IBM Securityインシデント対応者調査

–

2022年7月6～13日

MORNING CONSULT®

IBM®

主な調査結果

1. サイバーセキュリティー・インシデント対応者は、**他者/企業を助け保護するという使命感が、この職業に惹かれる最も大きな理由だと回答しています。** また、最も影響を及ぼす理由として続くのは「継続的な学習機会」と「問題解決に根ざしていること」でした。
2. **これと同時に「チームやクライアントに対する責任感」**と**「ステークホルダーの期待に応えること」**は、**サイバー・インシデント対応で最もストレスを感じる側面**として、約半数がストレス要因のトップ3に挙げています。
3. **回答者の48%によると、インシデント対応に関わる平均期間は2～4週間**です。 また、**30%近くが、インシデント対応に関わる期間**が平均**4週間以上**と回答しています。 圧倒的に多くの回答者が、2つ以上の重複するインシデントへの対応を任されることがよくあると述べています。
4. **攻撃への対応は、最初の3日間が最もストレスが大きいとされています。** さらに、3分の1超が、その対応の最もストレスの多い時期に、1日12時間以上働いていると回答しています。
5. サイバーセキュリティー・インシデント対応者の大多数は、**ランサムウェアの台頭により、サイバーセキュリティー・インシデント対応時に求められるストレス/心理的要求**が悪化したと考えており、全体で81%がそのような所感を述べています。
6. **サイバーセキュリティー・インシデント対応者の67%**が、**インシデント対応の結果、日常生活でストレス/不安を感じている**と回答しています。
7. **サイバーセキュリティー・インシデント対応者の65%近く**が、**サイバーセキュリティー・インシデントに対応した結果、メンタルヘルスに関する支援を求めたことがあるそうです。** また、回答者の大半（84%）が、適切なメンタルヘルス支援リソースを利用できると回答しています。

調査方法： 本調査は、2022年7月 6日～13日にかけて、IBMの委託を受け、Morning Consult社が実施したものです。本調査は、米国、英国、ドイツ、カナダ、オーストラリア、フランス、スペイン、ブラジル、日本、インドのグローバル市場において、サイバーセキュリティー・インシデント対応者1,107名を対象に実施されました。インタビューはオンラインで実施し、グローバル市場におけるサイバーセキュリティー・インシデント対応者の誤差は、95%の信頼度で±3%ポイントとなっています。

アジェンダ

サイバーセキュリティー・インシデント対応者の一般認識

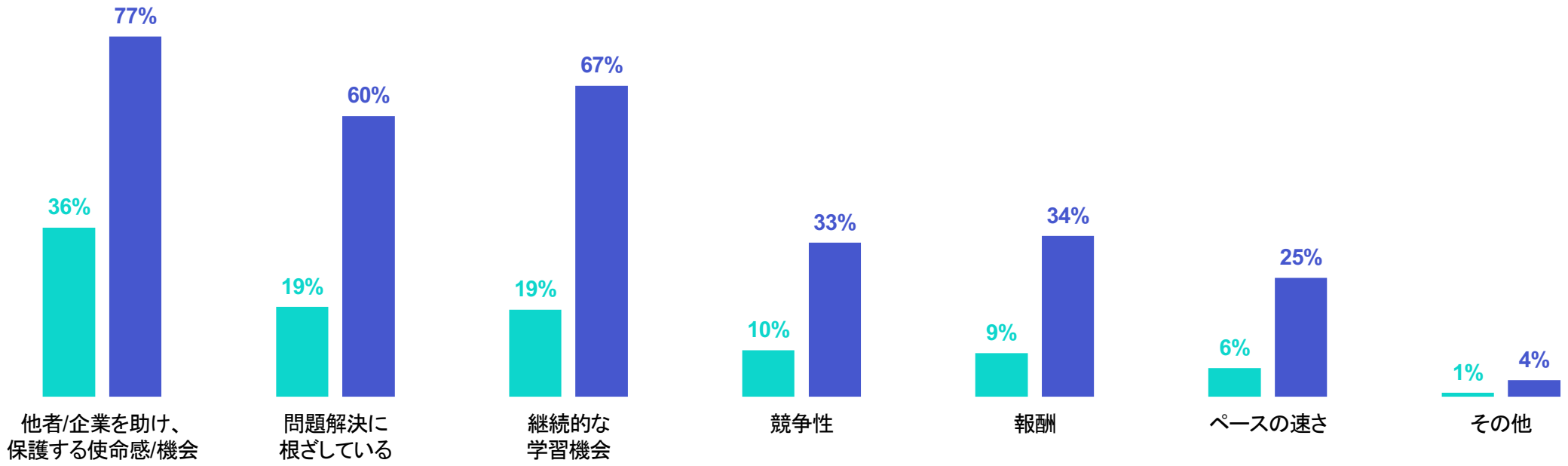
サイバーセキュリティー・インシデント対応時のストレス要因

メンタルヘルスと健康への影響

MORNING CONSULT

サイバーセキュリティー・インシデント対応者は、他者/企業を助け、保護するという使命感/機会、継続的な学習機会、および問題解決に根ざしていることが、この職業に惹かれる最も大きな理由だと回答

サイバーセキュリティー・インシデント対応という職業に惹かれた理由を表すものは、次のうちどれですか？上位3つを優先順位の高い順にドラッグ＆ドロップしてください。



MORNING CONSULT

他者/企業を助け、保護するという使命感/機会が、市場全体でサイバーセキュリティー・インシデント対応者を惹きつける理由として最も影響していたが、特にスペインと日本では、問題解決もサイバーセキュリティー・インシデント対応者にとって影響をもたらす理由であった

サイバーセキュリティー・インシデント対応という職業に惹かれた理由を表すものは、次のうちどれですか？ 上位3つを優先順位の高い順にドラッグ＆ドロップしてください。 **[最も上位の理由とした回答者の割合を示す]**

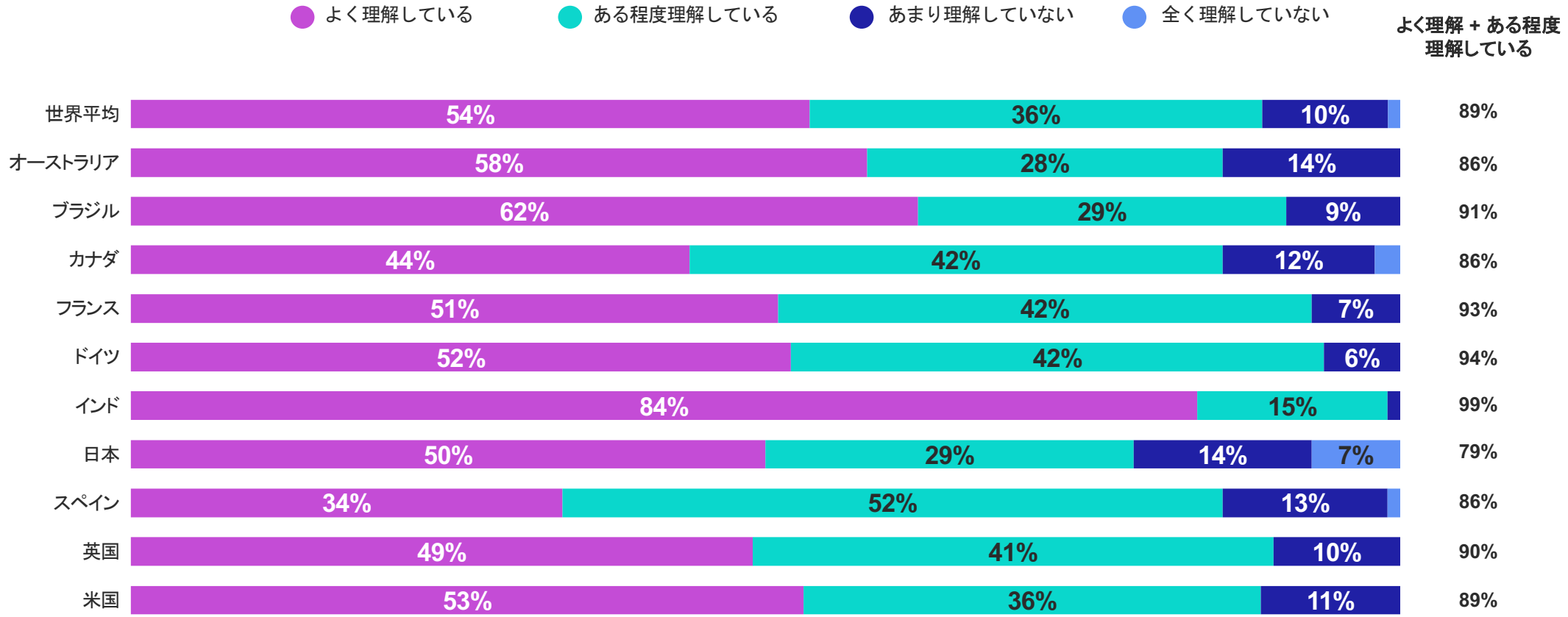
	米国	英国	ドイツ	カナダ	オーストラリア	フランス	スペイン	ブラジル	日本	インド
問題解決に根ざしている	15	15	17	19	20	19	31	16	29	13
ペースの速さ	5	10	5	4	9	4		11	5	8
競争性	11	10	12	10	6	15	9	4	8	11
他者/企業を助け、保護するという使命感/機会が与えられる	39	36	40	34	38	40	31	30	34	37
継続的な学習機会	19	21	15	19	19	13	23	21	15	23
報酬	11	7	9	13	8	8	5	16	7	8

3%未満の回答は除外

MORNING CONSULT

ほとんどの市場において、カナダ、スペイン、英国を除き、サイバーセキュリティー・インシデント対応者の半数以上が、上級管理職はインシデント対応関連の活動をとてもよく理解していると考えている

あなたの経験では、上級管理職（雇用主やクライアントの管理職を含む）は、インシデント対応関連の活動についてどの程度理解していると思いますか？

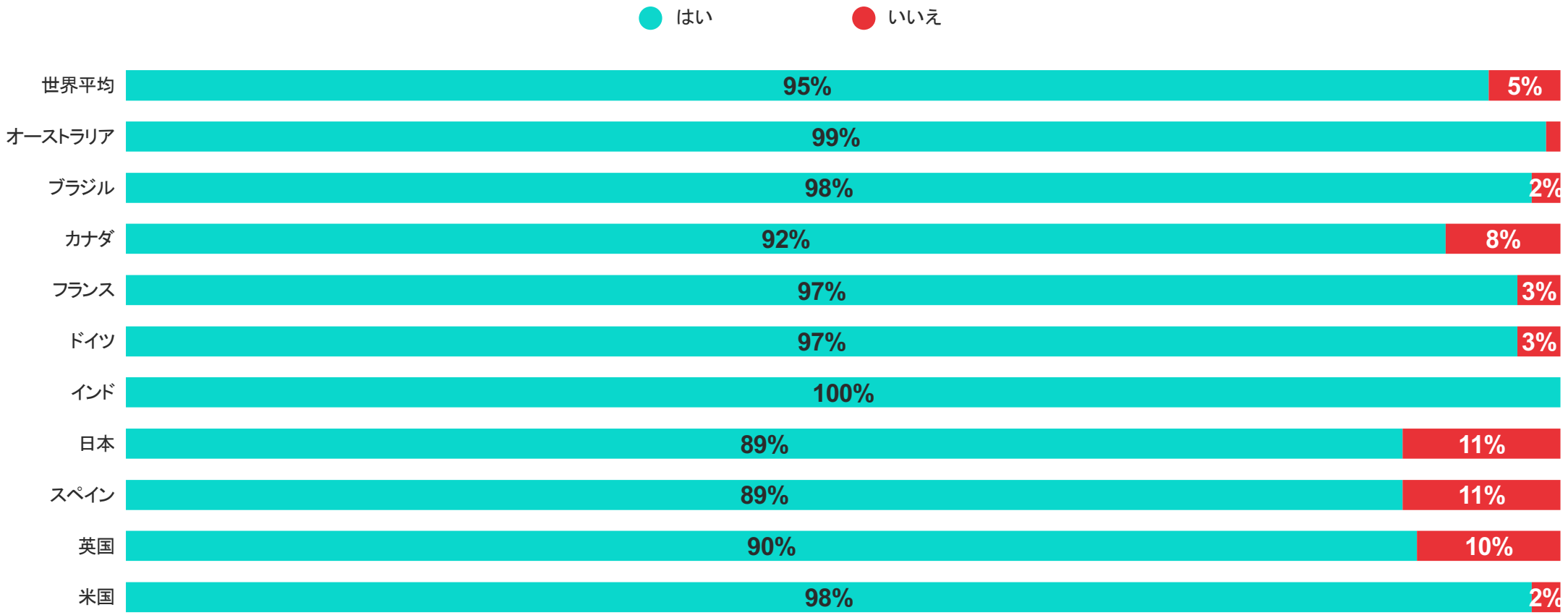


「世界平均」とは、米国、英国、ドイツ、カナダ、オーストラリア、フランス、スペイン、ブラジル、日本、インドのグローバル市場におけるサイバーセキュリティー・インシデント対応者の回答の合計を反映しています。

MORNING CONSULT

全市場のサイバーセキュリティー・インシデント対応者の大半は、上級管理職が成功に必要なサポート体制を提供していると考えている（95%）

上級管理職（雇用主および/またはクライアントの管理職を含む）は、成功に必要なサポート体制（人員配置、ツール、対応計画など）を提供してくれていると思いますか？



アジェンダ

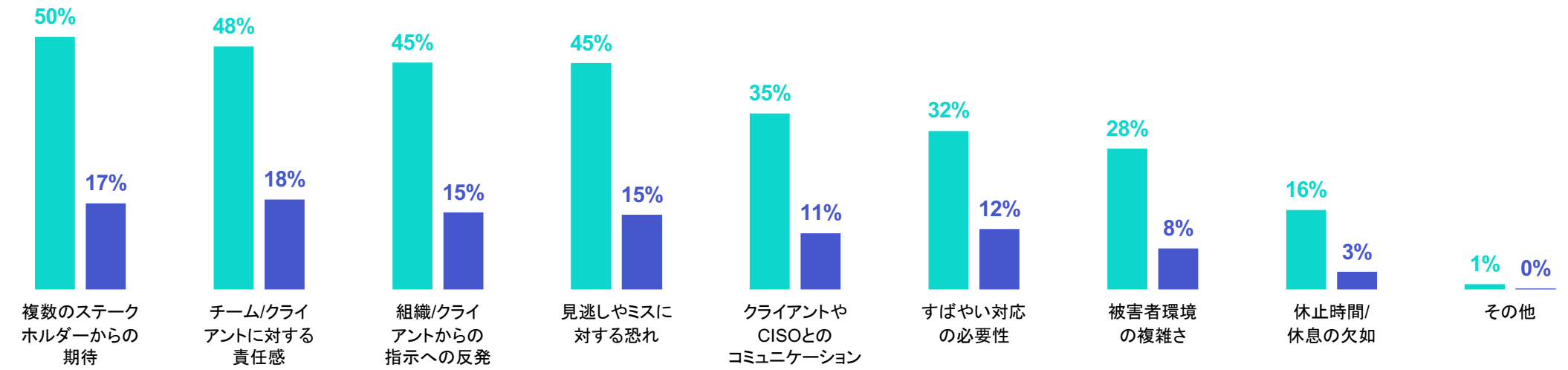
サイバーセキュリティー・インシデント対応者になることに
対する所感

サイバーセキュリティー・インシデント対応時のストレス要因

メンタルヘルスと健康への影響

サイバーセキュリティー・インシデントに対応する際に最もストレスを感じる側面は、複数のステークホルダーからの期待に応えることと、チーム/クライアントに対してインシデントを軽減しようとする責任感であるとされている

サイバーセキュリティー・インシデントへの対応で最もストレスを感じる側面は、次のうちどれだと思いますか？ 上位3つを優先順位の高い順にドラッグ＆ドロップしてください。



サイバーセキュリティー・インシデント対応時のストレス要因

カナダ、スペイン、インドのサイバーセキュリティー・インシデント対応者は、チーム/クライアントに対してインシデントを軽減しようという責任感が、サイバーセキュリティー・インシデント対応で最もストレスの大きい側面であると考えている

サイバーセキュリティー・インシデントへの対応で最もストレスを感じる側面は、次のうちどれだと思いますか？ 上位3つを優先順位の高い順にドラッグ＆ドロップしてください。 **[これをストレス要因の最上位に挙げた回答者の割合を示す]**

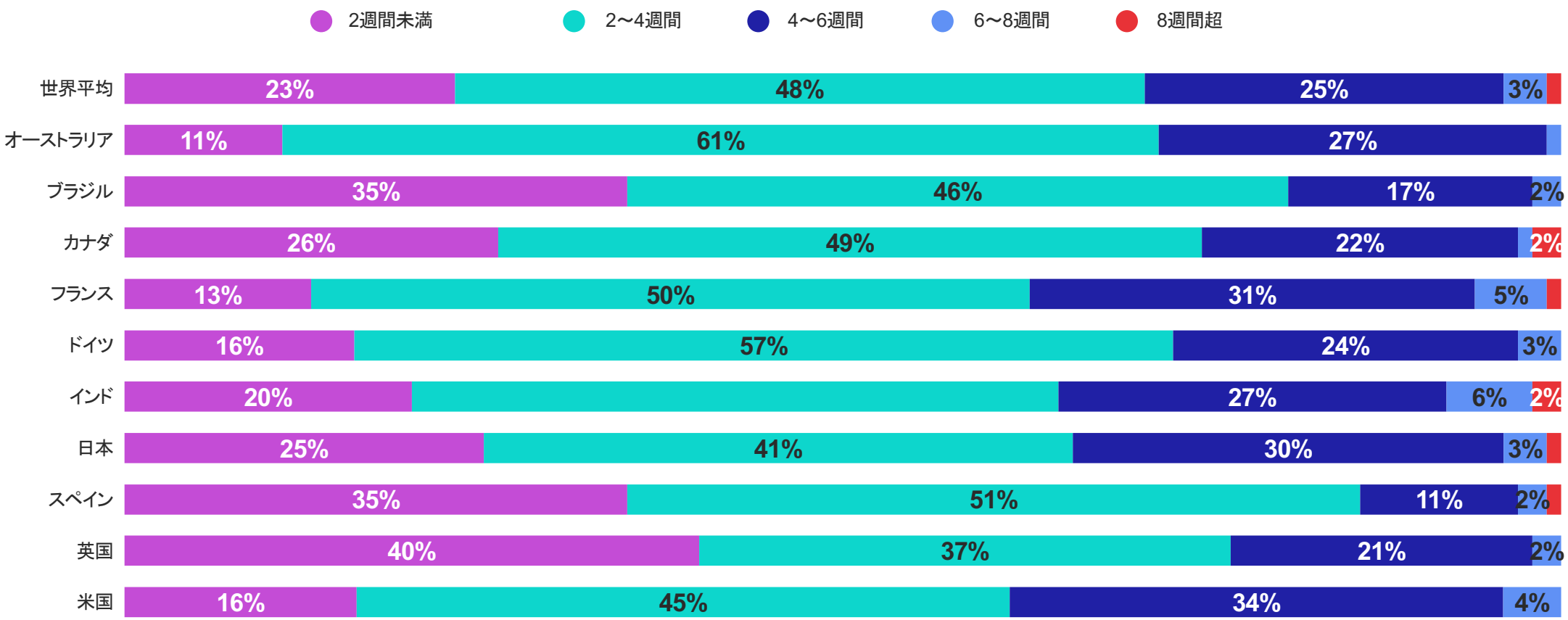
	米国	英国	ドイツ	カナダ	オーストラリア	フランス	スペイン	ブラジル	日本	インド
見逃しや間違い、もしくはその両方を犯すことへの恐れ	19	19	18	16	13	15	13	15	10	4
チーム/クライアントに対してインシデントを軽減しようとする責任感	15	15	14	23	16	19	23	14	16	26
クライアントやCISOとのコミュニケーションが不十分または不明確	15	10	11	7	16	10	7	13	11	7
組織/クライアントからの推奨対応/改善アプローチに対する反発	14	14	17	17	26	17	4	20	18	10
複数のステークホルダーからの期待に応える（例：経営幹部/取締役会などからのプレッシャー）	16	20	18	12	14	16	20	21	20	17
すばやい対応の必要性	10	14	14	13	8	9	19	8	12	16
休止時間/休息の欠如	4	3	3	5	4	3	3			7

3%未満の回答は除外

MORNING CONSULT

平均して、71%がインシデント対応の実施期間を4週間以内としている。 米国のサイバーセキュリティー・インシデント対応者の39%は、インシデント対応の平均実施期間が4週間超

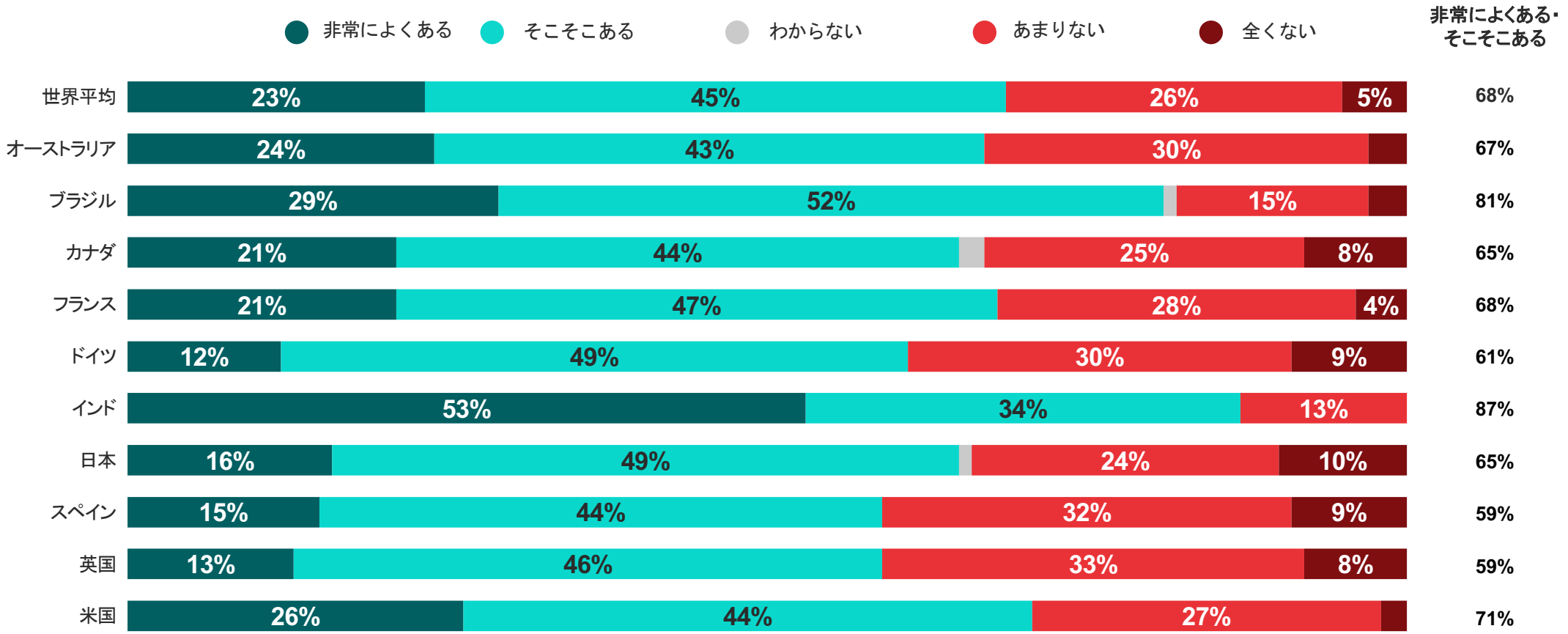
これまで対応したインシデントについて、インシデント対応実施の平均的な期間を教えてください。



MORNING CONSULT

大多数（68%）が、2つ以上の重複したサイバーセキュリティー・インシデントへの対応を任されることが非常によくある、またはそこそこあると回答

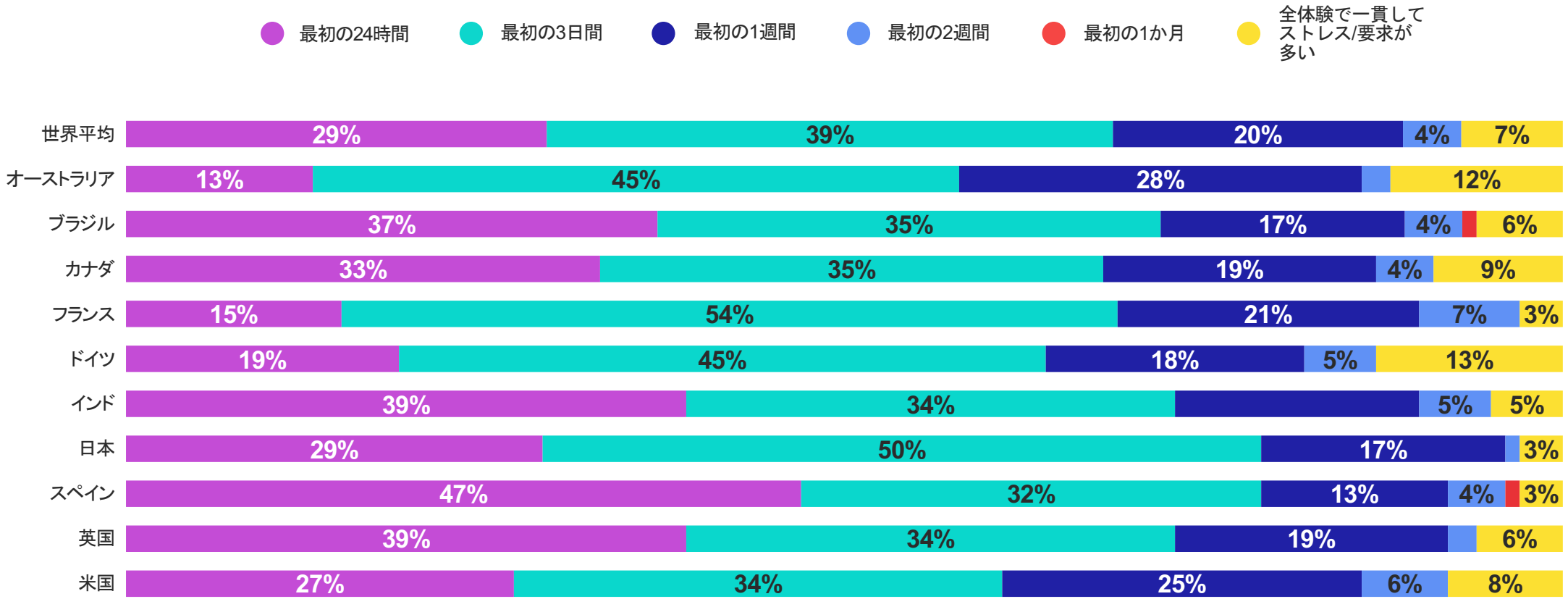
あなたの経験では、2つ以上の重複したサイバーセキュリティー・インシデントへの対応を任されることはよくありますか？



MORNING CONSULT

39%が、サイバーセキュリティー・インシデントに対応する際、最初の3日間が最もストレス/要求が高いと回答

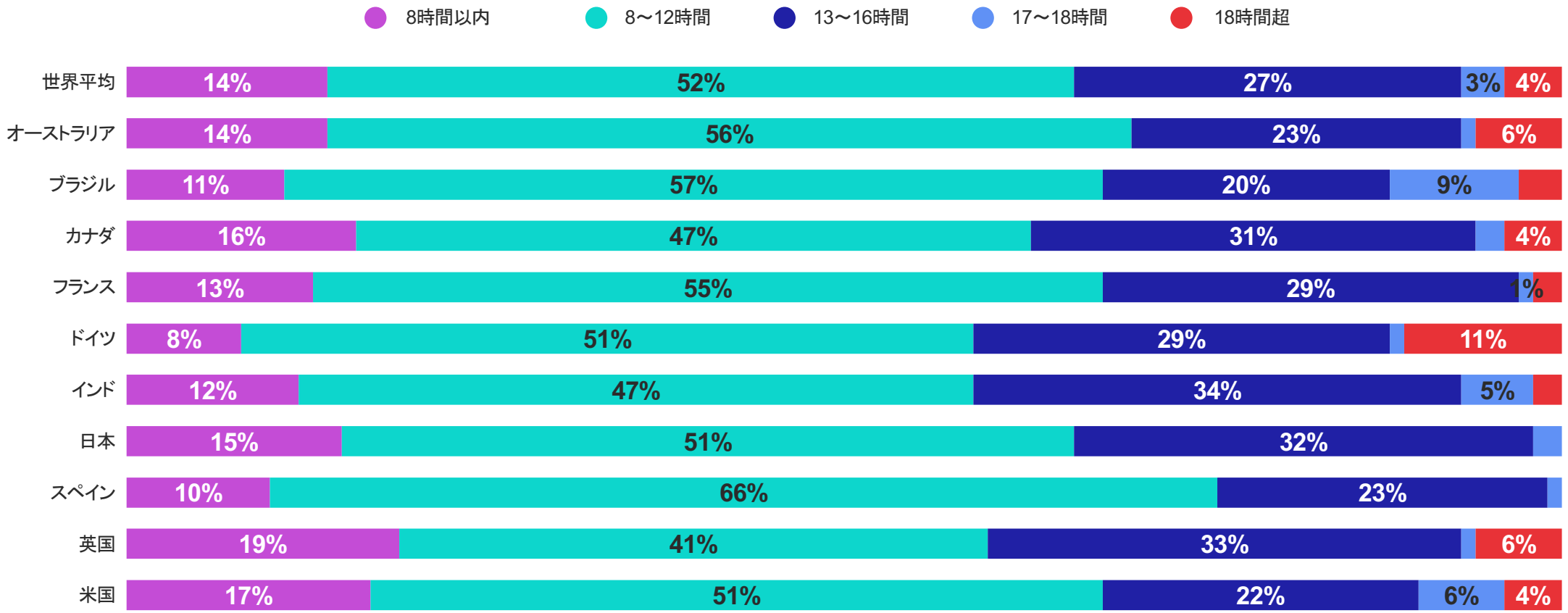
サイバーセキュリティー・インシデントに対応する際、最もストレス/要求が高い時期はいつですか？



MORNING CONSULT

3分の1超が、対応期間中の最もストレスの多い時期に、1日12時間以上働いていると回答

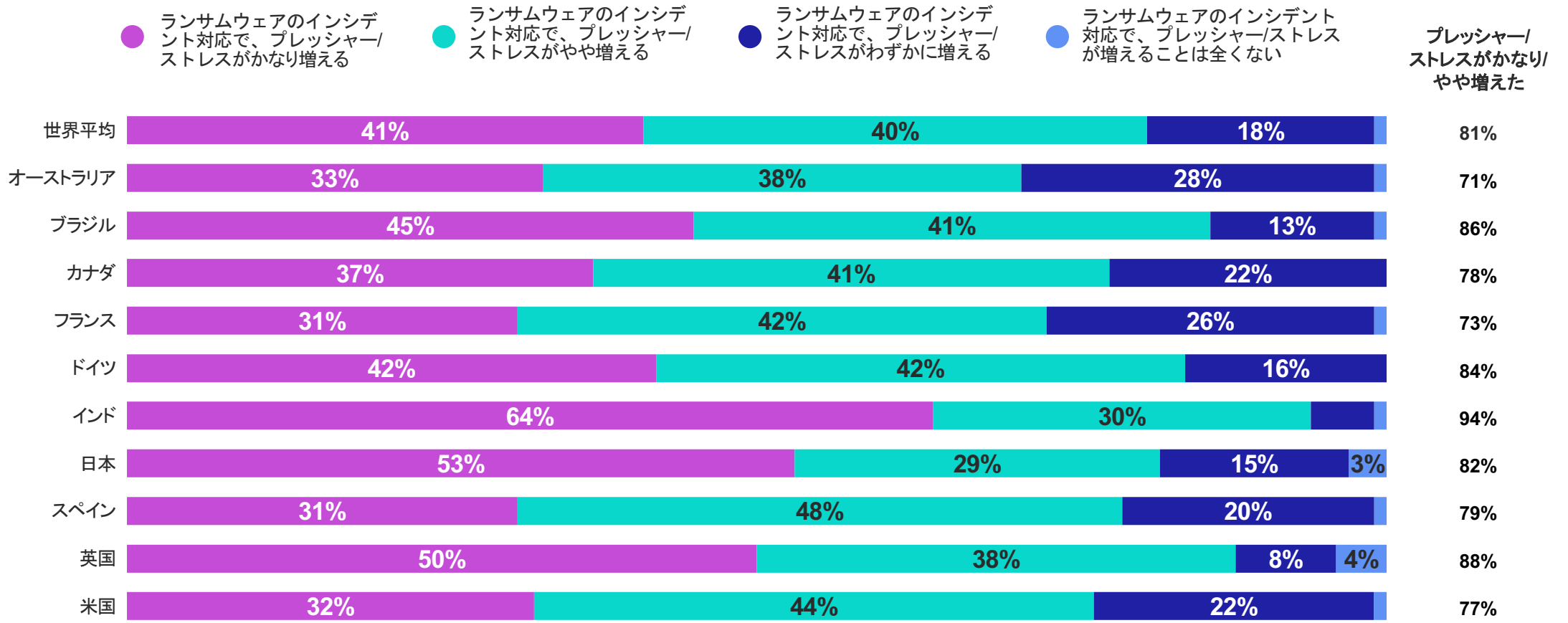
サイバーセキュリティー・インシデントに対応する際、最もストレスの多い期間中は1日平均何時間働いていますか？



MORNING CONSULT

全市場のサイバーセキュリティー・インシデント対応者の大半が、ランサムウェアの台頭により、サイバーセキュリティー・インシデント対応時のストレス/心理的要求が悪化したと考えており、全体で81%がこの所感を報告

ランサムウェアの台頭により、サイバーセキュリティー・インシデント対応時のストレス/心理的要求はどの程度悪化したと思いますか？



アジェンダ

サイバーセキュリティー・インシデント対応者であることに
対する所感

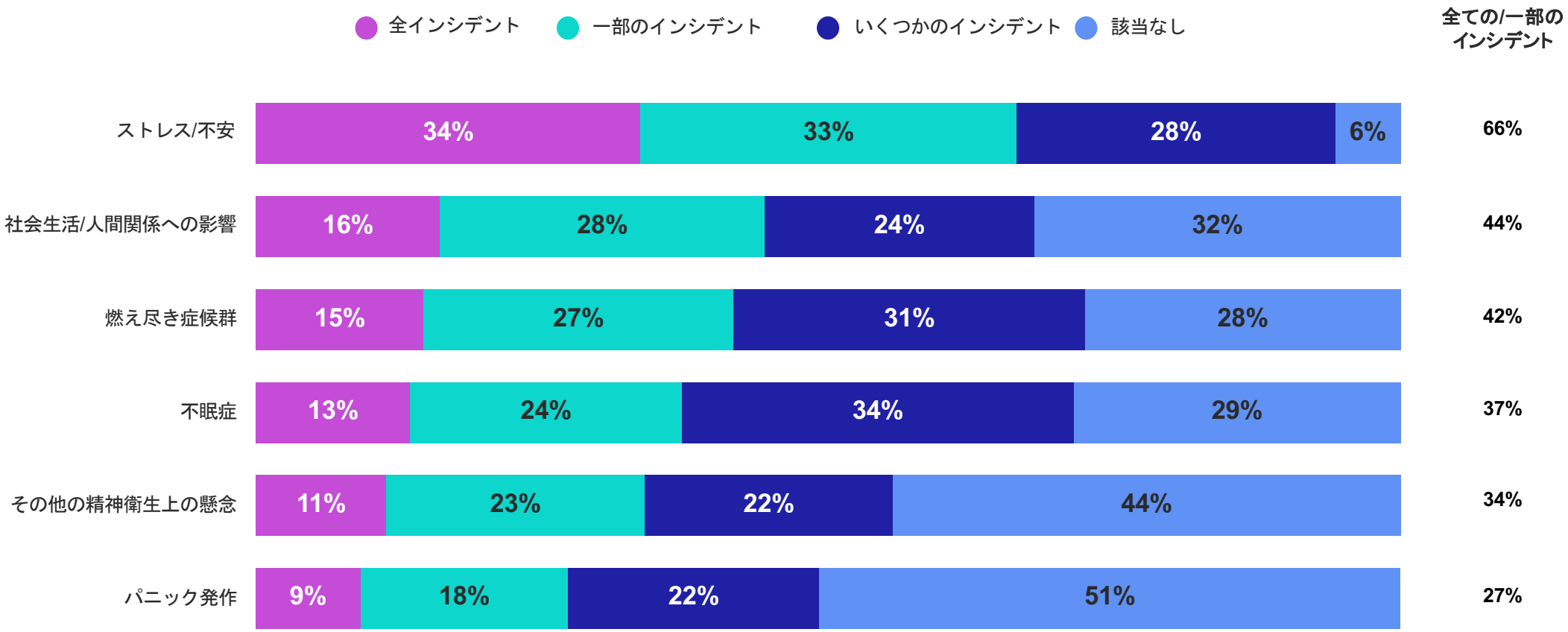
サイバーセキュリティー・インシデント対応時のストレス要因

メンタルヘルスと健康への影響

MORNING CONSULT

インシデント対応時のサイバーセキュリティー・インシデント対応者の所感/状況は、ストレス/不安が最も一般的（66%）だが、40%以上がサイバーセキュリティー・インシデント対応による社会生活/人間関係への影響（44%）と燃え尽き症候群（42%）を報告している

サイバーセキュリティー・インシデントへの対応中に、次のような所感/状況を経験したことはどの程度ありますか？



MORNING CONSULT

すべての国において、サイバーセキュリティー・インシデント対応中、最もよくある所感/状況はストレス/不安

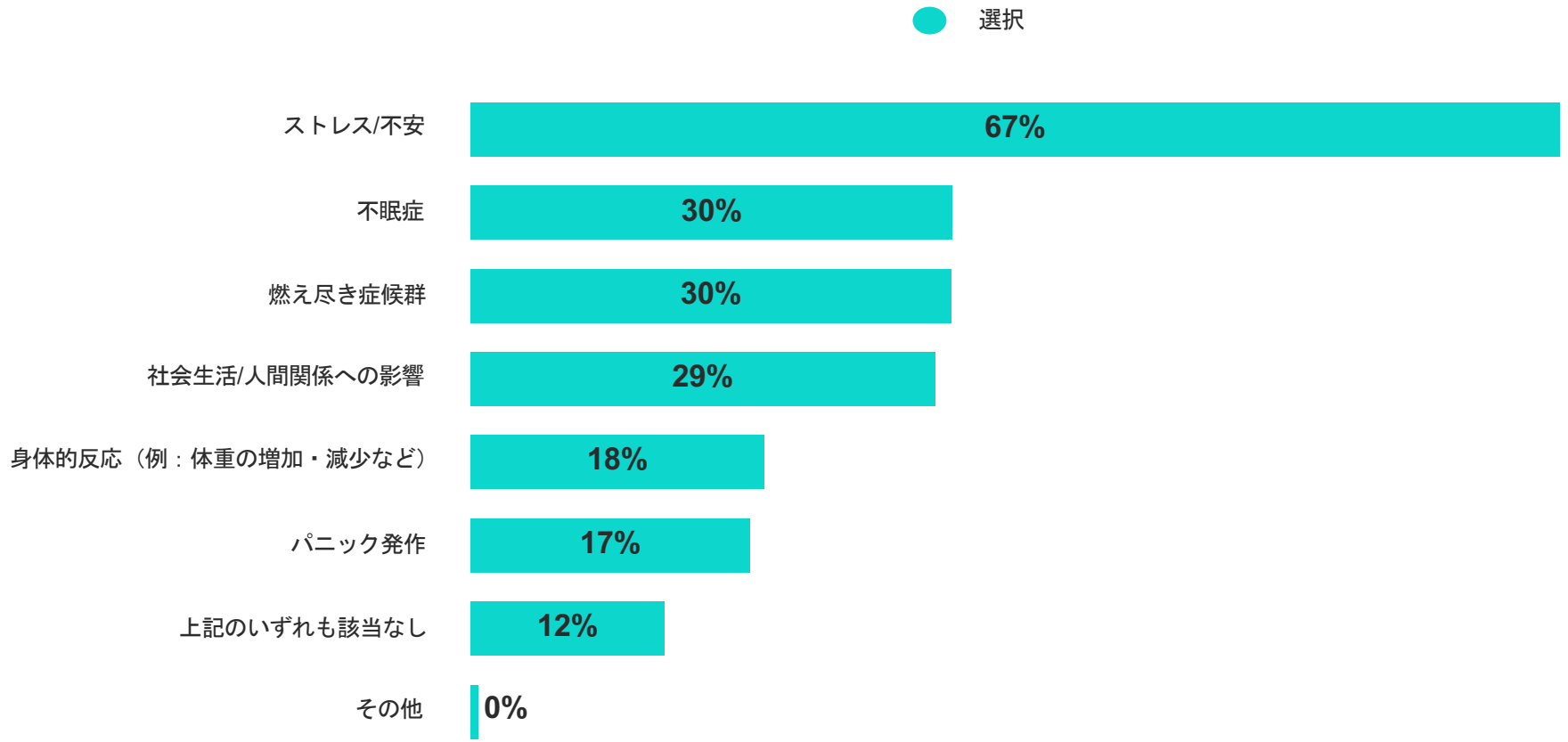
サイバーセキュリティー・インシデントへの対応中に、次のような所感/状況を経験したことはどの程度ありますか？ [全ての/一部のインシデントの割合を表示]

	米国	英国	ドイツ	カナダ	オーストラリア	フランス	スペイン	ブラジル	日本	インド
燃え尽き症候群	35	45	23	47	24	21	69	59	46	56
ストレス/不安	64	65	62	63	60	56	71	79	65	83
パニック発作	25	22	26	30	24	23	19	32	20	55
不眠症	34	29	34	34	22	30	48	62	33	50
社会生活/人間関係への影響	42	47	42	44	30	35	43	49	45	71
その他の精神衛生上の懸念	27	26	26	26	33	21	19	58	47	64

MORNING CONSULT

サイバーセキュリティー・インシデント対応者の3分の2（67%）が、サイバーセキュリティー・インシデント対応の結果、日常生活でストレス/不安を経験し、約30%が不眠（30%）、燃え尽き症候群（30%）、社会生活/人間関係への影響（29%）も経験

サイバーセキュリティー・インシデントに対応した結果、日常生活で以下のようなことを経験しましたか？ 該当するものをすべて選んでください。 [選択した割合（%）を表示]



MORNING CONSULT

英国、スペイン、ブラジルでは、サイバーセキュリティー・インシデント対応の結果、日常生活でストレス/不安を経験する傾向が高く、 スペインでは、他の国よりも高い割合でサイバーセキュリティー・インシデント対応者が燃え尽き症候群を経験していると報告

サイバーセキュリティー・インシデントに対応した結果、日常生活で以下のようなことを経験しましたか？ 該当するものをすべて選んでください。 [選択した割合（%）を表示]

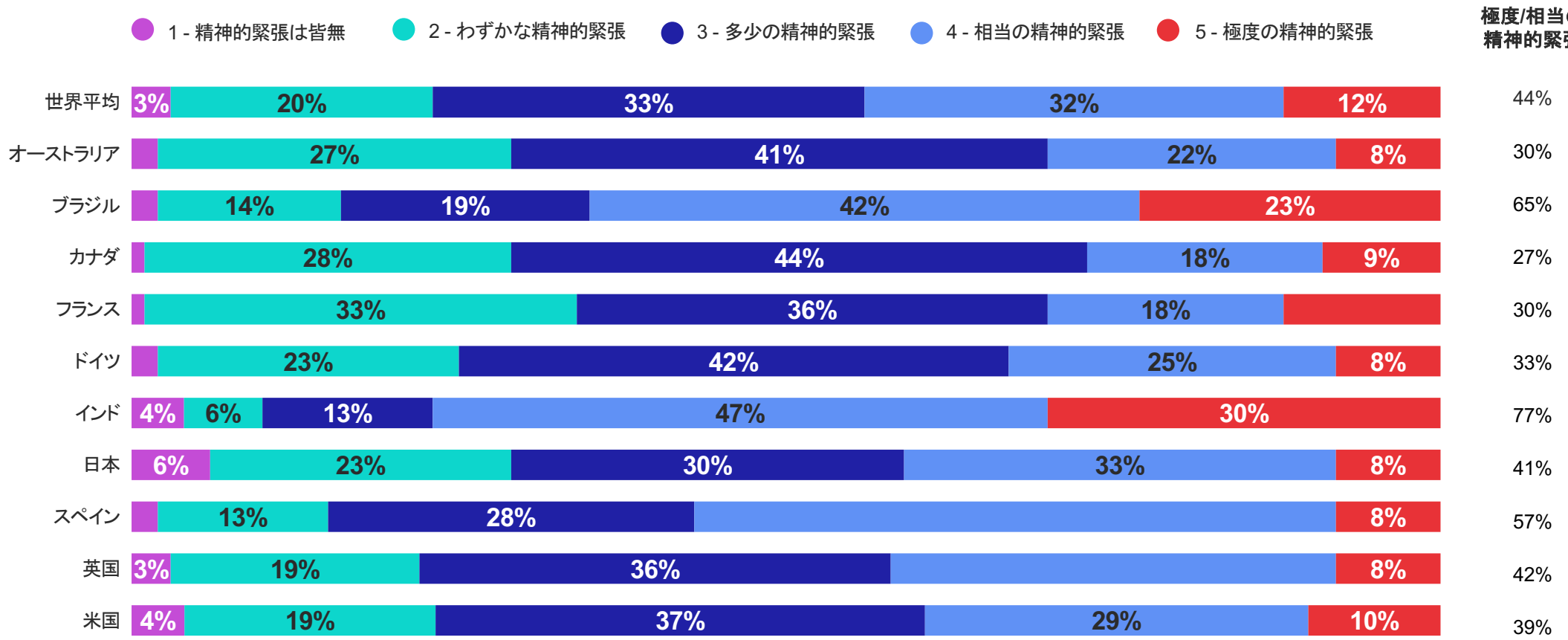
	米国	英国	ドイツ	カナダ	オーストラリア	フランス	スペイン	ブラジル	日本	インド
燃え尽き症候群	27	38	20	34	11	21	52	34	26	35
ストレス/不安	61	78	69	63	50	64	74	84	65	68
パニック発作	17	17	6	16	9	18	16	22	9	41
不眠症	20	20	36	24	14	36	42	60	20	34
社会生活/人間関係への影響	30	35	28	21	14	23	31	34	17	51
身体的反応（例：体重の増加・減少など）	16	12	15	15	16	10	16	28	20	34
上記のいずれも該当なし	10	7	6	18	31	13	8	● 3	13	

3%未満の回答は除外

MORNING CONSULT

サイバーセキュリティー・インシデント対応者の40%超が、大規模なサイバーセキュリティー・インシデント対応の結果、極度、またはかなりの精神的緊張を経験したと答えており、ブラジル（65%）、インド（77%）、スペイン（57%）でこの所感を表明する傾向が高い

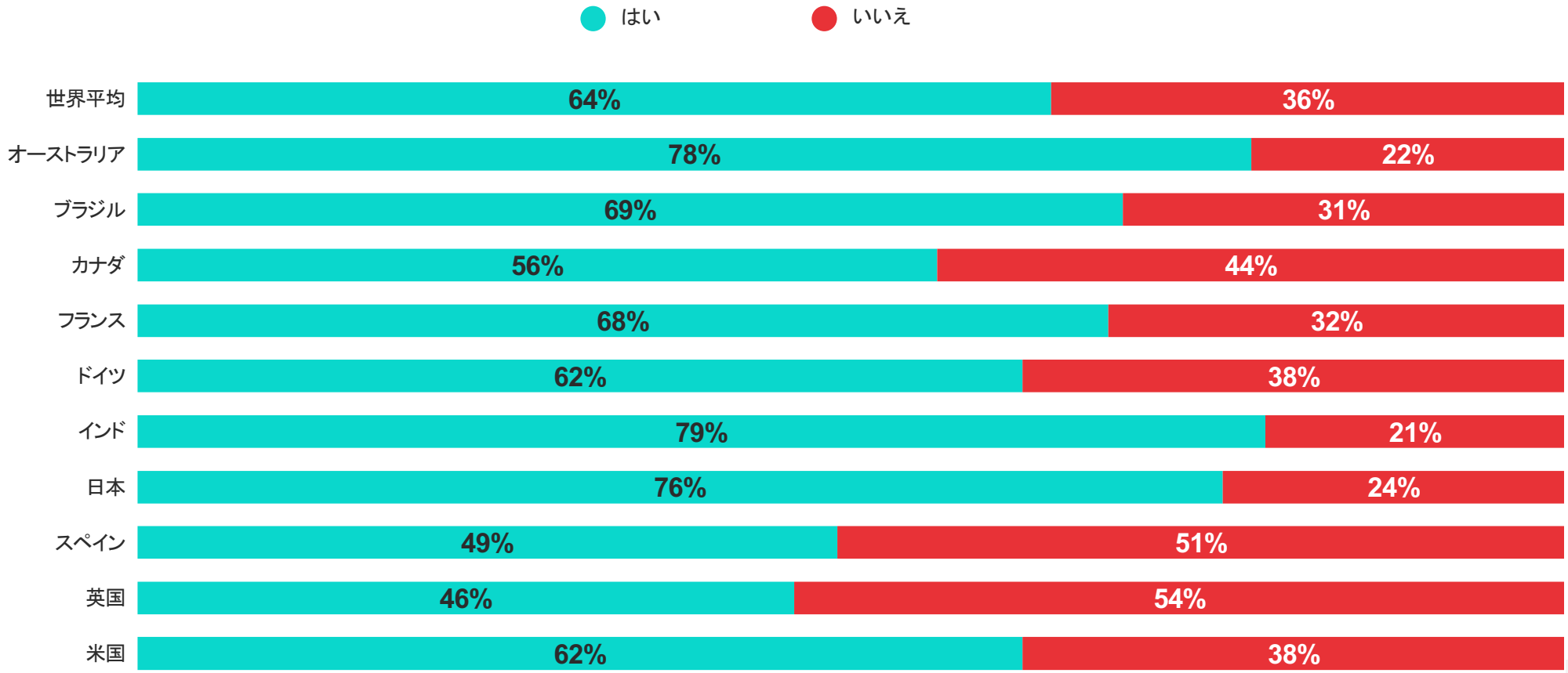
大規模なサイバーセキュリティー・インシデント（WannaCry（2017年）、NotPetya（2017年）、SolarWinds（2021年）、Kaseya（2022年）など）への対応で被った精神的緊張を1～5段階評価で、1を「ほとんど負担はない」、5を「極度の精神的負担」とした場合、どのようにランク付けしますか？



MORNING CONSULT

64%がサイバーセキュリティー・インシデント対応の結果、心の健康のサポートを求めたことがあり、オーストラリア（78%）、インド（79%）、日本（76%）では、心の健康のサポートを求めたと回答する割合が他の国よりも高い

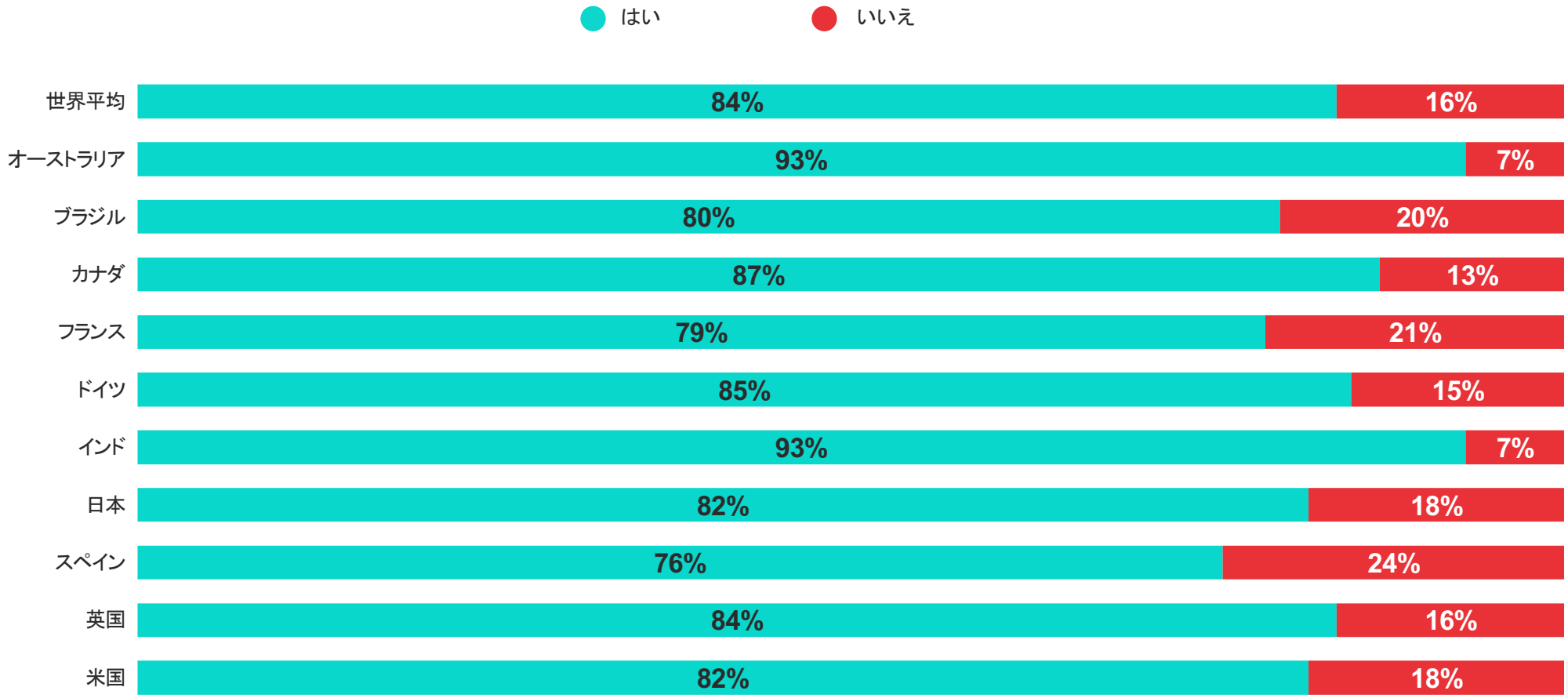
サイバーセキュリティー・インシデント対応の結果として、心の健康のサポートを求めたことがありますか？



MORNING CONSULT

サイバーセキュリティー・インシデント対応者の大半が、適切なメンタルヘルスのサポートリソースが利用可能だと回答しており、全体で84%がそのように回答

適切なメンタルヘルスサポートのリソースを利用できると思いますか？



MORNING CONSULT

インシデント対応者を成功に導くために企業が取るべきステップ

インシデント対応者は、常に拡大し続ける環境を、進化を続ける攻撃的な脅威から保護する使命があります。 サイバー危機に危機感はつきものですが、企業がサイバー危機に備えることで、迅速かつコスト効率の高い対応と復旧を実現し、インシデント対応者の不要なプレッシャーを軽減することができます。 企業のサイバー準備対策とインシデント対応の有効性を高めるための2つの重要なステップをご紹介します。

1. **詳細なインシデント対応計画とプレイブックを作成する**： 各企業の環境、技術、リソースに合わせてカスタマイズした計画とプレイブックを作成することが重要です。 こうすれば、企業はセキュリティー・インシデント発生時に必要なリソースを前もって確保し、連絡網を確立するとともに、インシデント対応の保持契約を締結し、サイバー危機発生時にインシデント対応サービスを容易に利用できるようにすることができます。

2. **プレッシャー下でのインシデント対応のリハーサルとテストを行う**： 組織のセキュリティー・チームがサイバー攻撃によって試されるのは、もはや「もしも起きたら」ではなく「いつ起きるか」の問題です。 シミュレーション演習を行うことで、組織とセキュリティー・チームは、プレッシャー下で対応するのがどのようなものかを実感し、実際のセキュリティー事象が発生したときに効果的に活動するために改善すべきギャップや領域、プロセスを特定することができます。 これには、外部のセキュリティー・チームが自社の対応チームに正しく統合されているかどうかを確認することも含まれます。

その他のリソース

– IBM Securityのインシデント対応者向け ウェビナー（2022年10月12日米国東部標準時13時）に登録する
– IBM Security X-Forceコンサルティングを予約する
– IBM Security X-Force のインシデント対応サブスクリプションの詳細を確認する