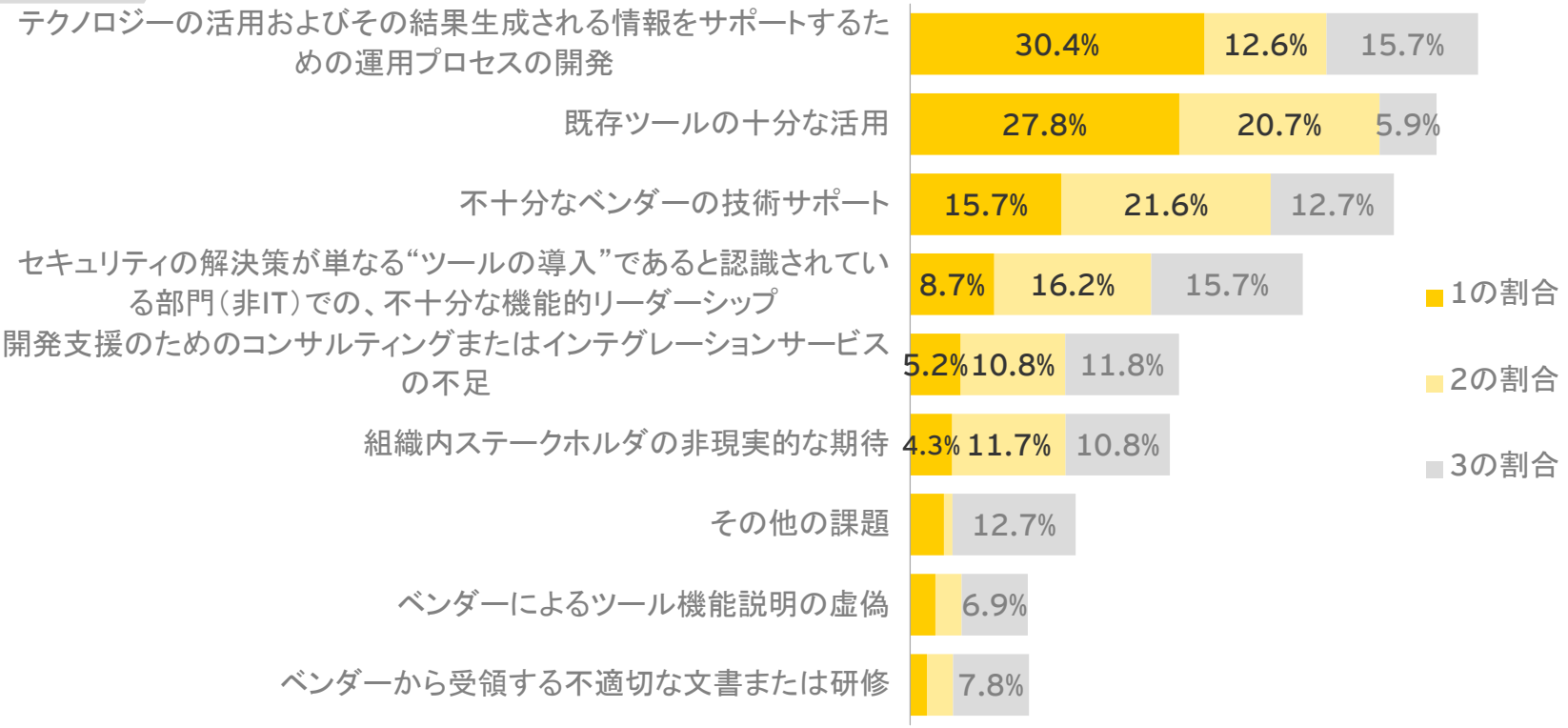


3.ツールとテクノロジー
3.5.b.情報セキュリティツールの課題1

- 日本もグローバルも共に、1位「テクノロジーの活用及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」、2位「既存ツールの十分な活用」が課題
- 日本は、「不十分なベンダーの技術サポート」を課題として認識している

Q11b.新しいツールやテクノロジーの課題について、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。

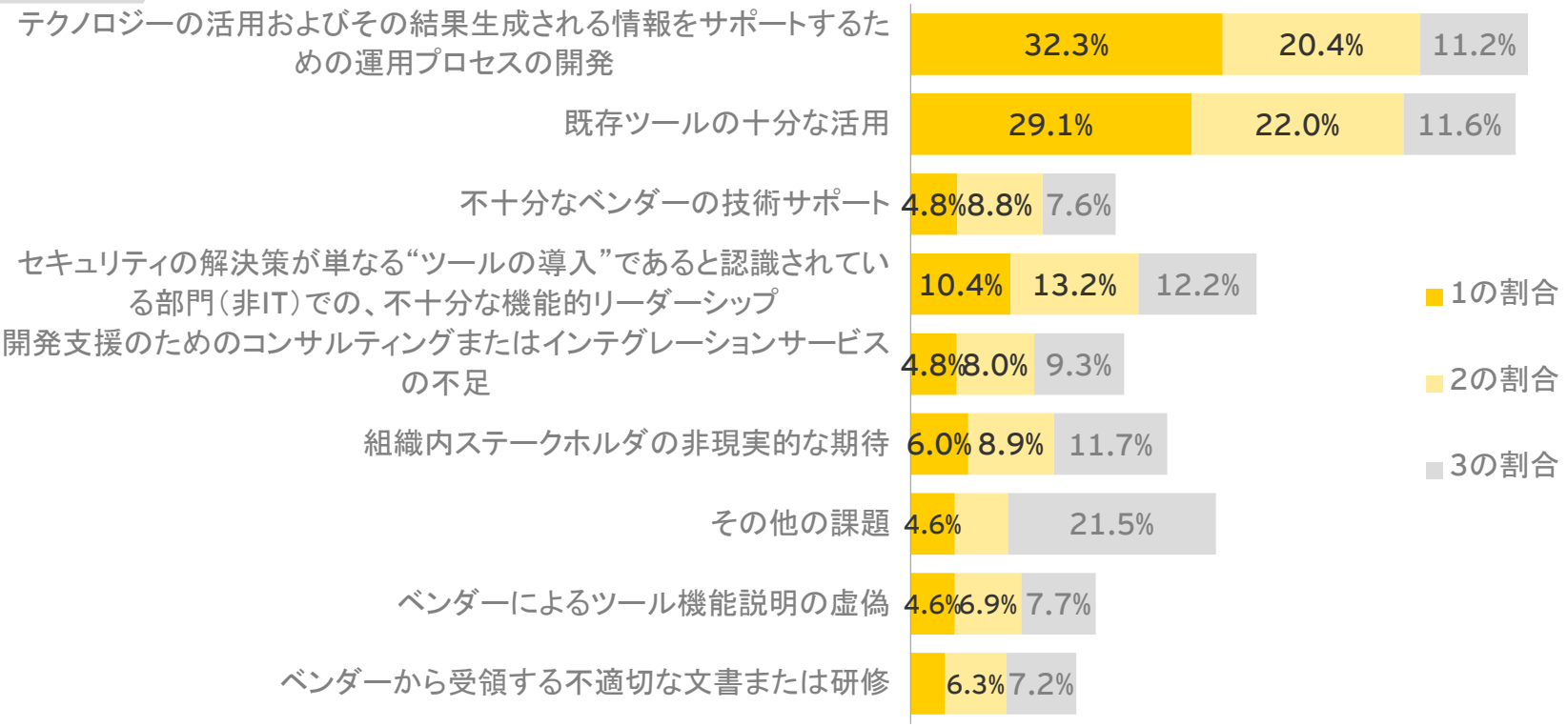
日本



3.ツールとテクノロジー
3.5.b.情報セキュリティツールの課題2

Q11b.新しいツールやテクノロジーの課題について、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。

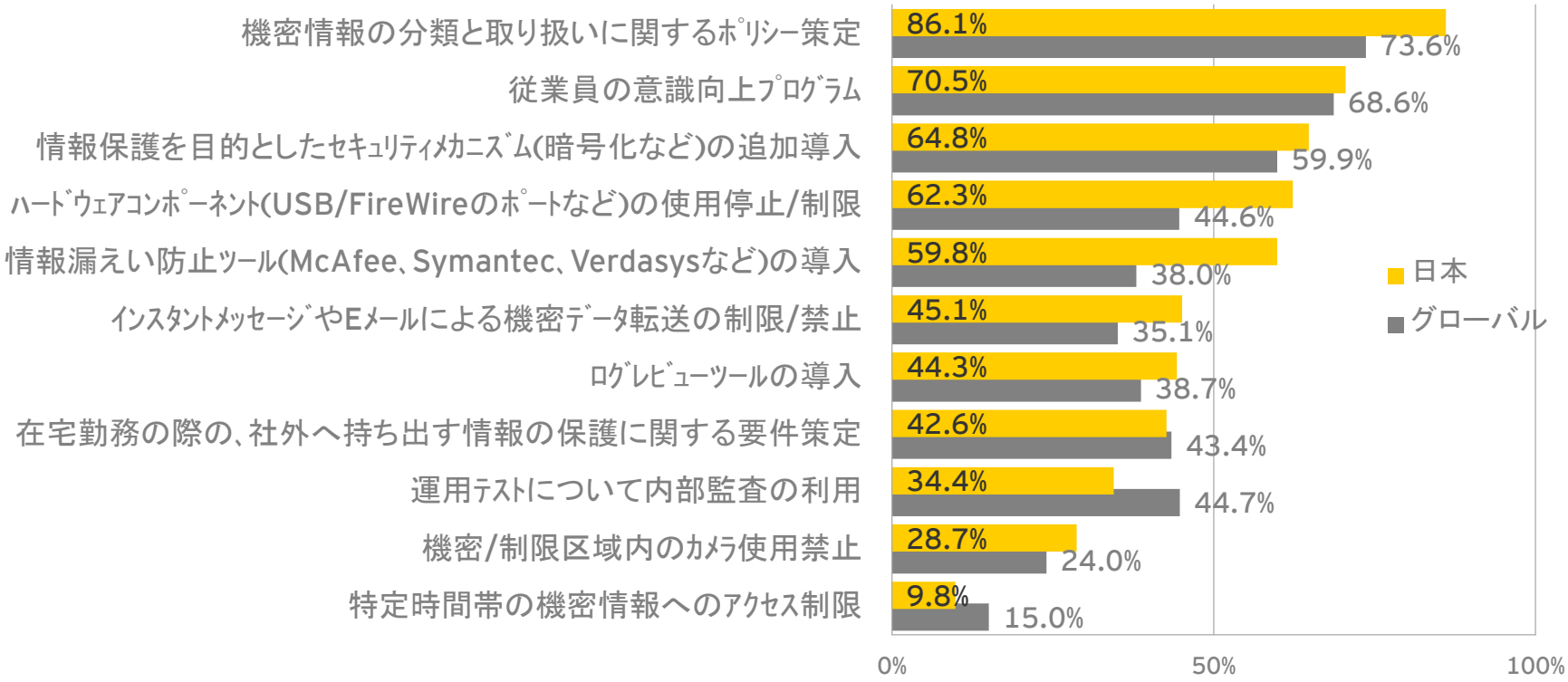
グローバル



3.ツールとテクノロジー
3.6.機密情報漏えい防止対策

- 日本もグローバルも共に、同様の対策をとっている

Q12.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。

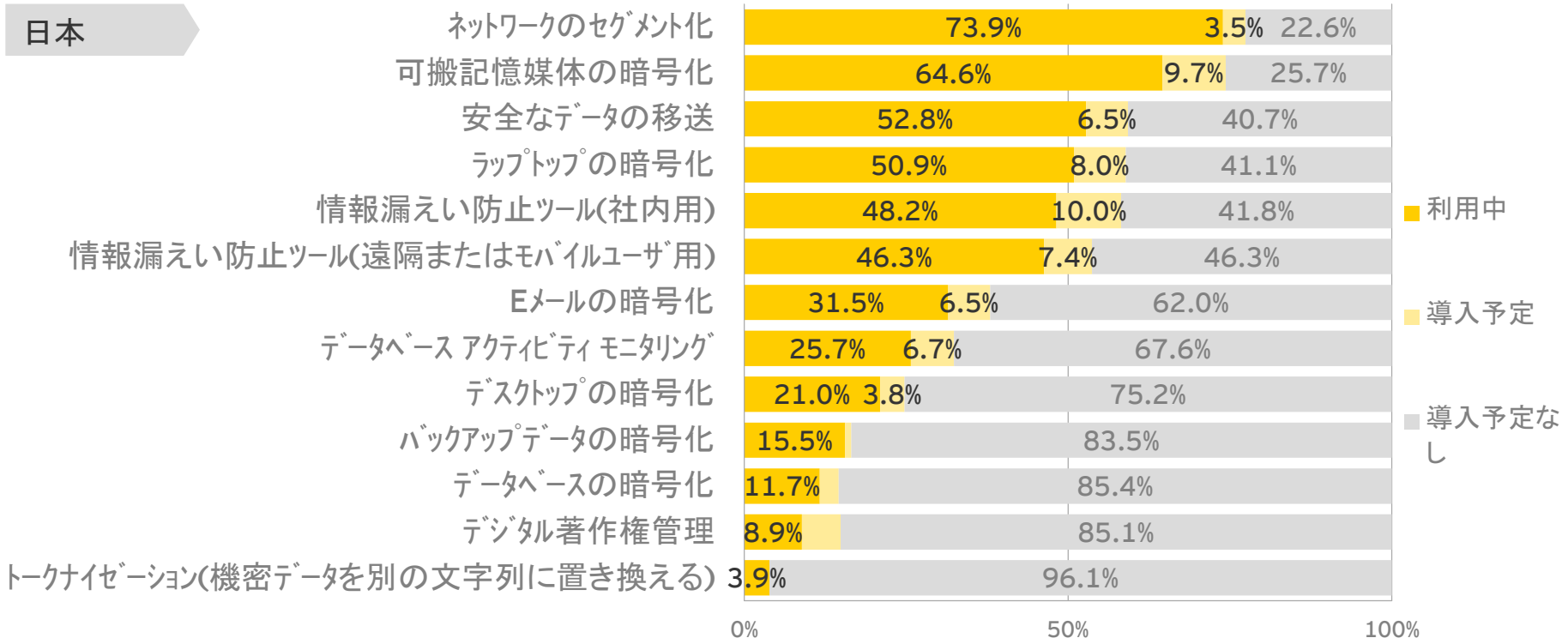


3.ツールとテクノロジー
3.7.情報漏えい防止技術の導入状況1

- 日本もグローバルも共に、情報漏えい防止技術を利用している
- グローバルでは、このような技術を積極的に活用する傾向がある（導入予定が高い）
- 日本は、「バックアップデータの暗号化」、「データベースの暗号化」、「トークナイゼーション」の活用が低い

Q13.現在利用している、または導入予定の情報漏えい防止技術について、該当するものをすべて選択してください。

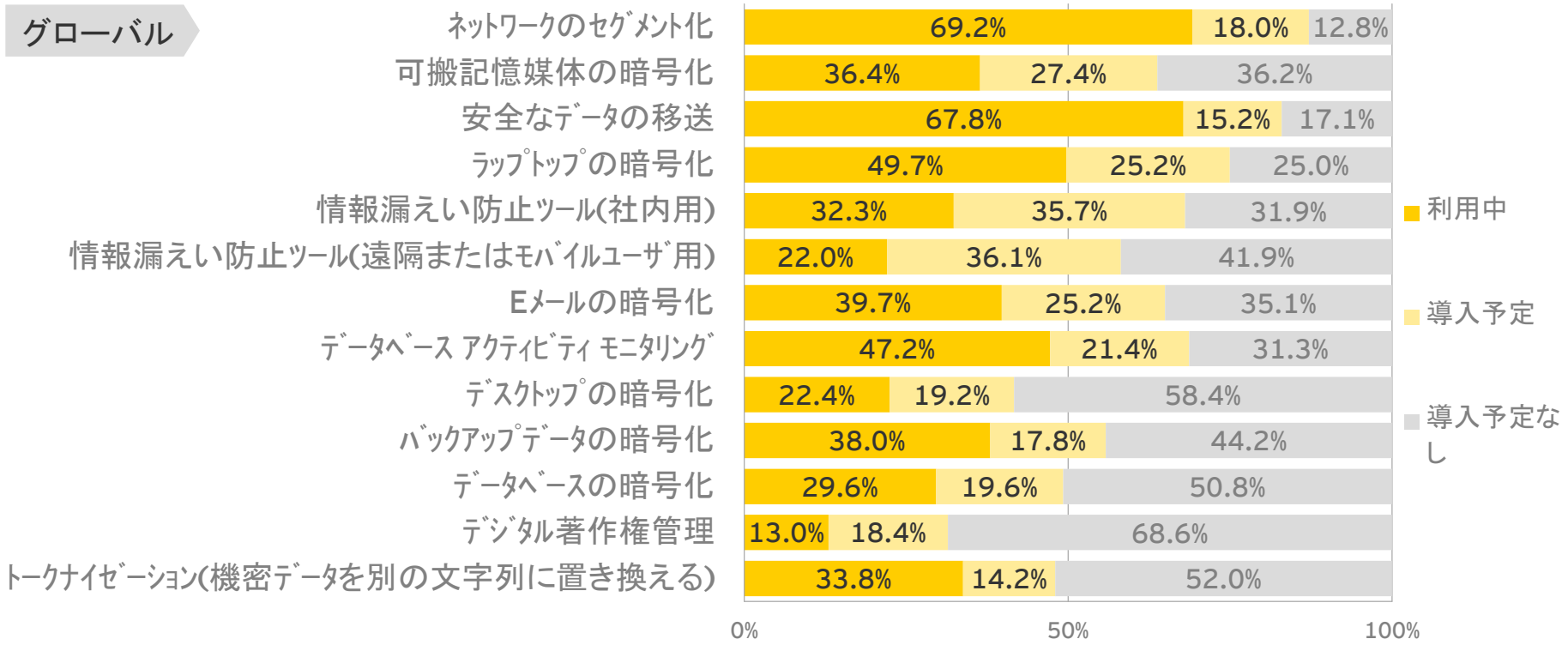
日本



3.ツールとテクノロジー
3.7.情報漏えい防止技術の導入状況2

Q13.現在利用している、または導入予定の情報漏えい防止技術について、該当するものをすべて選択してください。

グローバル



3.ツールとテクノロジー
3.8.情報漏えい防止ツールの利用状況1

- 日本もグローバルも共に、情報漏洩防止ツールを利用している
- グローバルでは、積極的に活用する傾向がある（導入予定が高い）

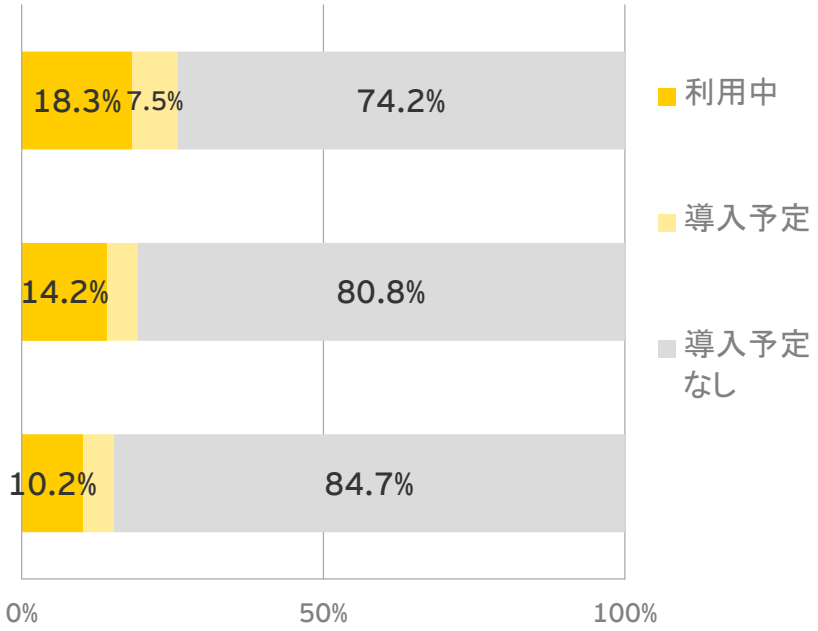
Q14.“情報漏えい防止（DLP）”とは、情報がどのように使用（場合によっては悪用）されているかを検出することができるツールの名称で、McAfee, Symantec, Verdasys, RSAといったベンダーから製品が提供されています。該当するものをすべて選択してください。

日本

実行データ：エンドユーザのPC内にあるツールで、情報が不適切に使用された場合警告を発する／ブロックする。

データの使用：ネットワークに設置するツールでネットワーク内のデータ伝送をスキャンする

保存データ：レポジトリをスキャンするツールで、適切なアクセス制御なく保存されているデータをスキャンする。



3.ツールとテクノロジー
3.8.情報漏えい防止ツールの利用状況2

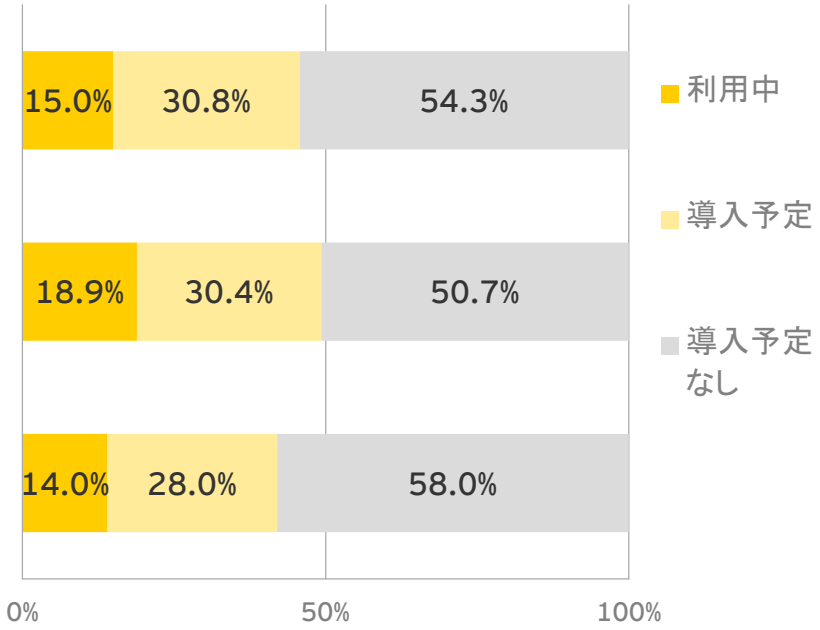
Q14.“情報漏えい防止（DLP）”とは、情報がどのように使用（場合によっては悪用）されているかを検出することができるツールの名称で、McAfee, Symantec, Verdasys, RSAといったベンダーから製品が提供されています。該当するものをすべて選択してください。

グローバル

実行データ：エンドユーザのPC内にあるツールで、情報が不適切に使用された場合警告を発する／ブロックする。

データの使用：ネットワークに設置するツールでネットワーク内のデータ伝送をスキャンする

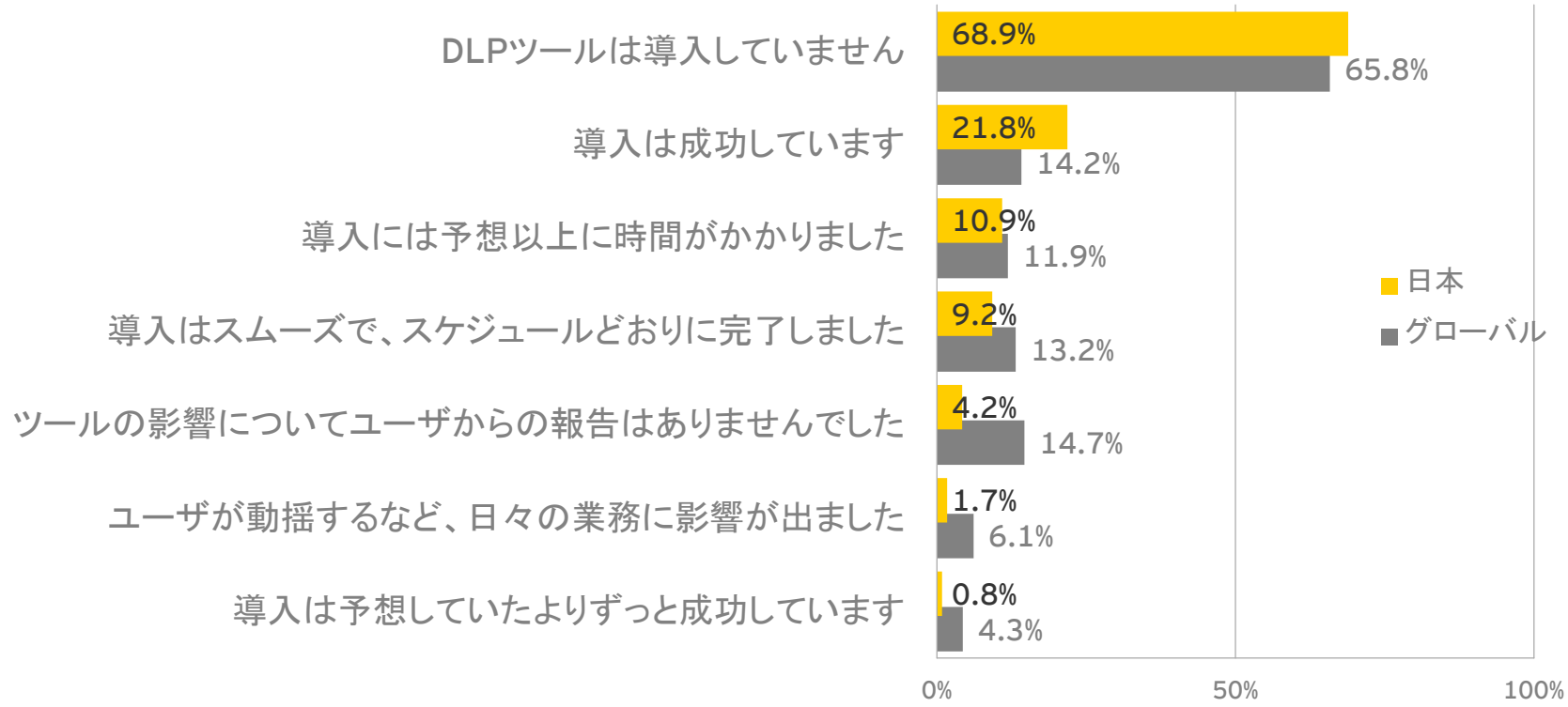
保存データ：レポジトリをスキャンするツールで、適切なアクセス制御なく保存されているデータをスキャンする。



3.ツールとテクノロジー
3.9.アクセス権管理プログラムの使用状況

- 日本もグローバルも共に、DLPツールの導入はまだ少ない

Q15.社内のシステムやデータに対するアクセス権のリスクに対応するため、アイデンティティ/アクセス管理プログラムを使用していますか？ 該当するものをすべて選択してください。

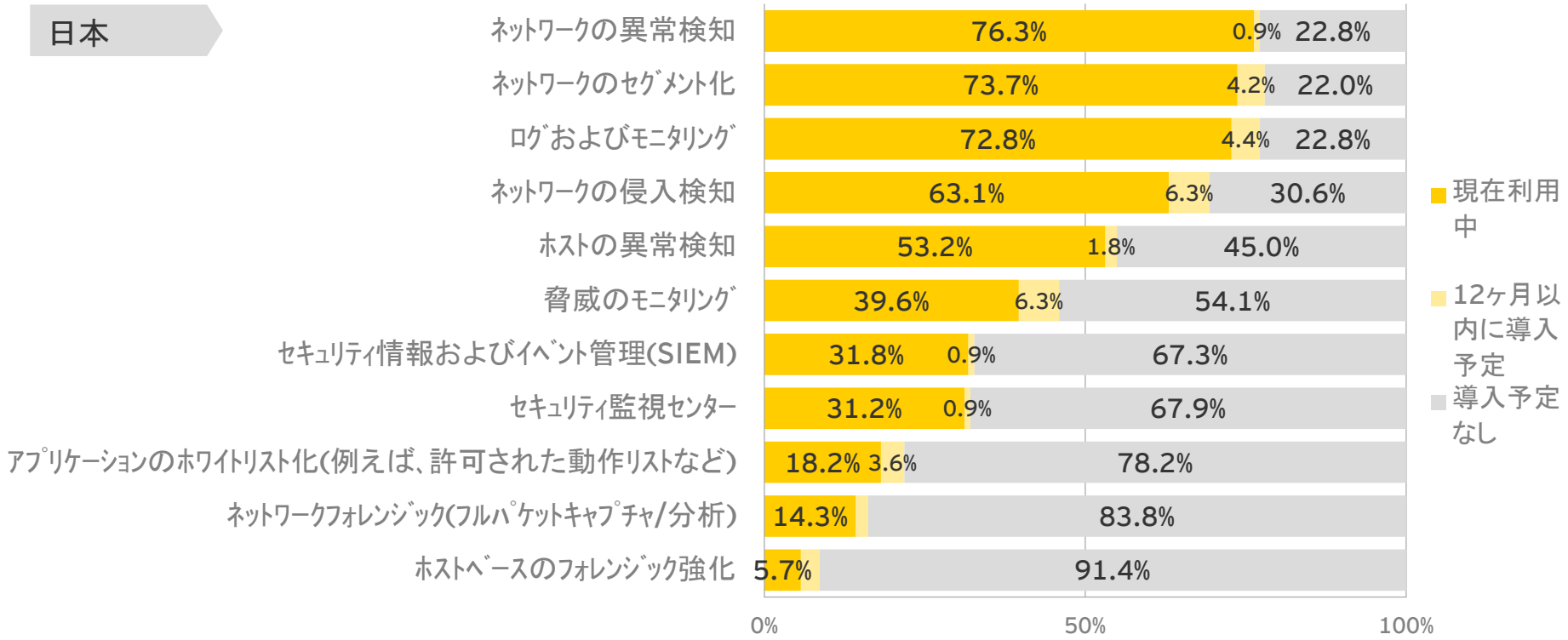


3.ツールとテクノロジー
3.10.外部からの攻撃に対する技術1

- 日本もグローバルも共に、外部からの攻撃に対する技術を導入している
- グローバルでは、このような技術を積極的に活用する傾向がある（導入予定が高い）

Q16.外部からの攻撃を防ぎ、検知し、対応するために、現在利用中のまたは導入予定の技術はありますか？該当するものをすべて選択してください。

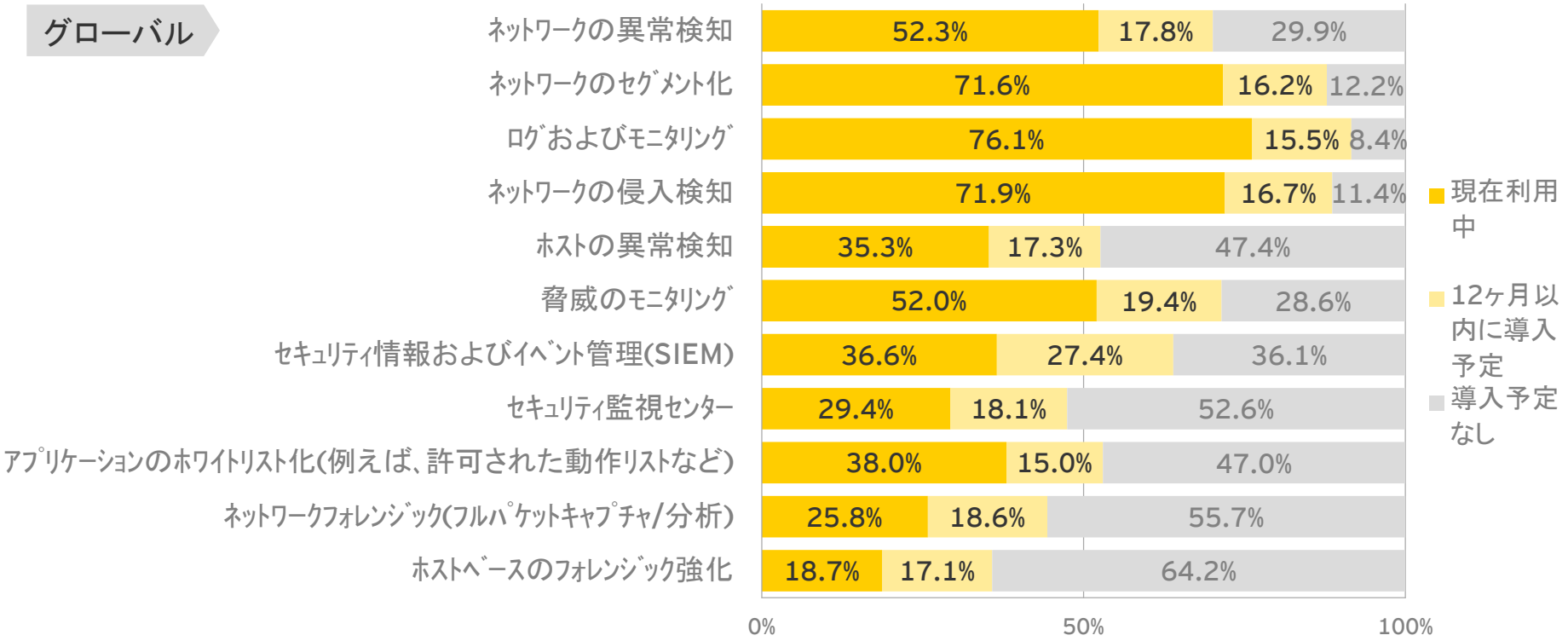
日本



3.ツールとテクノロジー
3.10.外部からの攻撃に対する技術2

Q16.外部からの攻撃を防ぎ、検知し、対応するために、現在利用中のまたは導入予定の技術はありますか?
該当するものをすべて選択してください。

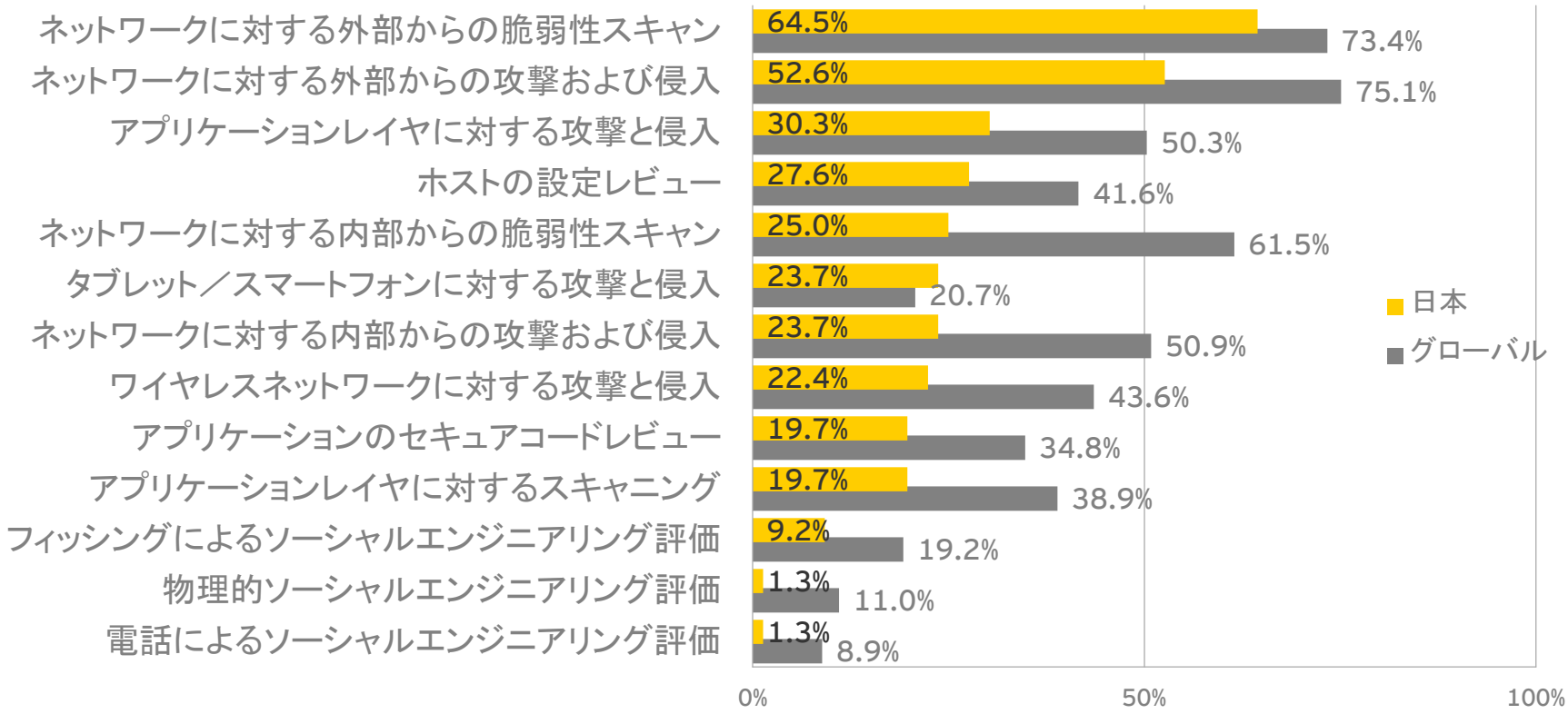
グローバル



3.ツールとテクノロジー
3.11.技術的セキュリティテストの実施状況

- 日本は、実施している割合が低く、ほとんど全ての項目でグローバルの半分程度

Q17.今後一年間で実施予定の技術的セキュリティテストまたは評価について、該当するものをすべて選択してください。



4.戦略・ガバナンスとコントロール

- 新しい脅威に対する情報セキュリティ戦略の見直しの必要性
- 情報セキュリティマネジメントシステムの導入状況
- ITリスク管理プログラムの導入状況
- セキュリティ基準・フレームワークの導入状況
- セキュリティ・アーキテクチャの導入状況
- グローバルは情報セキュリティ評価に外部機関を利用
- 情報取り扱いの管理対策としての外部評価の利用
- 日本は事業継続管理のテストや訓練が少ない
- 日本は第三者機関による事業継続管理の評価が少ない

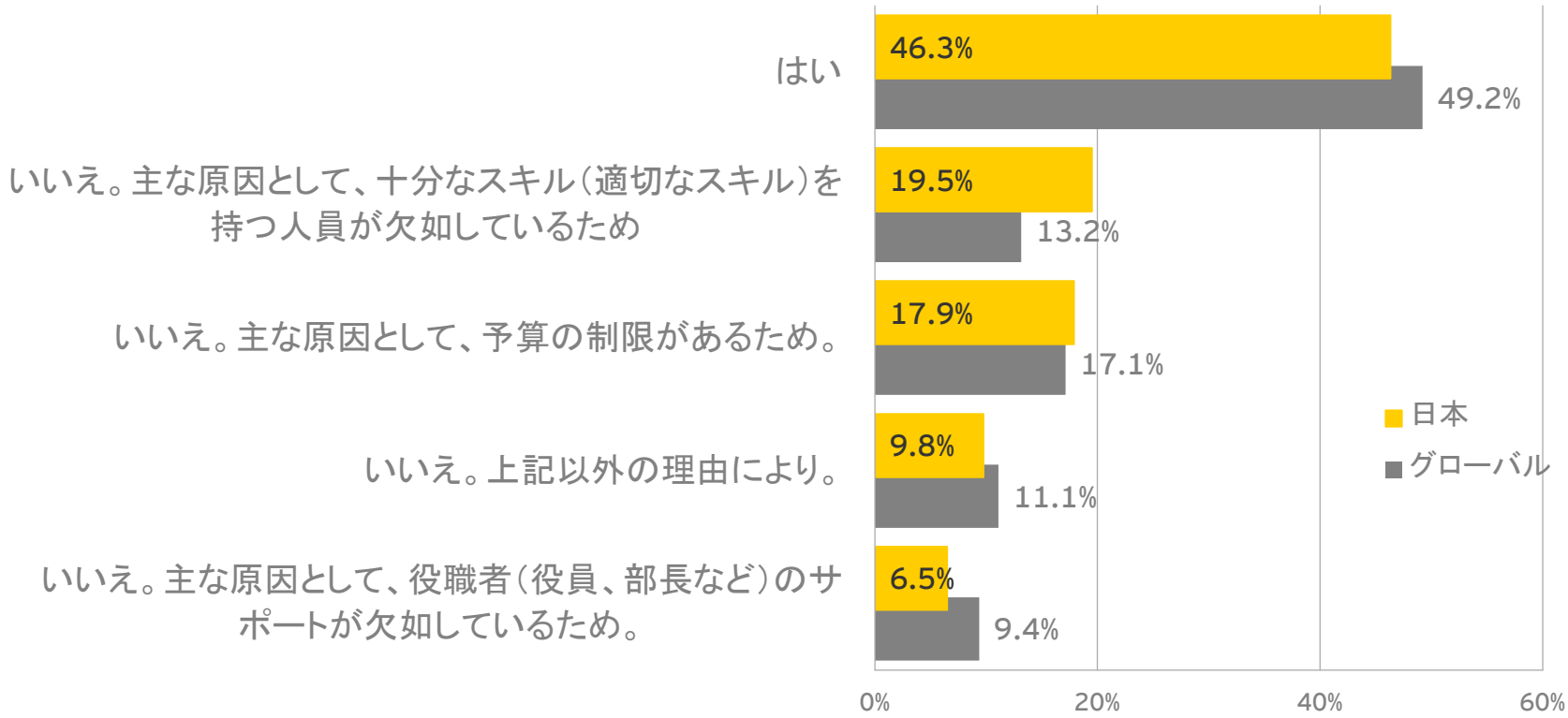
4.戦略・ガバナンスとコントロール 調査結果の概要

1. 新しい脅威に対する情報セキュリティ戦略の見直しの必要性
   - 半数の企業が中長期の情報セキュリティ戦略を策定していない
2. 情報セキュリティマネジメントシステムの導入状況
   - 日本は認証重視、グローバルは基準重視
3. ITリスク管理プログラムの導入状況
   - 日本は、ITリスク管理プログラムの導入が遅れている
4. セキュリティ基準・フレームワークの導入状況
   - グローバルではISO27001・27002、Cobit, ITILの利用が進んでいる
5. セキュリティ・アーキテクチャの導入状況
   - グローバルで導入が進む
6. グローバルは情報セキュリティの評価に外部機関を利用
   - 自主点検と内部監査だけでなく外部機関の評価も
7. 情報取り扱いの管理対策としての外部評価の利用
   - グローバルで進むSSAE16, ISAE3402などの外部評価を活用
8. 日本は事業継続管理のテストや訓練が少ない
9. 日本は第三者機関（外部委託業者など）の事業継続管理の評価が少ない
   - グローバルでは、報告書の請求、質問書の送付、監査を実施

4.戦略・ガバナンスとコントロール
4.1.情報セキュリティ部門の状況

- 日本もグローバルも同じ傾向

Q18.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?

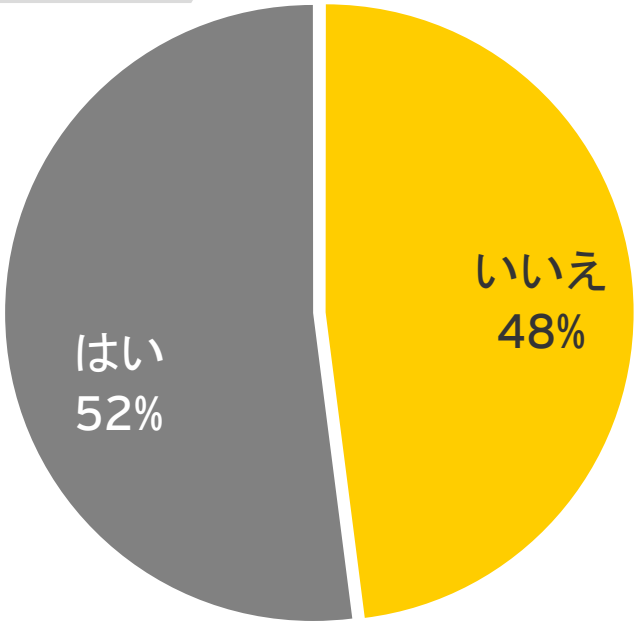


4.戦略・ガバナンスとコントロール
4.2.状況セキュリティ戦略の策定状況

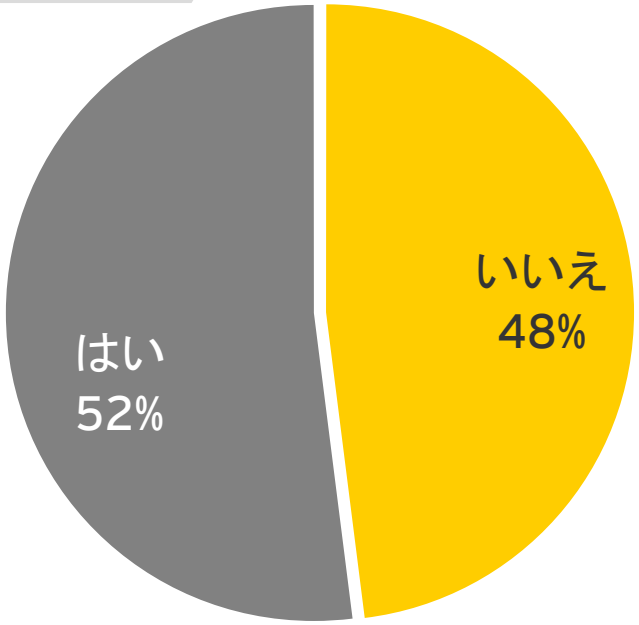
- 日本もグローバルも共に、半数の企業が中長期の情報セキュリティ戦略を策定していない

Q19.今後3年間の情報セキュリティ戦略を策定していますか？ 該当するものを1つ選択してください。

日本



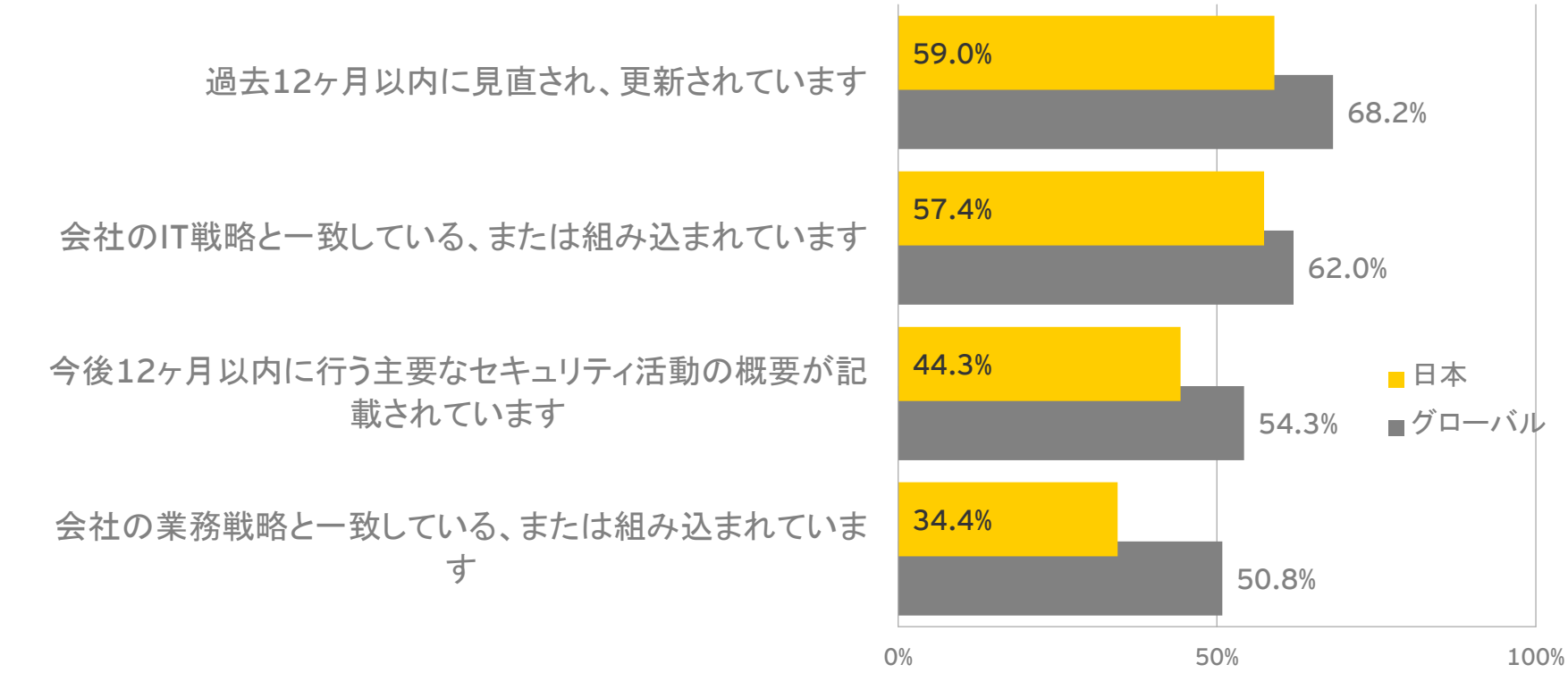
グローバル



4.戦略・ガバナンスとコントロール
4.2.a.情報セキュリティ戦略の内容

- 日本もグローバルも同じ傾向

Q19a. 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。（Q19で[情報セキュリティ戦略を策定している]と回答した方のみ回答）

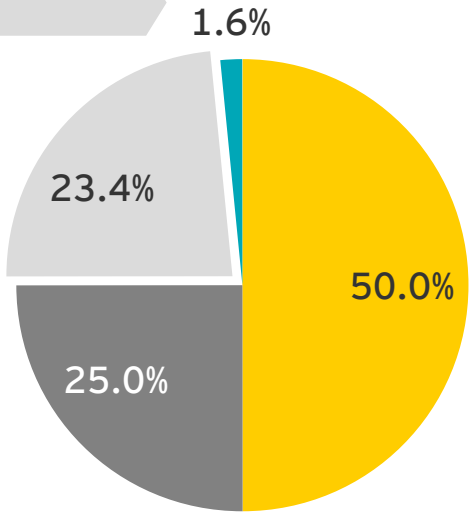


4.戦略・ガバナンスとコントロール
4.2.b.脅威に対する情報セキュリティー戦略

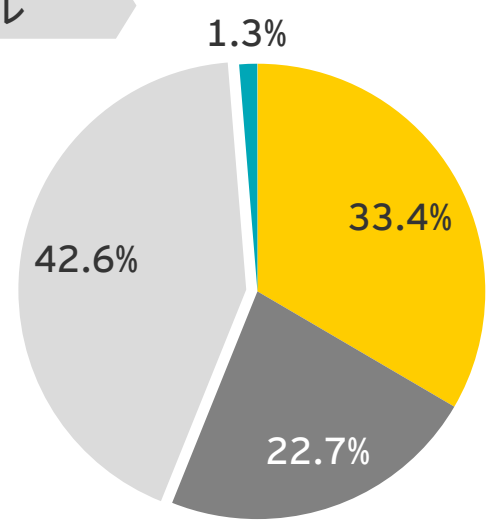
- 日本は、「情報セキュリティ戦略を新たなリスクへの対応させるために変更する必要がある」と認識している

Q19b.今日のセキュリティ脅威の背景という観点から、貴社の情報セキュリティ戦略に最も該当するものを、下記の項目から1つ選択してください。（Q19で[情報セキュリティ戦略を策定している]と回答した方のみ回答）

日本



グローバル



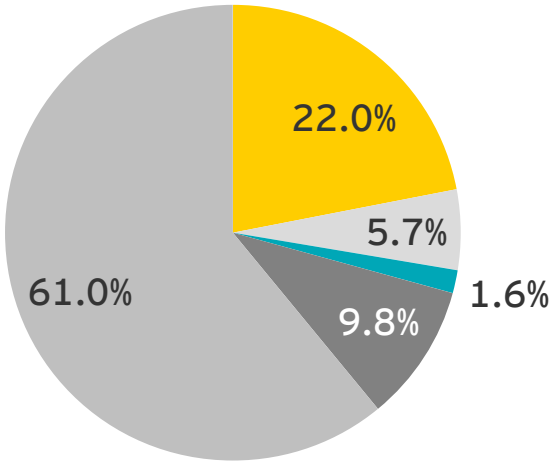
- 会社の情報セキュリティ戦略は、新たなリスクに対応するため変更する必要があります
- 会社は、リスクを理解するために、更なる調査が必要です
- 現在の会社の情報セキュリティ戦略は、リスクに十分対応しています
- テクノロジーに関連する「新たな」または「増加する」リスクがあるとは思いません

4.戦略・ガバナンスとコントロール
4.3.情報セキュリティマネジメントシステム

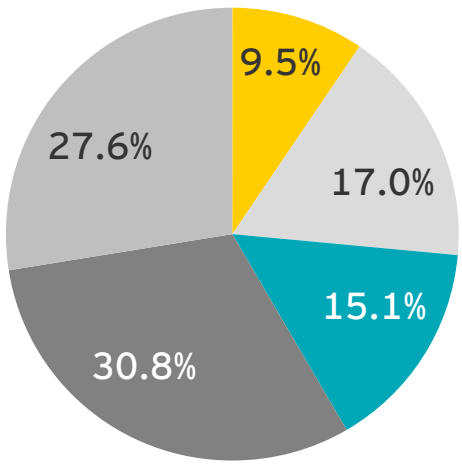
- 日本は、情報セキュリティ管理のための情報セキュリティマネジメントシステム（ISMS）を導入している（日本22%、グローバル10%）

Q20.情報セキュリティ管理のための情報セキュリティマネジメントシステム（ISMS）を導入していますか?該当するものを1つ選択してください。

日本



グローバル



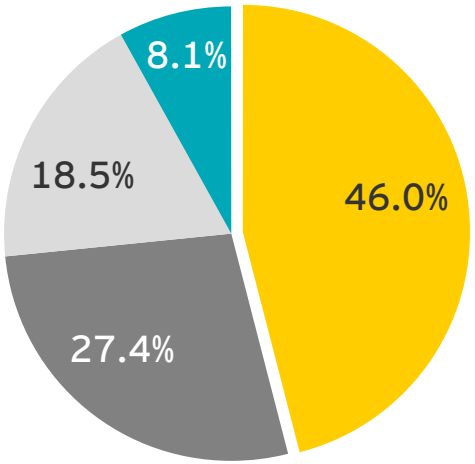
- 導入しており、認証を取得しています（ISO/IEC 27001:2005など）
- 導入していますが、認証は取得していません
- 現在、導入中です
- 導入していませんが、検討中です
- 導入・検討しておりません

4.戦略・ガバナンスとコントロール
4.4.ITリスク管理プログラム

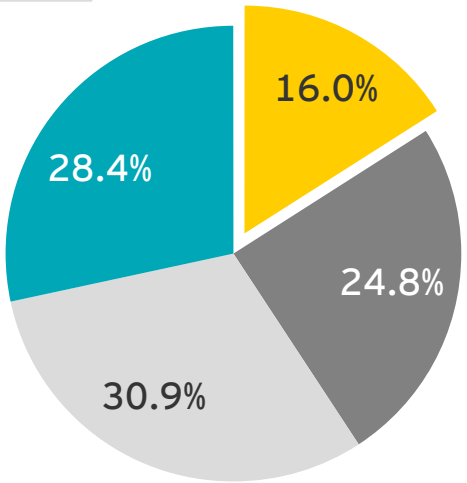
- 日本は、ITリスク管理プログラムの導入が遅れている
- ITリスク管理プログラムを1年以内に導入予定の割合は日本8%、グローバル28%と、今後も差が開く傾向

Q21.貴社では、正式なITリスク管理プログラムはありますか？（正式なITリスク管理プログラムには、指定されたリーダー、リスクアセスメントの実施、リスクレベルの測定が含まれます） 該当するものを1つ選択してください。

日本



グローバル



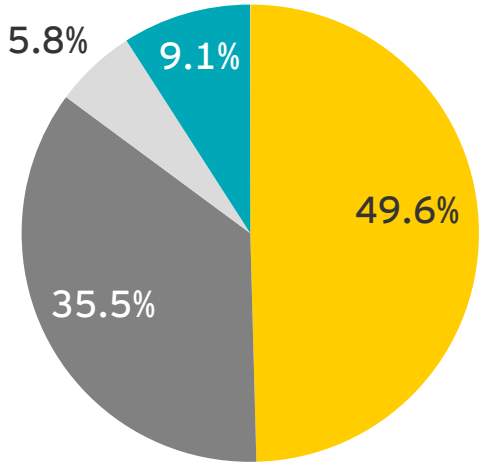
- ITリスク管理プログラムはありませんし、検討もしていません
- はい。会社はITリスク管理プログラムを3年以上前から確立しています
- はい。ITリスク管理プログラムは3年未満ですが存在しています
- ITリスク管理プログラムはありませんが、今後12ヵ月以内に検討する予定です

4.戦略・ガバナンスとコントロール
4.5.取締役会での報告・検討状況

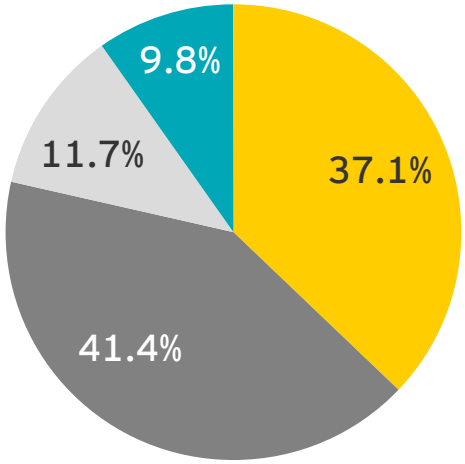
- 日本もグローバルも同じ傾向

Q22.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で取り上げられますか？（もし取締役会が無ければ、組織の経営トップにおいて） 該当するものを1つ選択してください。

日本



グローバル

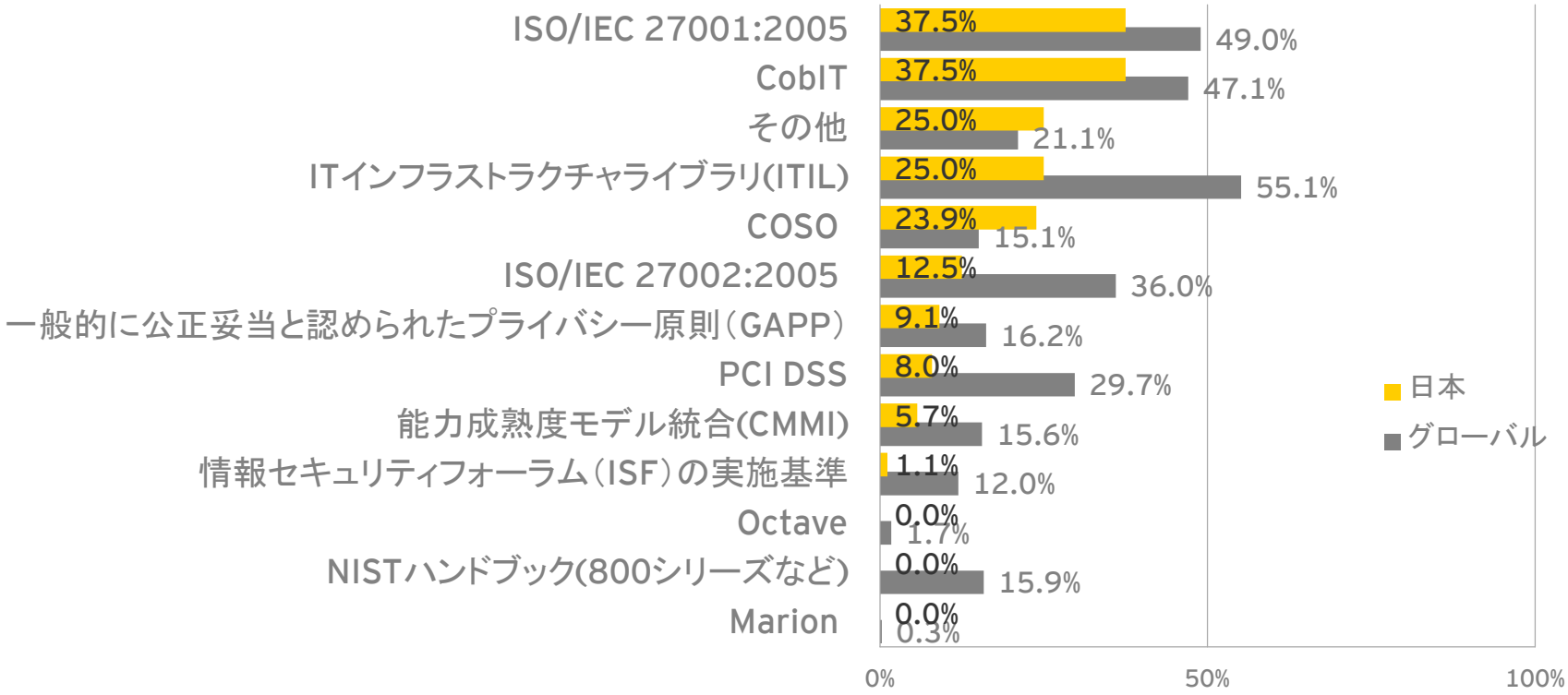


■ 年に一度/殆どありません
■ おおよそ4半期に一度あります
■ 取締役会の都度あります
■ 全くありません

4.戦略・ガバナンスとコントロール
4.6.セキュリティ基準・フレームワークについて

- 日本は、セキュリティ基準・フレームワークにISO27001・27002、Cobit, ITILを利用することが少ない

Q23.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。

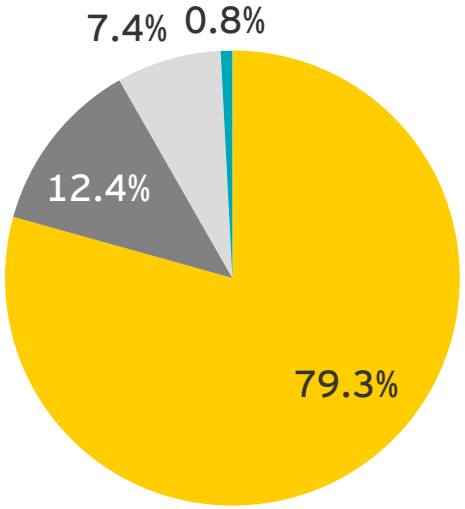


4.戦略・ガバナンスとコントロール
4.7.セキュリティ・アーキテクチャ

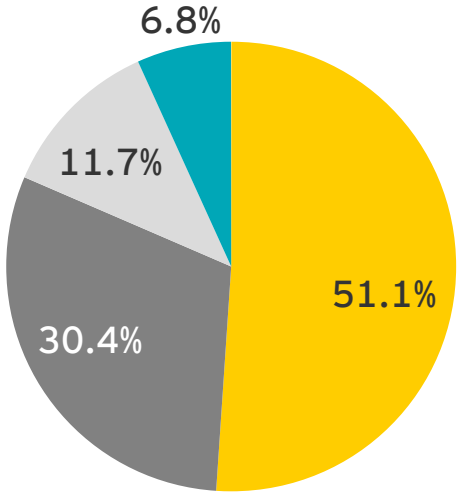
- 日本もグローバルも共に、セキュリティアーキテクチャのフレームワークを確立している企業が少ない
- 日本は、セキュリティアーキテクチャの検討が遅れている

Q24.正式なセキュリティアーキテクチャのフレームワークを確立していますか?

日本



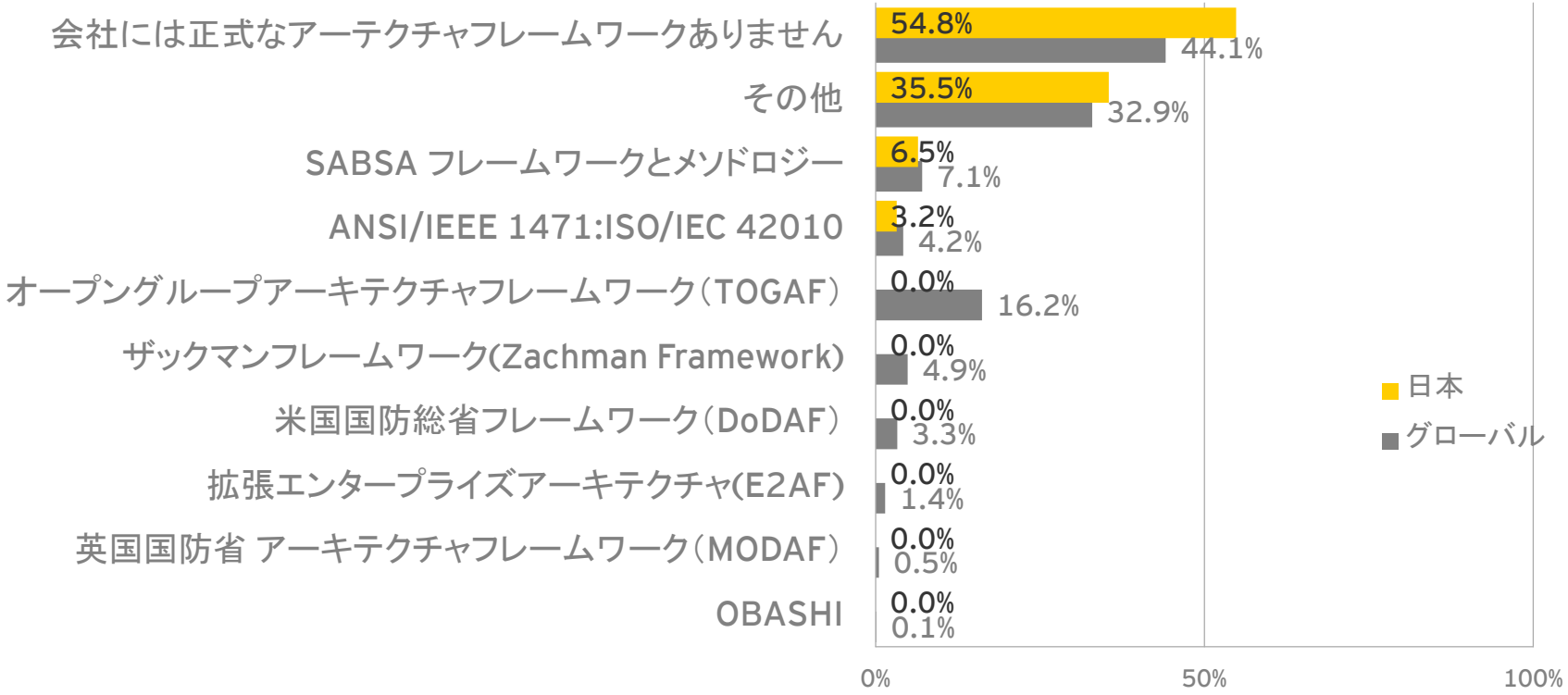
グローバル



- いいえ、確立していません。検討もしていません
- いいえ、しかし検討はしています
- はい、会社は正式なアーキテクチャのフレームワークを確立しています
- はい、会社は最近、正式なアーキテクチャのフレームワークを確立しました

4.戦略・ガバナンスとコントロール
4.7.a.フレームワークの内訳

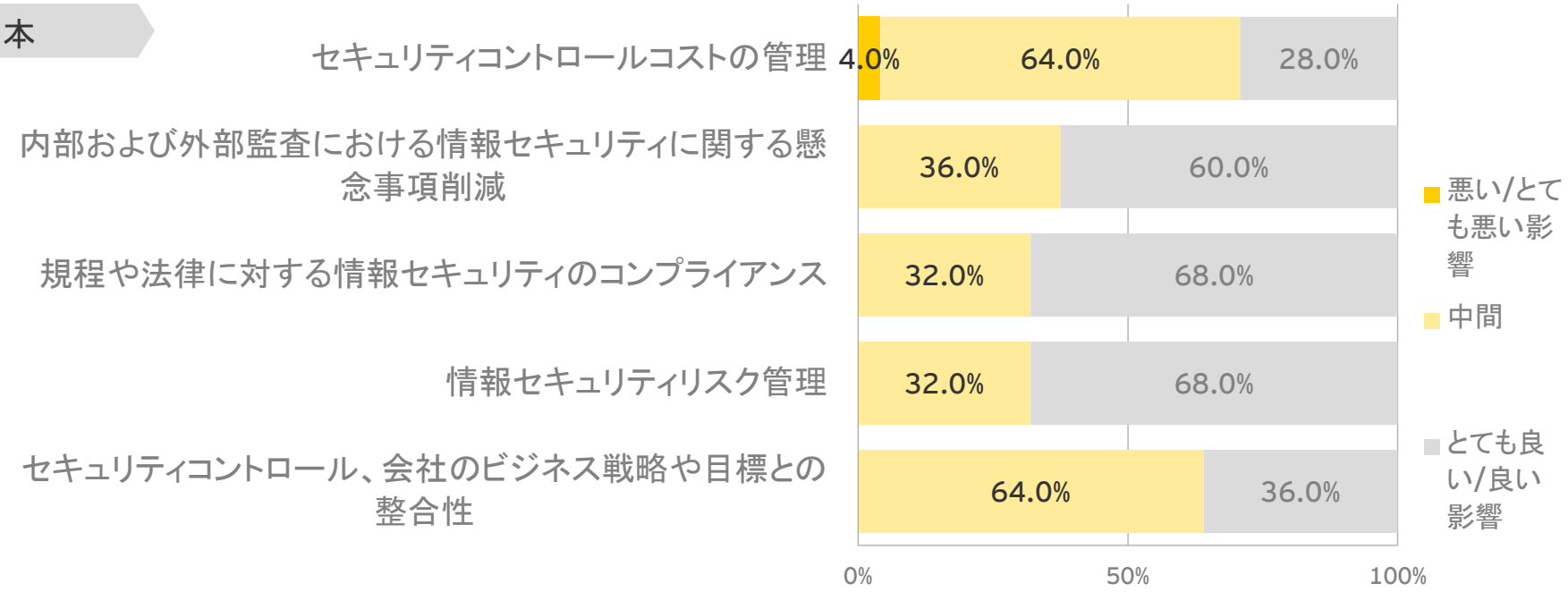
Q24a.どの正式なセキュリティアーキテクチャのフレームワークが使われていますか？　該当するものをすべて選択してください。（Q24で[セキュリティアーキテクチャ・フレームワークを確立している/検討中]と回答した方のみ回答）



4.戦略・ガバナンスとコントロール
4.7.b.フレームワークのインパクト1

Q24b.セキュリティアーキテクチャフレームワークは、下記のカテゴリーにおいて、会社のステークホルダや機能に対しどのようなインパクトがありますか？（Q24で[セキュリティアーキテクチャ・フレームワークを確立している/検討中]と回答した方のみ回答）

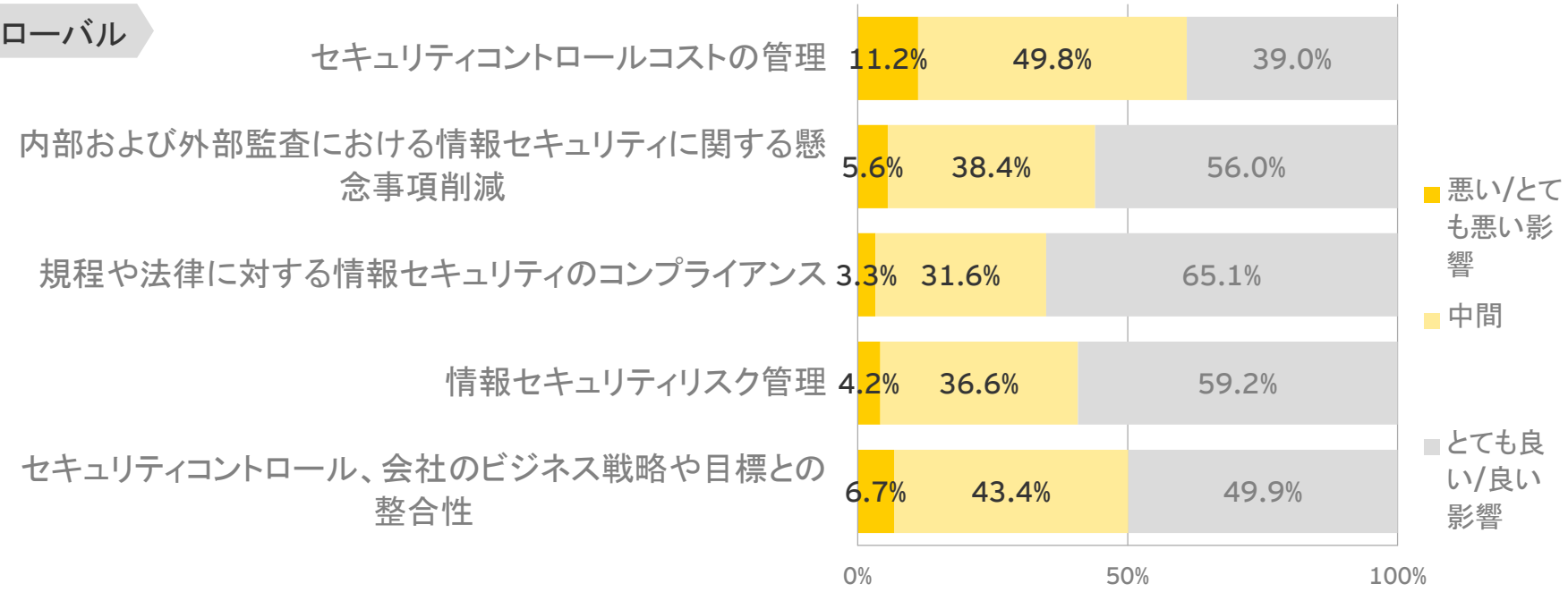
日本



4.戦略・ガバナンスとコントロール
4.7.b.フレームワークのインパクト2

Q24b.セキュリティアーキテクチャフレームワークは、下記のカテゴリーにおいて、会社のステークホルダや機能に対しどのようなインパクトがありますか？（Q24で[セキュリティアーキテクチャ・フレームワークを確立している/検討中]と回答した方のみ回答）

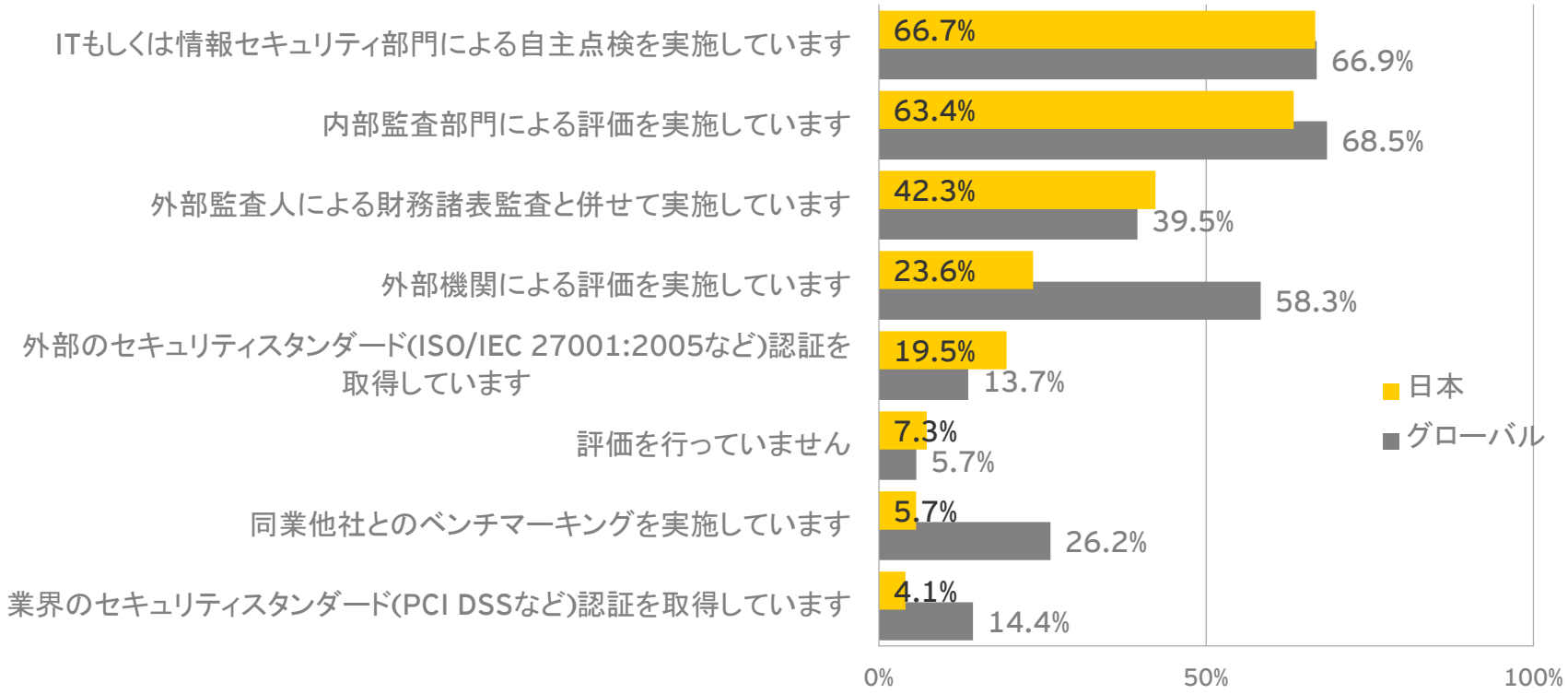
グローバル



4.戦略・ガバナンスとコントロール
4.8.情報セキュリティの評価

- 日本もグローバルも共に、3分の2の企業が情報セキュリティの品質や有効性を評価するために自主点検及び内部監査を実施している
- グローバルでは、さらに外部機関による評価（58%）を実施している（日本は23%）

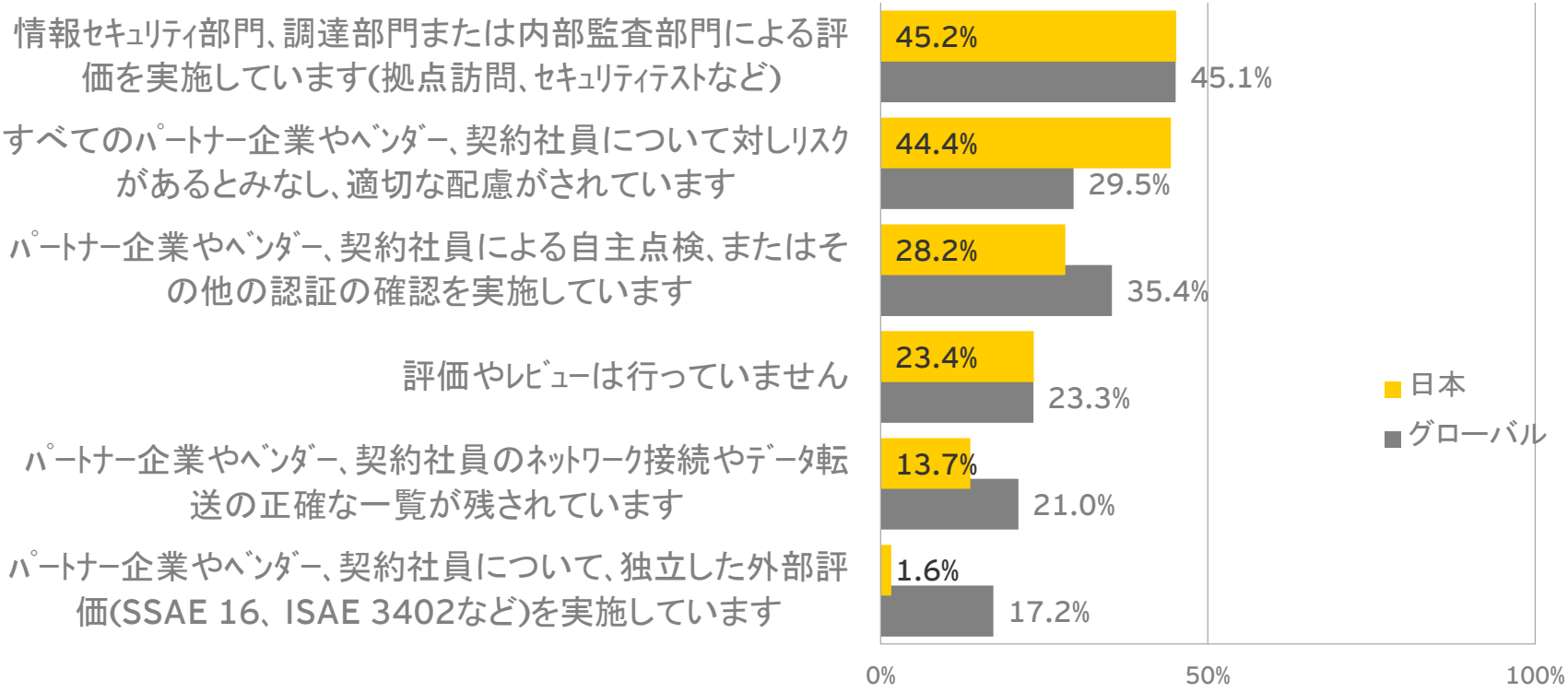
Q25.情報セキュリティの品質や有効性をどのように評価していますか？ 該当するものをすべて選択してください。



4.戦略・ガバナンスとコントロール
4.9.情報取り扱いの管理対策

- グローバルは、SSAE16, ISAE3402などの外部評価を活用している（グローバル17%、日本2%）

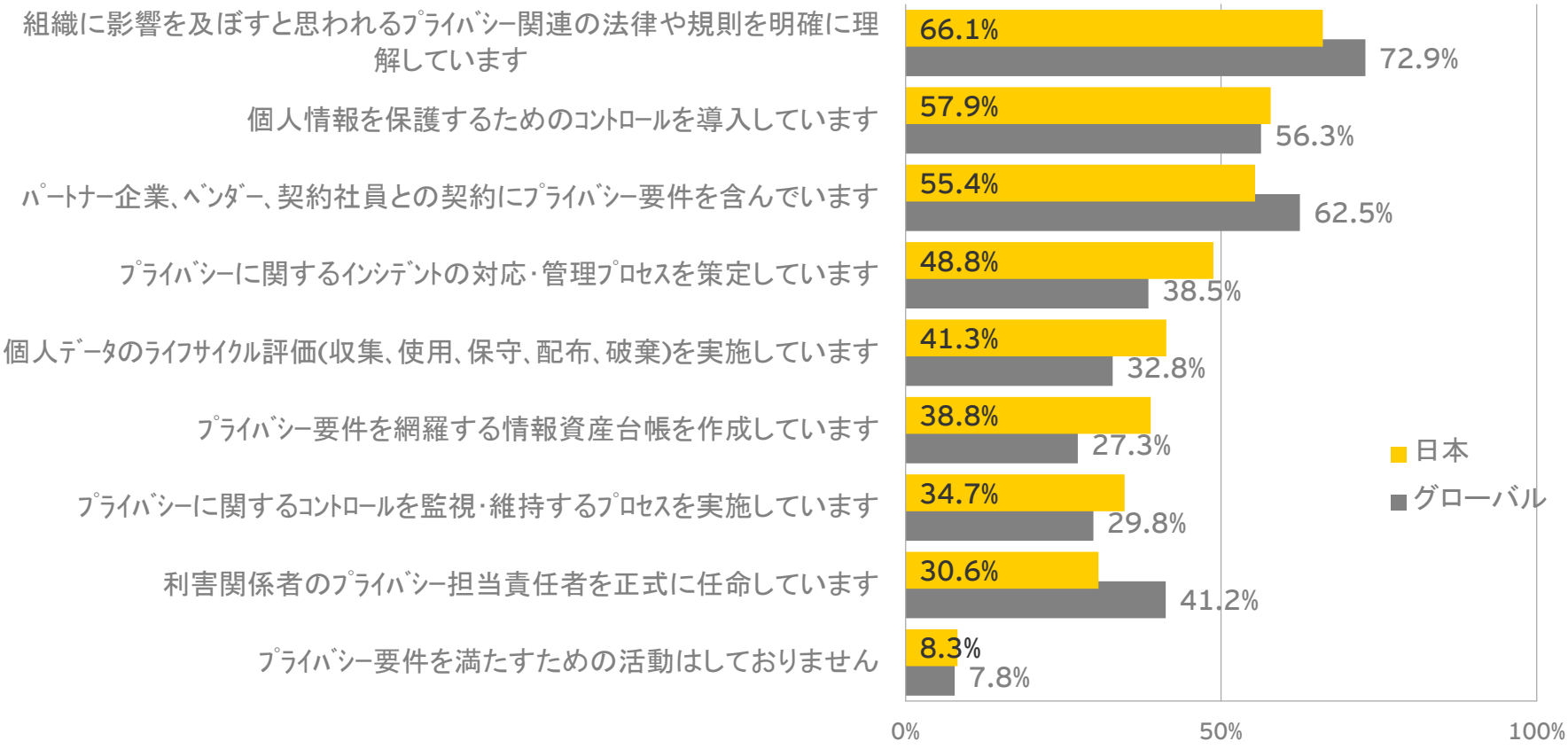
Q26.パートナー企業、ベンダー、契約社員が貴社の情報を適切に取り扱い、管理するために、どのような対策を実施していますか？ 該当するものをすべて選択してください。



4.戦略・ガバナンスとコントロール
4.10.プライバシーについて

日本もグローバルも同じ傾向にある

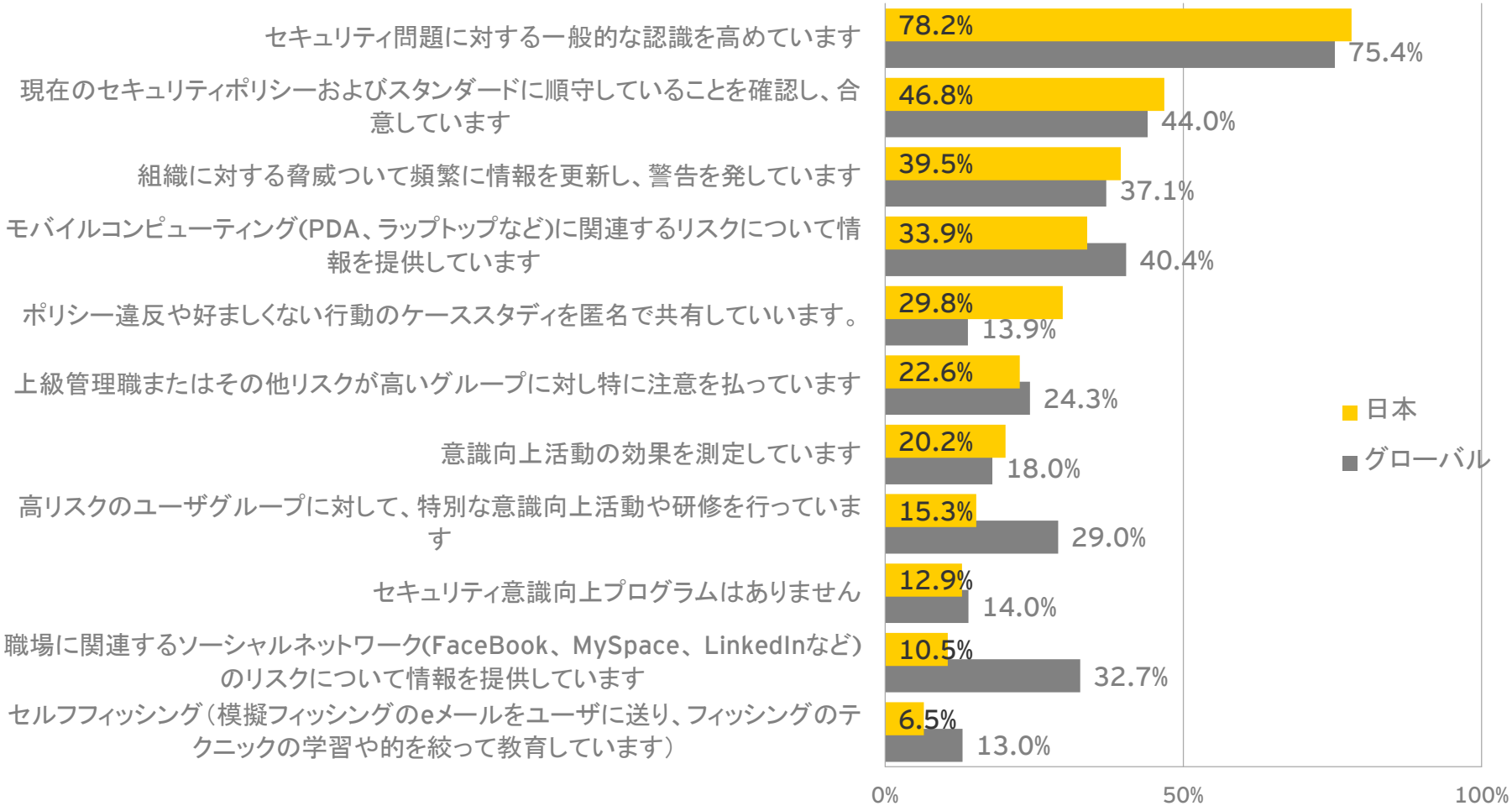
Q27.貴社のプライバシーについて、該当するものをすべて選択してください。



4.戦略・ガバナンスとコントロール
4.11.意識向上プログラム

- グローバルでは、意識向上活動や研修実施やソーシャルネットワークに関するリスク情報の提供が進んでいる

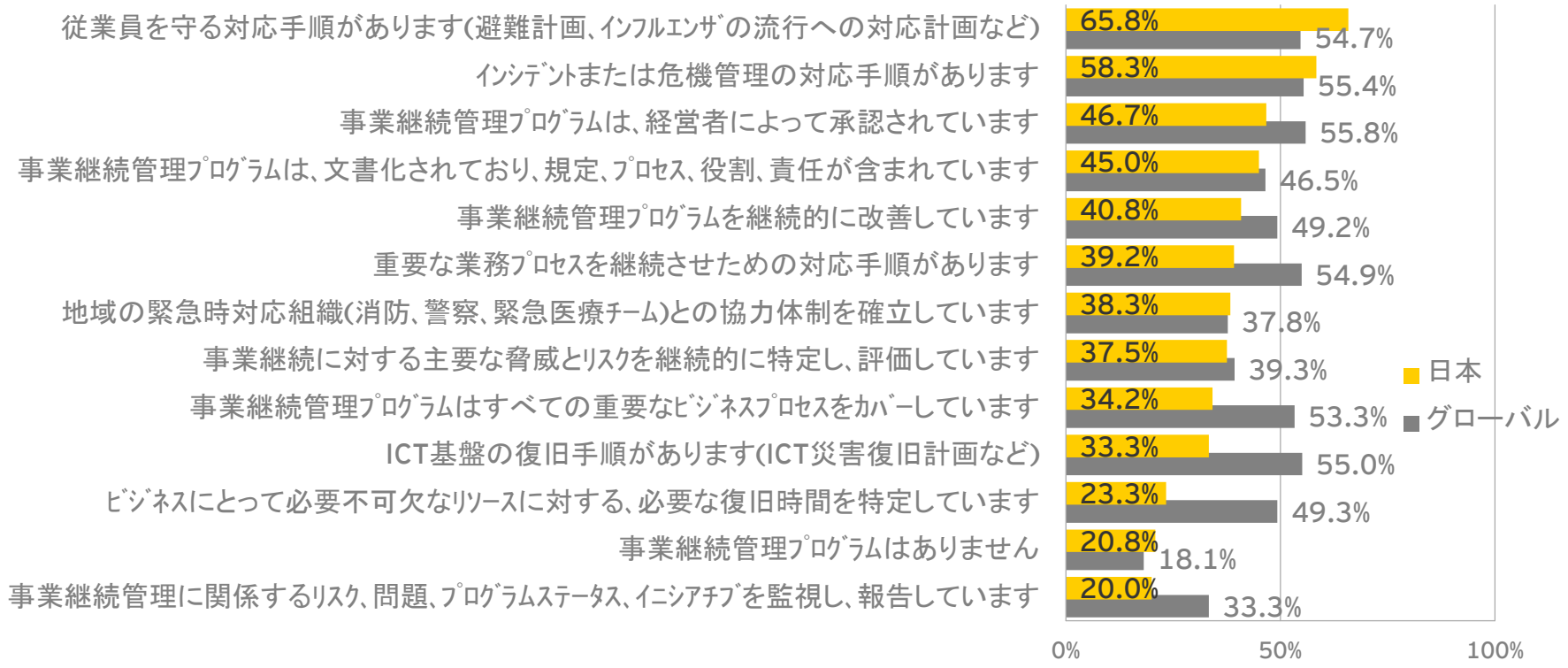
Q28.貴社で現在実施している意識向上プログラムについて、該当するものをすべて選択してください。



4.戦略・ガバナンスとコントロール
4.12.事業継続管理戦略およびプログラム

- グローバルは、事業継続管理プログラムが適切に実施されるための施策が多い

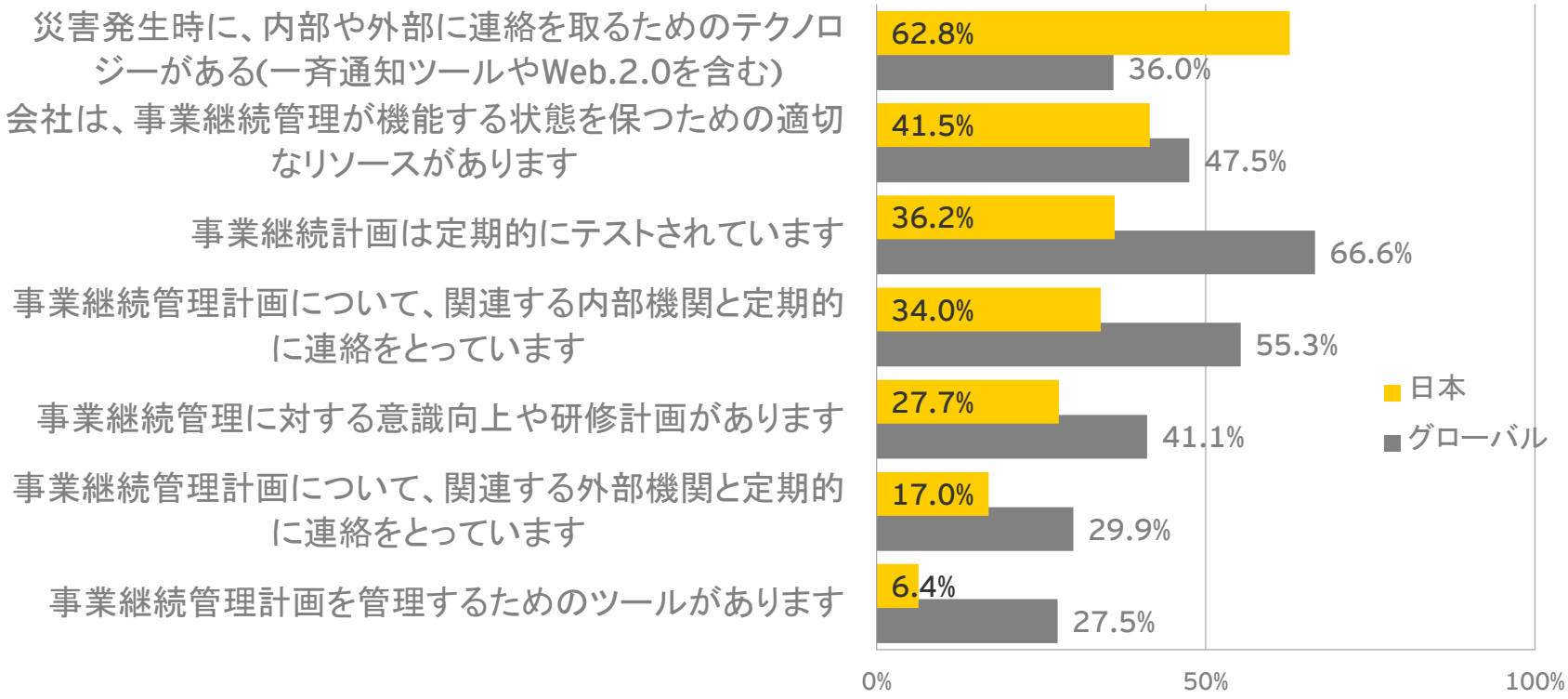
Q29.貴社の事業継続管理（BCM）戦略およびプログラムにあてはまる項目について、該当するものをすべて選択してください。



4.戦略・ガバナンスとコントロール
4.13.事業継続管理プログラム展開

- 日本は、「災害発生時の連絡に関するテクノロジー」を積極的に展開している
- 日本は、定期的なテスト、定期的な連絡及び研修計画などの実施が低い

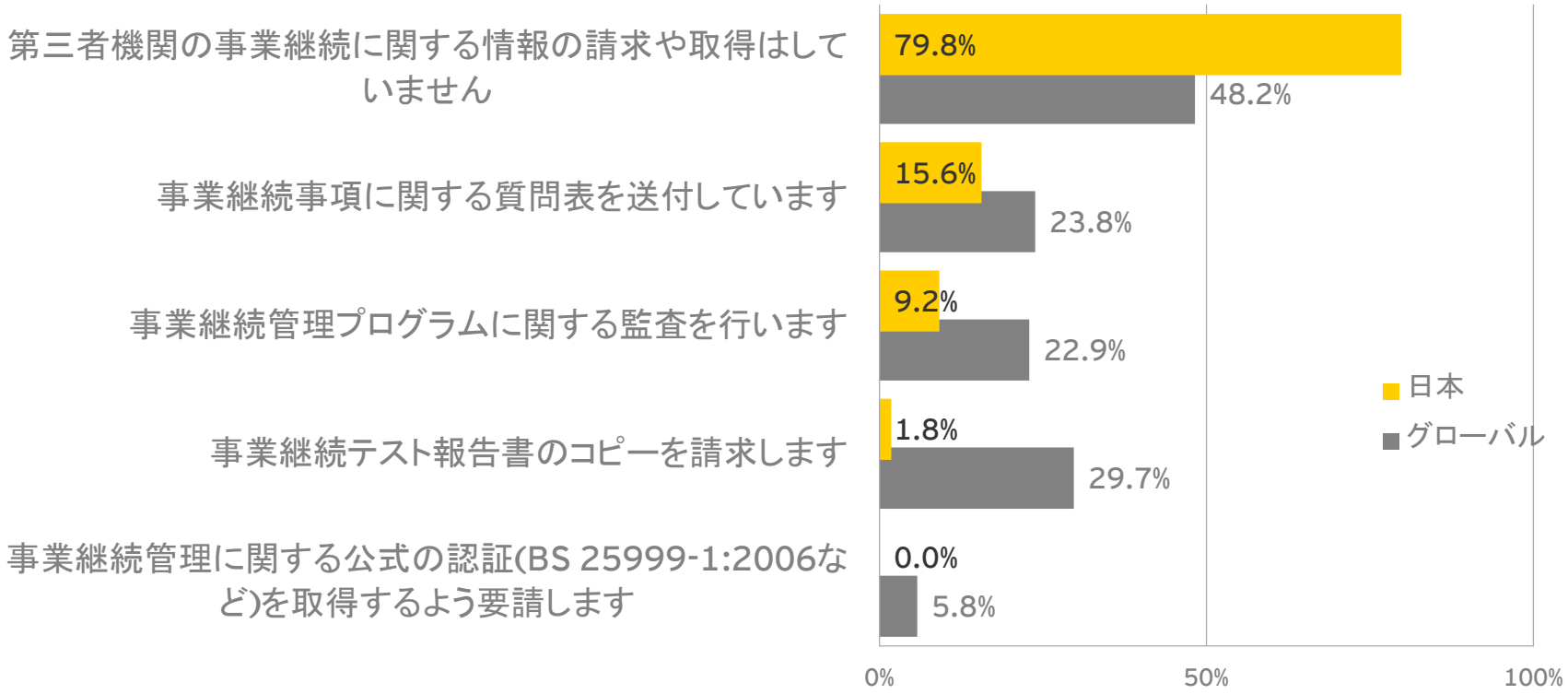
Q30.貴社の事業継続管理プログラム展開にあてはまる項目について、該当するものをすべて選択してください。



4.戦略・ガバナンスとコントロール
4.14.第三者機関の事業継続管理評価

- グローバルでは、「事業継続テスト報告書のコピーの請求」、「事業継続事項に関する質問書の送付」、「事業継続プログラムに関する監査」を実施し、外部委託業者の対応能力を評価することが多い

Q31.貴社にとって重要な第三者機関（外部委託業者など）の事業継続管理に関する対応能力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。



Ernst & Young ShinNihon LLC

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15万2千人の構成員は、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、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、日本最大規模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。