1000人の声プロジェクト
1000人の声を届けよう

中部経済同友会 1000人の声プロジェクト × 安全保障から経営を考える委員会

経済安全保障に関するアンケート調査結果

1．アンケート調査の概要

【アンケートの目的】

- 米中対立やロシアによるウクライナ侵攻などにより、経済安全保障に関する企業の取組・対策が極めて重要になってきている。
- 中部地区企業の経済安全保障に関する実態と課題を把握することを目的に、アンケート調査を実施した。

【アンケート期間】

- 2023年7月24日（月）～8月18日（金）まで

【アンケート回答社数】

- 114社

中小企業	48社
大企業	64社
無回答	2社

依頼文

中部経済同友会
会員各位

中部経済同友会　安全保障から経営を考える委員会×1000人の声プロジェクト
会員アンケート「経済安全保障に関するアンケート調査」

日頃は本会活動にご支援いただき、誠にありがとうございます。
当委員会は「企業を取り巻く安全保障の本質を理解する」をテーマに、不確実な社会によって安全保障上のリスクが多様化する中で、対応に苦慮する企業への一助となる活動を目指しております。
今年度末には活動報告書の発表を予定しております。
このたび、会員企業の皆様から、経済安全保障に関する取り組み状況や課題をお聞きしたく、アンケート調査を実施することといたしました。
ぜひとも回答へのご協力をお願いいたします。
調査結果については個別の企業および団体名を伏せた形で、会員の皆様にお知らせするとともに、活動報告書においても活用させていただきます。

<ご留意事項>
○ 当アンケートは、本会会員の皆様全員に送信しております。
○ ご回答は、会員ご本人のほか、貴社のご担当の方にもご回答いただけます。
○ 設問は選択式（一部、任意で記述式あり）、計21問です。
○ 回答の一時保存ができませんので、お時間のあるときにご回答ください。
○ 調査結果については個別の企業および団体名を伏せた形で、会員の皆様にお知らせするとともに、報告書においても活用させていただきます。

1．アンケート調査の概要

【質問内容】

分野	設問	設問内容	回答方法
1. 企業属性	Q1～Q6	従業員数、業種等	ー
2. 経済安全保障全般	Q7	経済安全保障に対する意識	5択
	Q8	経済安全保障に対する取組み（問13種）	5択
	Q9	経済安全保障の取組み上の課題	14択（複数回答）
	Q10	米中対立の影響	12択（複数回答）
	Q11	ウクライナ侵攻に伴う対ロシア制裁の影響	13択（複数回答）
3. サプライチェーン	Q12	サプライチェーン上の課題	14択（複数回答）
	Q13	サプライチェーン強靭化に向けた取組み（問13種）	3択（実施の場合は具体的取組を記載）
	Q14	レジリエンスの維持・向上に向けての政府への要望事項	12択（複数回答）
	Q15	中小企業の大企業に対する要望、大企業の中小企業に対する要望事項	12択（複数回答）
4. サイバーセキュリティ	Q16	サイバーセキュリティ対策上の課題	9択（複数回答）
	Q17	「サイバーセキュリティ経営ガイドライン(Ver3.0)」に対する取組み（問13種）	3択（実施の場合は具体的取組を記載）
	Q18	レジリエンスの維持・向上に向けての政府への要望事項	8択（複数回答）
	Q19	中小企業の大企業に対する要望、大企業の中小企業に対する要望事項	11択（複数回答）
5. その他	Q20	その他政府への要望事項	13択（複数回答）
	Q21	経済安全保障全般に対する意見等	自由回答

2．アンケート調査の結果（主なポイント）

1 経済安全保障全般

- ✓ ７割以上の企業が「強く意識している」または「ある程度意識している」と回答。但し、中小企業では「強く意識している」との回答は約１割にとどまった。
- ✓ 各取組状況では、全体として、情報管理体制やサイバーセキュリティの強化に「取り組んでいる」および「今後取り組む予定」を合わせた回答は8割以上と最多。
- ✓ 一方で、専門部署や担当役員の設置、社内研修や専門人材の育成に「取り組んでいる」および「今後取り組む予定」を合わせた回答は2～3割程度と低調。さらに中小企業ではその割合が低く、専門人材育成に「取り組んでいる」との回答はゼロ。
- ✓ 取り組みを推進する上での課題は、企業規模を問わず、「情報の適時切々な取得」「取引企業の動向把握」「自社における事業リスクの把握」が上位を占めた。

2 米中対立、ロシアによるウクライナ侵攻の影響

- ✓ 米中対立の影響は、全体および大企業では「中国の規制強化によるコスト増」とする回答が最多。中小企業では「取引や売上の減少」との回答が多かった。
- ✓ ロシアによるウクライナ侵攻の影響は、企業規模を問わず「仕入価格の高騰」とする回答が他項目を引き離して最多。次いで「物流の遅延・物流コストの増加」との回答が多かった。
- ✓ 一方で、それぞれ全く影響のないとの回答も全体では約2割。中小企業では３割程度。





2．アンケート調査の結果（主なポイント）

3 **サプライチェーン**

- ✓ 課題は、全体では「調達コスト、物流コスト増大への対応」とする回答が最多。また、大企業では「BCPの策定と実行」との回答が多かった。
- ✓ 各取組状況では、いずれの項目も「実施している」および「実施する予定」を合わせた回答は5割以上。但し、中小企業では「最適化を担う人材の確保・育成」「他企業との連携体制強化」を実施しているとの回答が低調。
- ✓ 政府への要望は、企業規模を問わず「サーバーセキュリティの強化」が最多。
- ✓ サプライチェーンのレジリエンス向上に向けて、中小→大企業、大→中小企業に求めることは、どちらからも「サイバーセキュリティ対策の共有」とする回答が最多。

4 **サイバーセキュリティ**

- ✓ 課題は、全体では「高度化・巧妙化するサイバー攻撃への対応」「専門人材の育成」「従業員教育の徹底」の順に多い。中小企業では「コスト負担の増大」とする回答が最多。
- ✓ 経営ガイドラインについて、「実施している」および「実施する予定」を合わせた回答は概ね7割程度。大企業ではほぼ8割超。一方で、「実施している」と回答した割合は、大企業と中小企業で大きな格差があった。
- ✓ 政府への要望は、全体として「サイバーセキュリティ強靭化に関する助成金・補助金の充実」とする回答が最多。
- ✓ サイバーセキュリティ対策の強化を図る上で、中小→大企業、大→中小企業に求めることは、サプライチェーンと同様に、どちらからも「サイバーセキュリティ対策の共有」とする回答が最多。いかに企業間の情報連携・共有を図っていくのかが求められる。

5 **政府への要望（サプライチェーン・サイバー以外）**

- ✓ 全体では「資源・エネルギーの自給率向上」「日本政府のインテリジェンス能力の強化」「基幹インフラの信頼性・安全性向上」の順に多かった。
- ✓ 大企業では「日本政府のインテリジェンス能力強化」とする回答が最多。中小企業では「資源・エネルギーの自給率向上」に次いで「日本の財政の健全化」「食糧自給率の向上」の順に多かった。

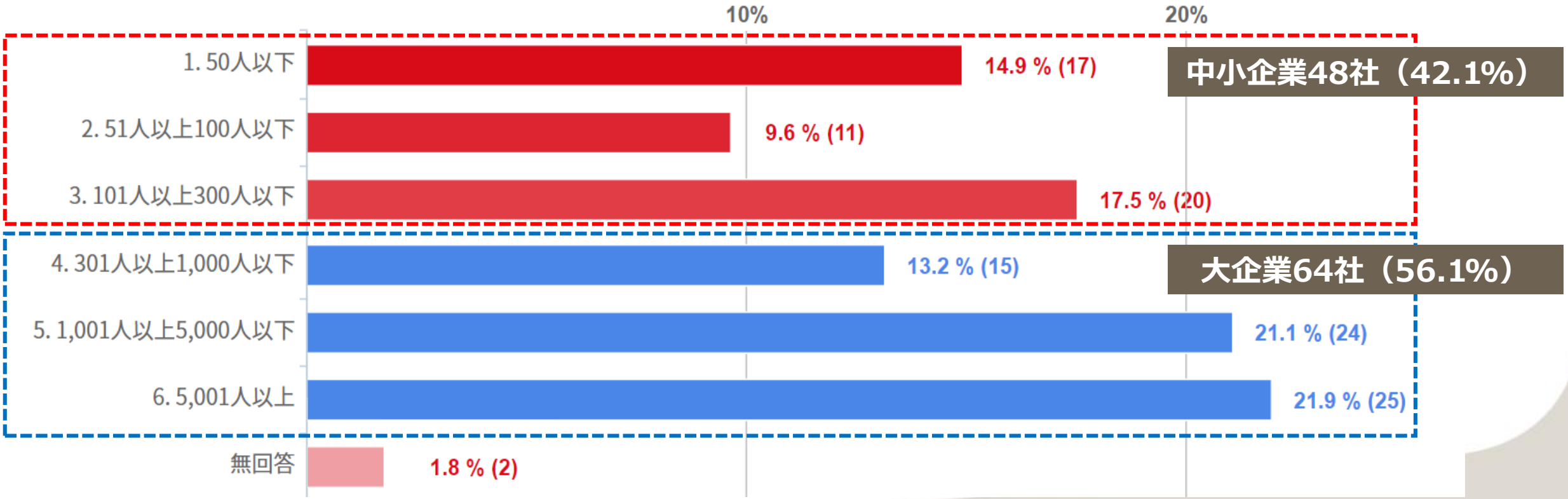
３．アンケート調査の結果

（１）回答企業の属性

企業規模（従業員数）

従業員数300人以下を中小企業、301人以上を大企業と定義する（中小企業庁による中小企業定義（製造業その他）に基づく）。

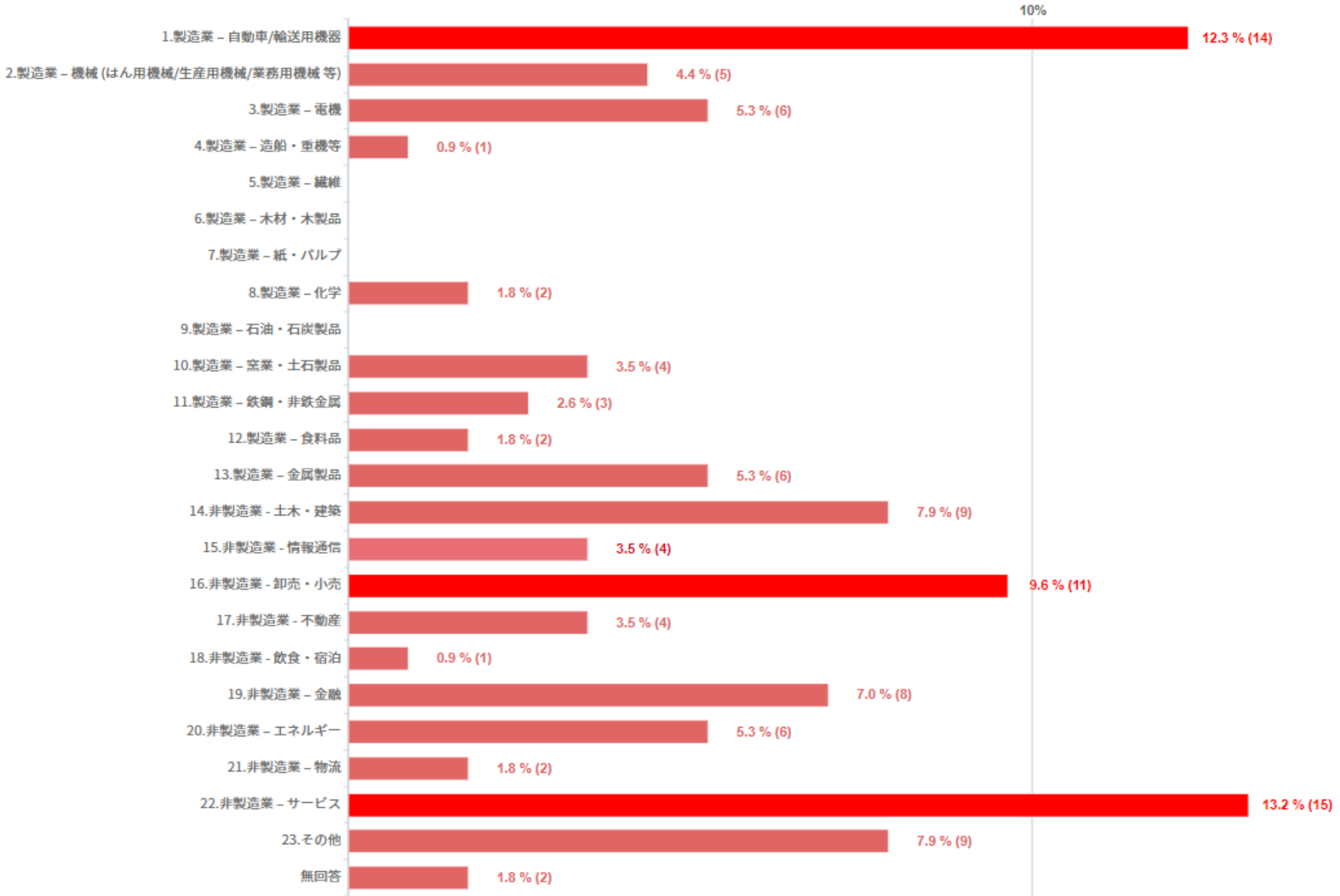
（N＝114）



（１）回答企業の属性

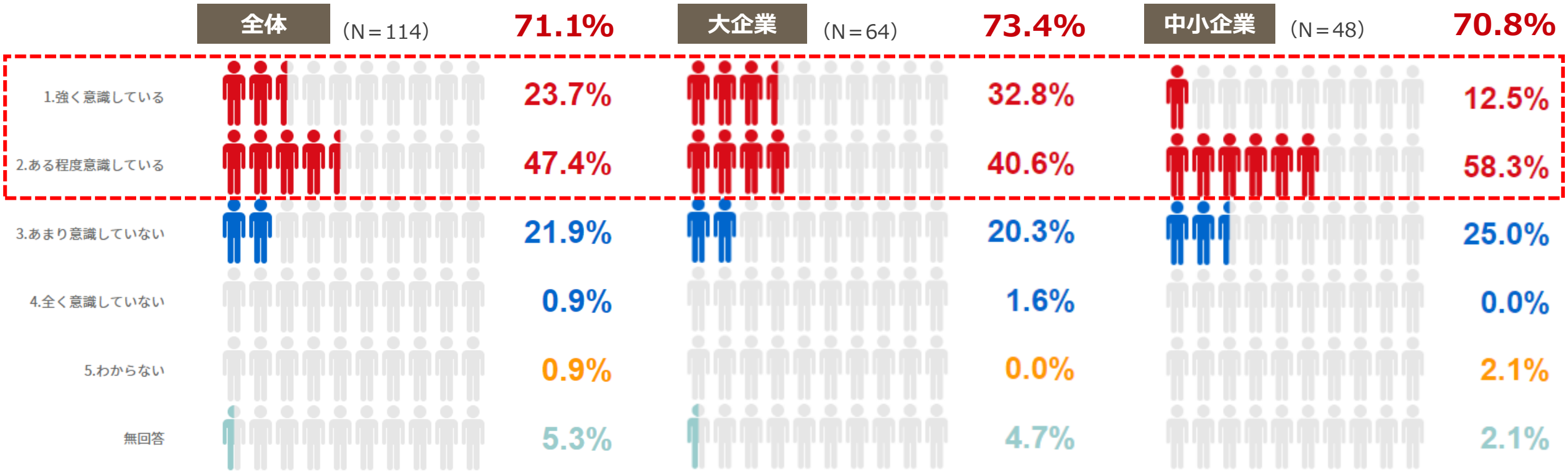
業種

（N＝114）



（２）経済安全保障全般

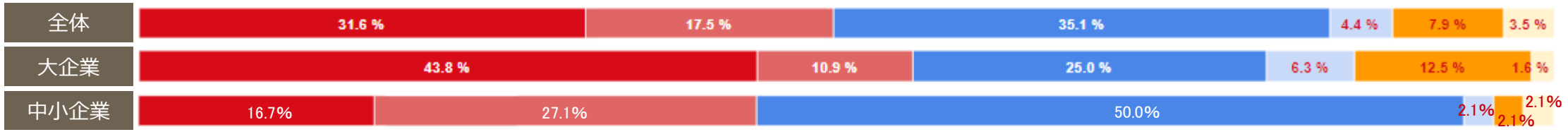
Q7.経済安全保障について、どの程度**意識**していますか。



（２）経済安全保障全般

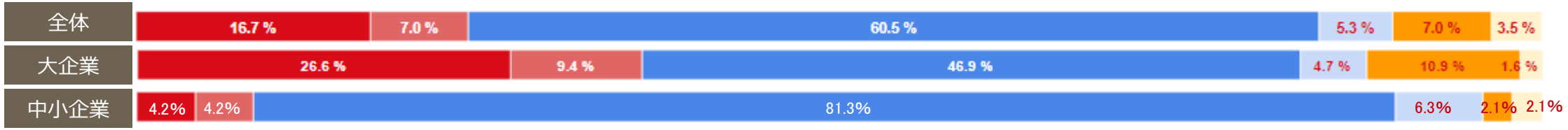
Q8.貴社の経済安全保障に向けた**取り組み状況**について教えてください。

1.取締役会や役員会での議題として取り扱い



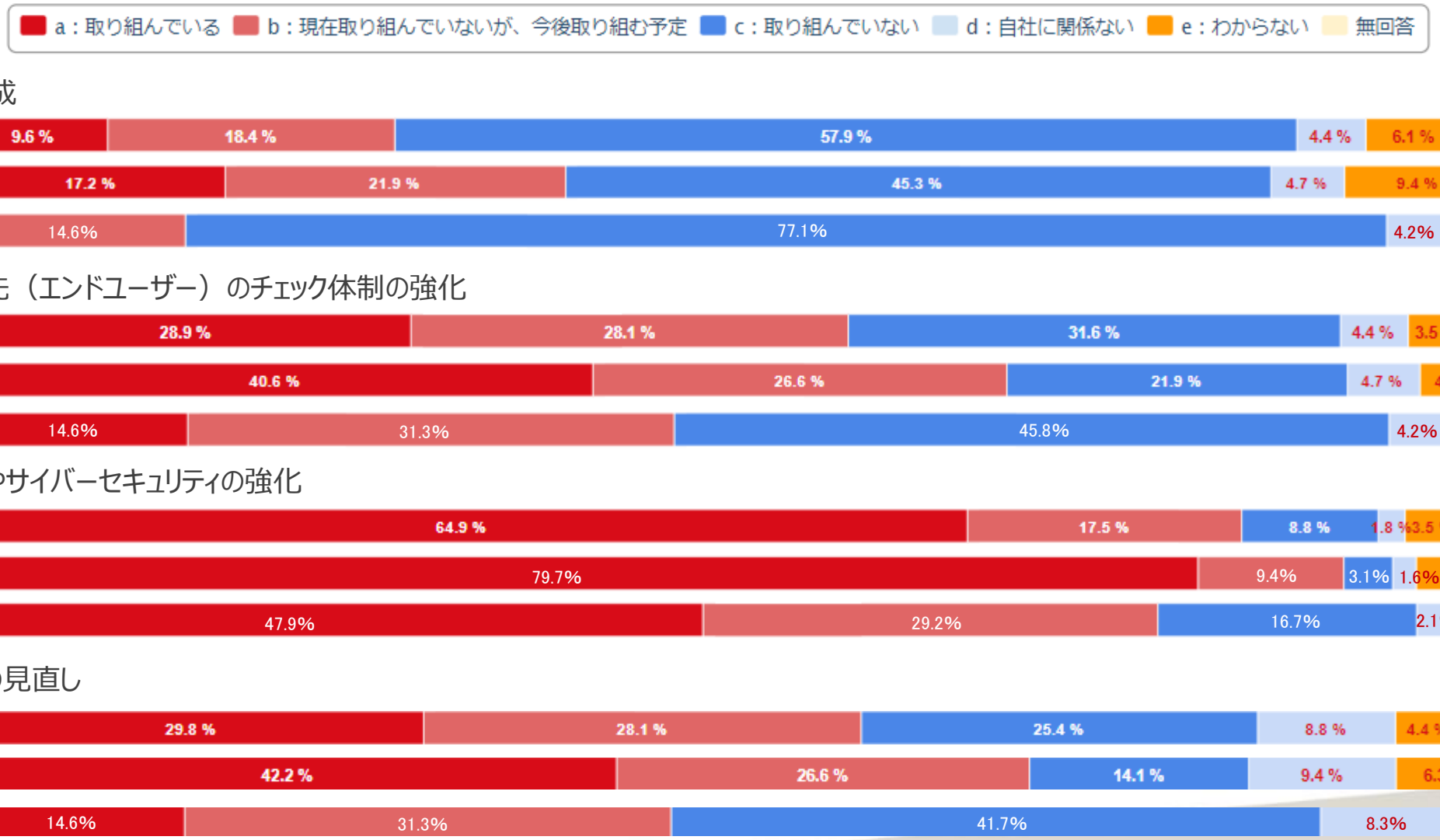
2.社内研修の開催

3.専門部署の設置



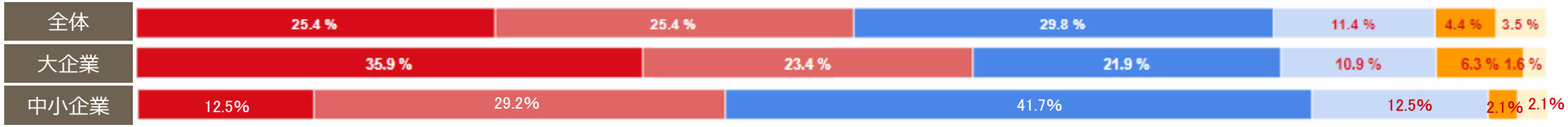
4.担当役員の設置

（２）経済安全保障全般

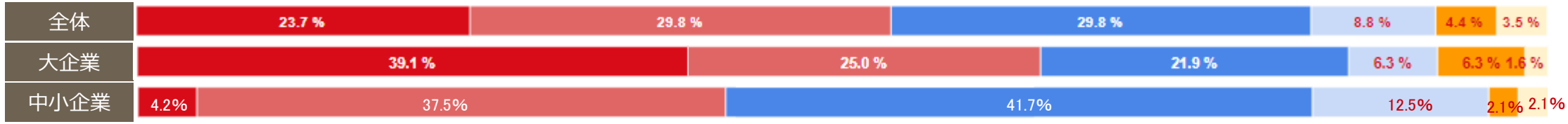

a：取り組んでいる
b：現在取り組んでいないが、今後取り組む予定
c：取り組んでいない
d：自社に関係ない
e：わからない
無回答
5.専門人材の育成
全体 9.6 % 18.4 % 57.9 % 4.4 % 6.1 % 3.5 %
大企業 17.2 % 21.9 % 45.3 % 4.7 % 9.4 % 1.6 %
中小企業 14.6% 77.1% 4.2% 2.1% 2.1%
6.取引先や需要先（エンドユーザー）のチェック体制の強化
全体 28.9 % 28.1 % 31.6 % 4.4 % 3.5 % 3.5 %
大企業 40.6 % 26.6 % 21.9 % 4.7 % 4.7 % 1.6 %
中小企業 14.6% 31.3% 45.8% 4.2% 2.1% 2.1%
7.情報管理体制やサイバーセキュリティの強化
全体 64.9 % 17.5 % 8.8 % 1.8 % 3.5 % 3.5 %
大企業 79.7% 9.4% 3.1% 1.6% 4.7% 1.6%
中小企業 47.9% 29.2% 16.7% 2.1% 2.1% 2.1%
8.サプライチェーンの見直し
全体 29.8 % 28.1 % 25.4 % 8.8 % 4.4 % 3.5 %
大企業 42.2 % 26.6 % 14.1 % 9.4 % 6.3 % 1.6 %
中小企業 14.6% 31.3% 41.7% 8.3% 2.1% 2.1%

（２）経済安全保障全般

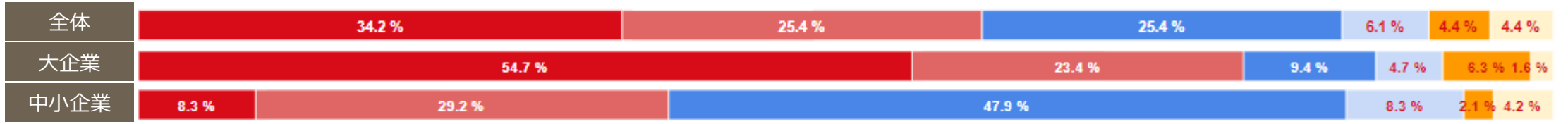
9.生産拠点の変更や多元化



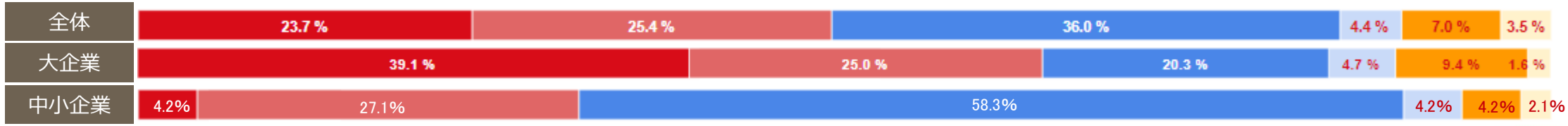
10.自社の技術について秘匿分野・領域の選定



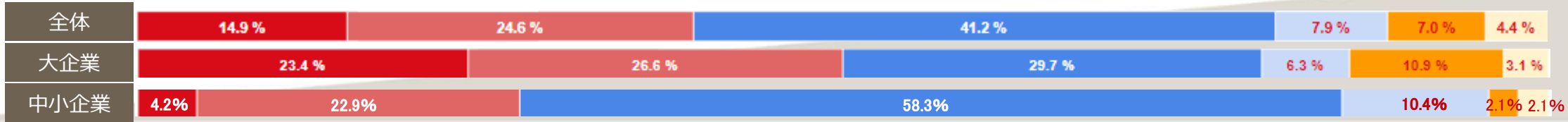
11.知的財産の取り扱いルールの策定



12.経済安全保障を踏まえた事業リスクの評価

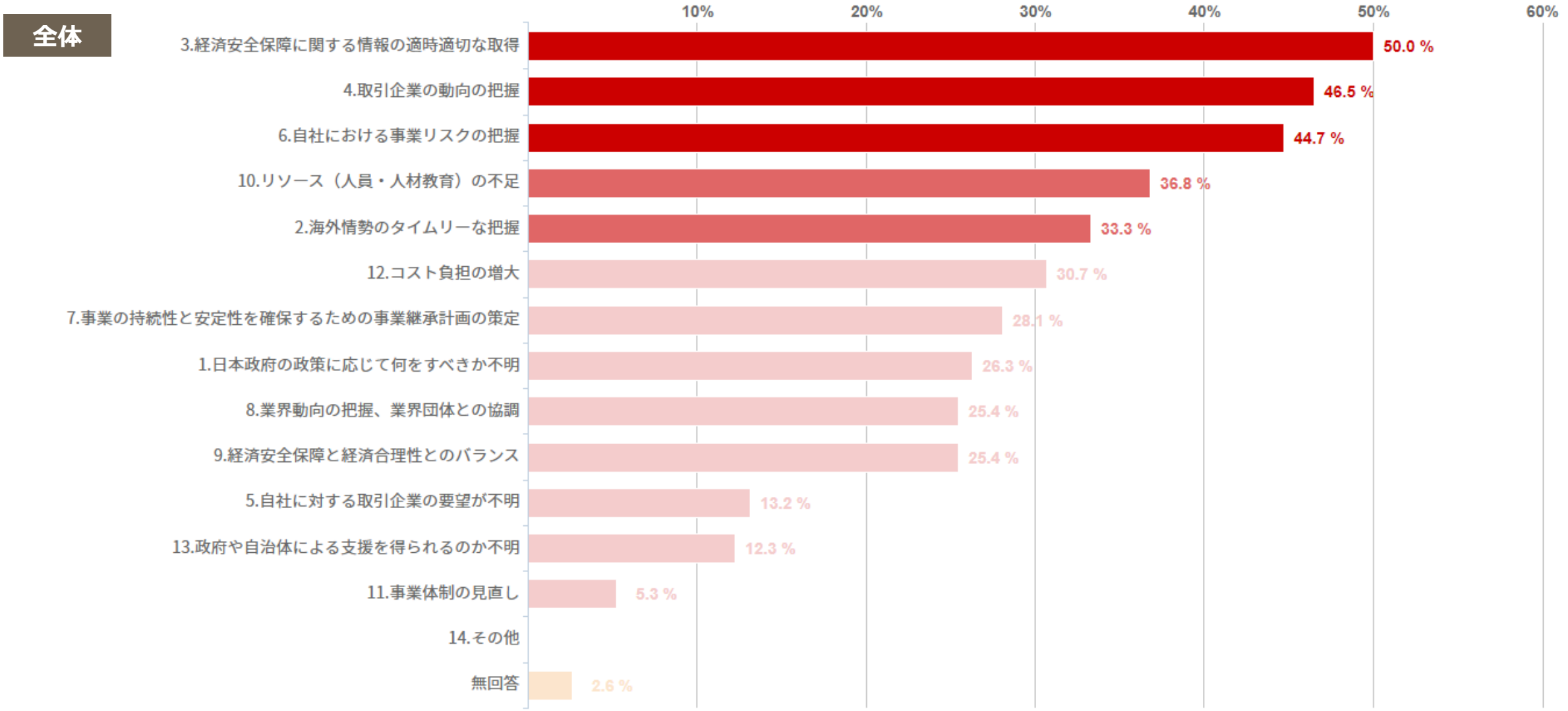


13.経済安全保障に関する社内規定・方針の策定



（２）経済安全保障全般

Q9. 経済安全保障に向けた取り組みを推進する上での**課題**は何ですか。（N＝114）

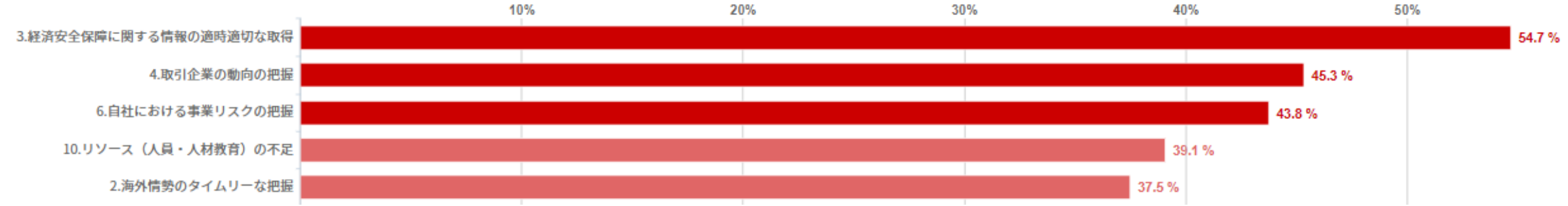


（２）経済安全保障全般

Q9. 経済安全保障に向けた取り組みを推進する上での**課題**は何ですか。（規模別；上位５）

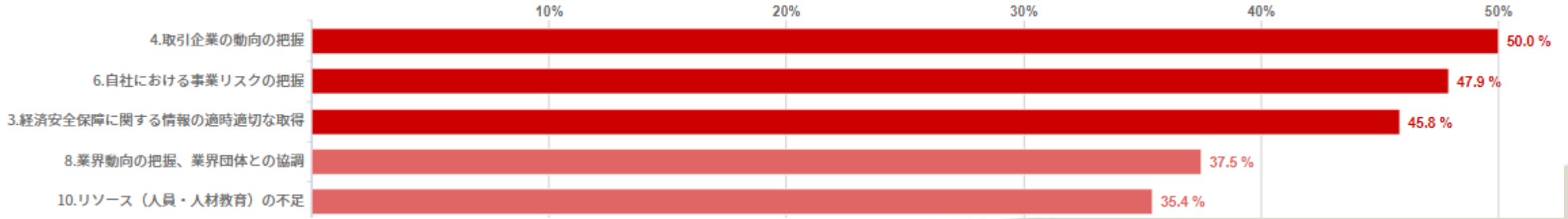
大企業

（N＝64）



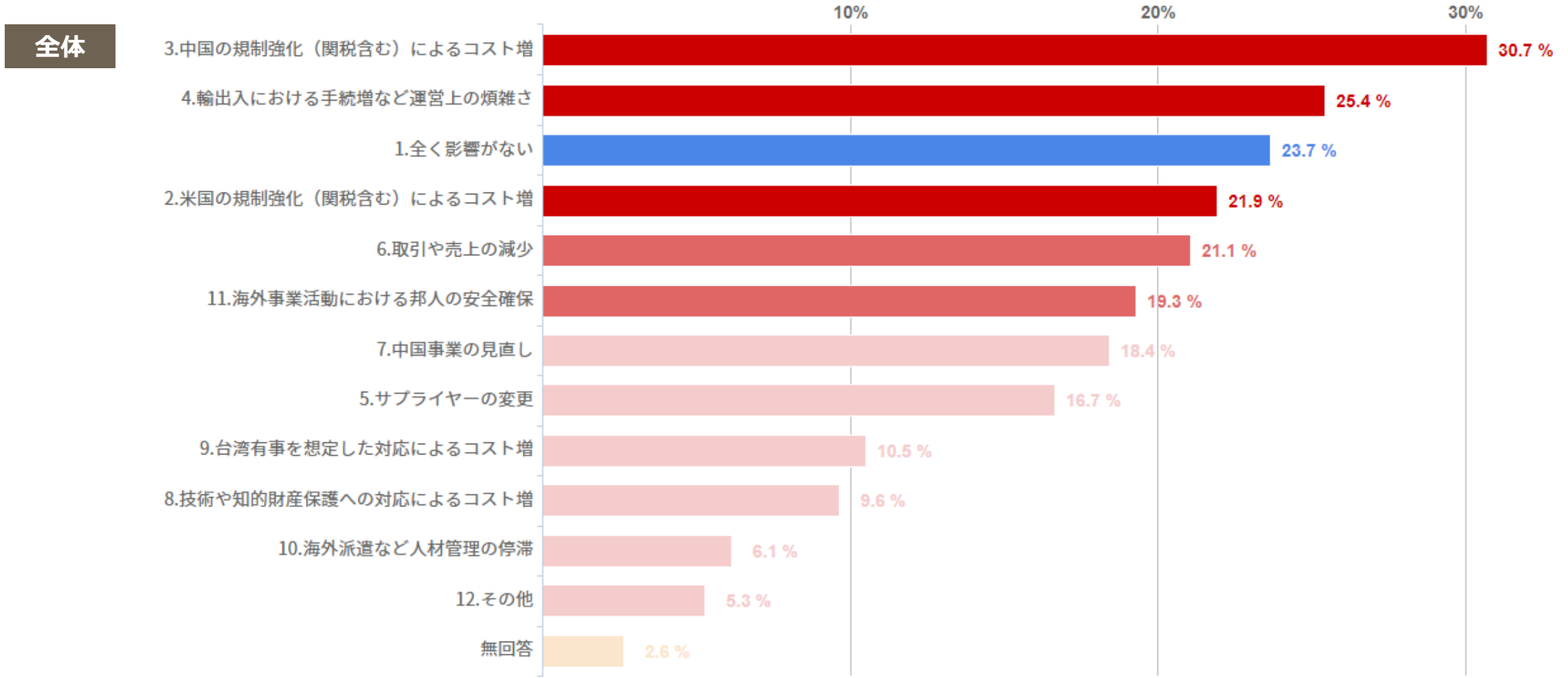
中小企業

（N＝48）



（２）経済安全保障全般

Q10. **米中対立**の影響は、貴社の事業に何らかの形で出ていますか。「影響が出ている」場合、もしくは今は影響が出ていない場合でも「今後想定される影響」があれば２以降より選択して下さい。なお、「全く影響がない」場合は１を選択してください。（N＝114）

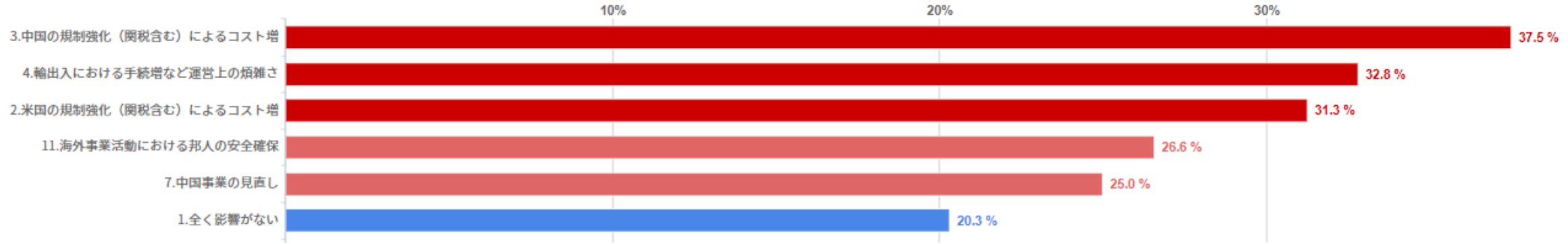


（２）経済安全保障全般

Q10. **米中対立**の影響は、貴社の事業に何らかの形で出ていますか。「影響が出ている」場合、もしくは今は影響が出ていない場合でも「今後想定される影響」があれば２以降より選択して下さい。なお、「全く影響がない」場合は１を選択してください。
（規模別；上位５）

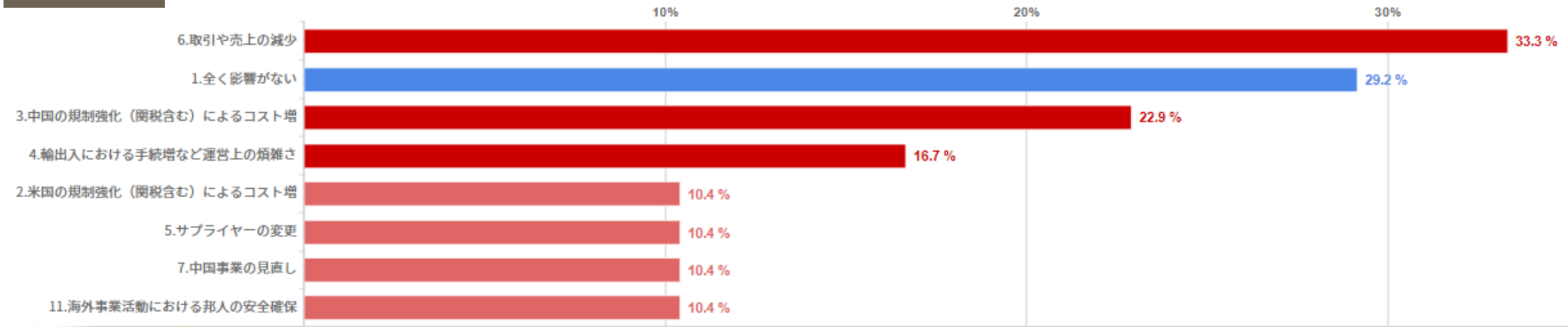
大企業

（N＝64）



中小企業

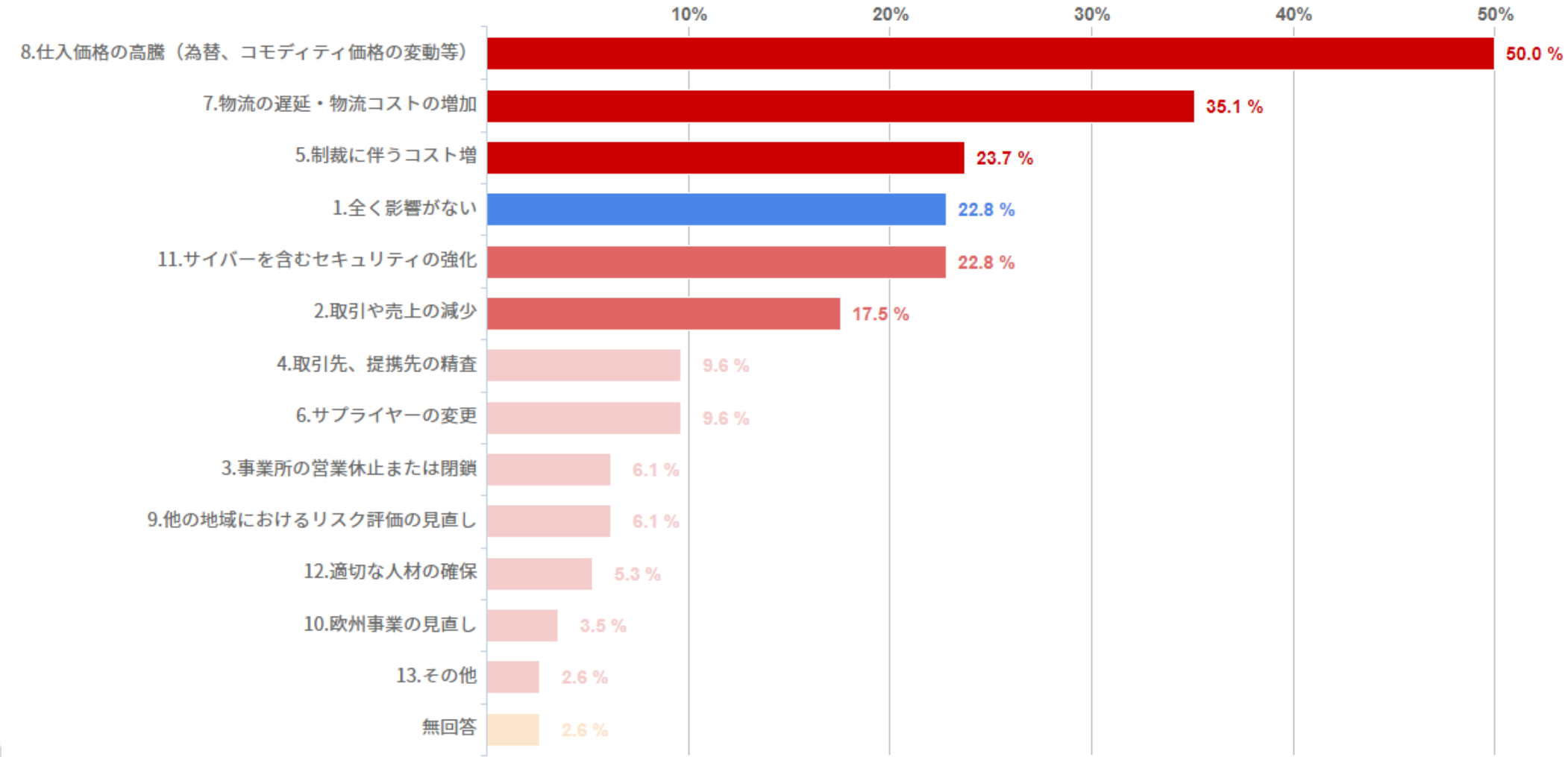
（N＝48）



（２）経済安全保障全般

Q11. **ロシアによるウクライナ侵攻**とこれに伴う対露制裁の影響は、貴社の事業に何らかの形で出ていますか。「影響が出ている」場合、もしくは今は影響が出ていない場合でも「今後想定される影響」があれば２以降より選択して下さい。なお、「全く影響がない」場合は１を選択してください。（N＝114）

全体

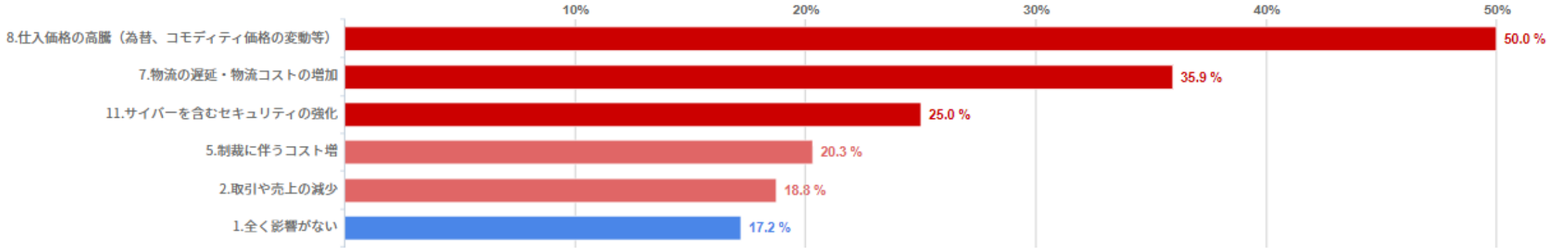


（２）経済安全保障全般

Q11. **ロシアによるウクライナ侵攻**とこれに伴う対露制裁の影響は、貴社の事業に何らかの形で出ていますか。「影響が出ている」場合、もしくは今は影響が出ていない場合でも「今後想定される影響」があれば２以降より選択して下さい。なお、「全く影響がない」場合は１を選択してください。（規模別；上位５）

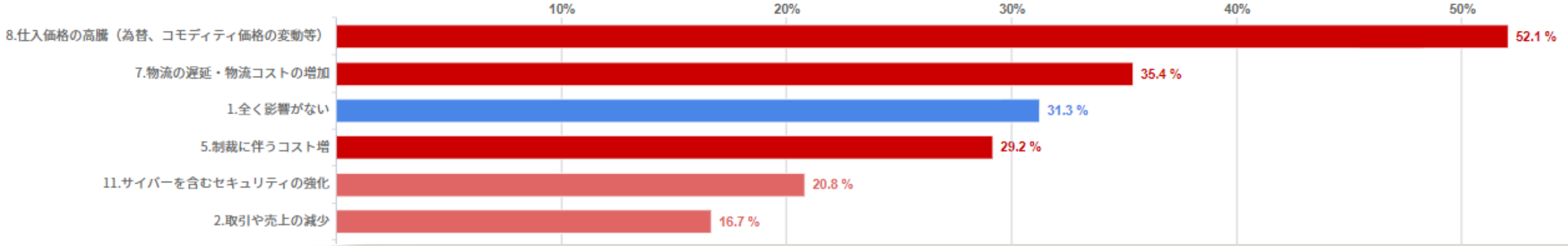
大企業

（N＝64）



中小企業

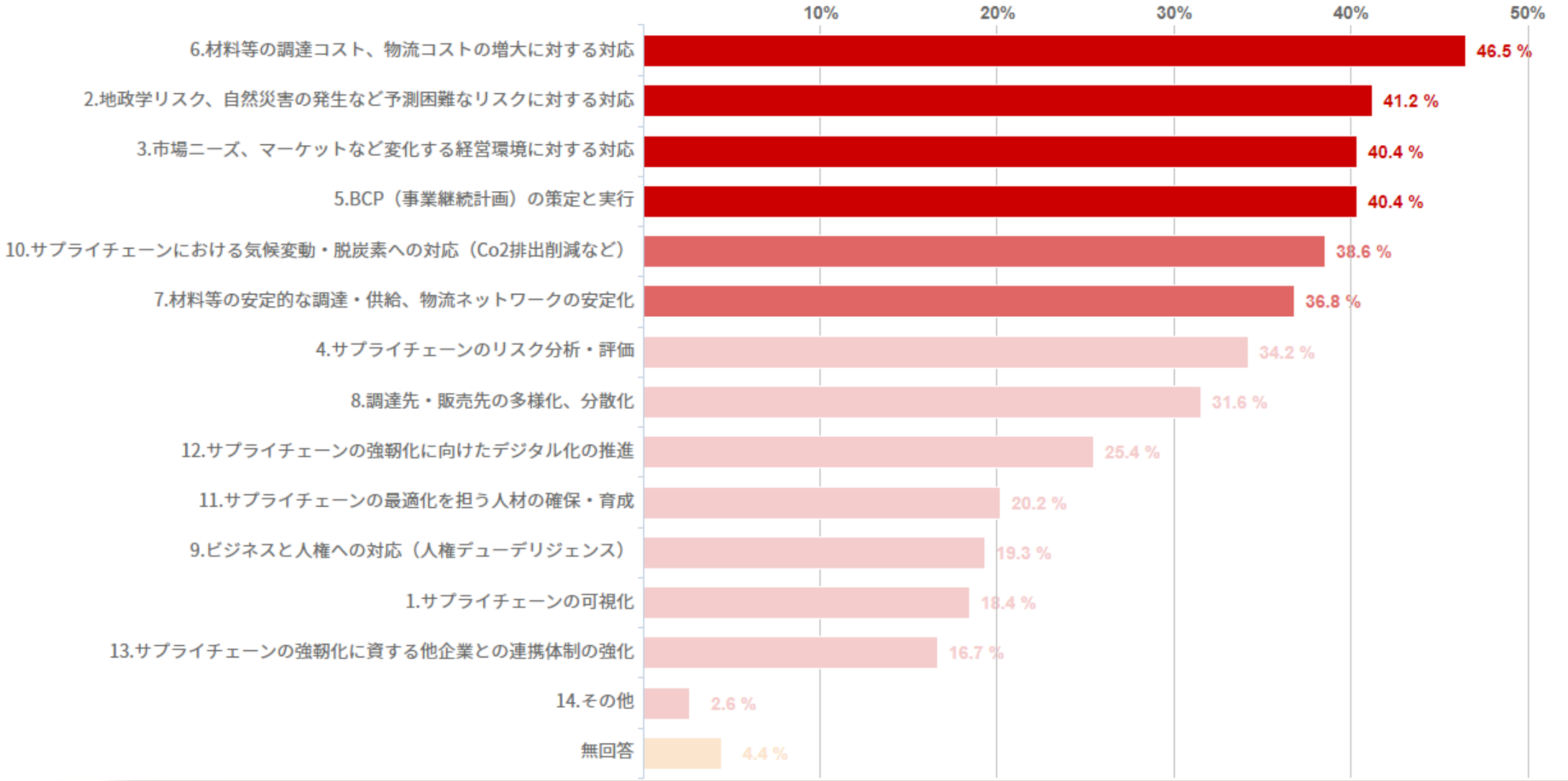
（N＝48）



（３）サプライチェーン

Q12. 貴社におけるサプライチェーン上の**課題**は何ですか。（N＝114）

全体

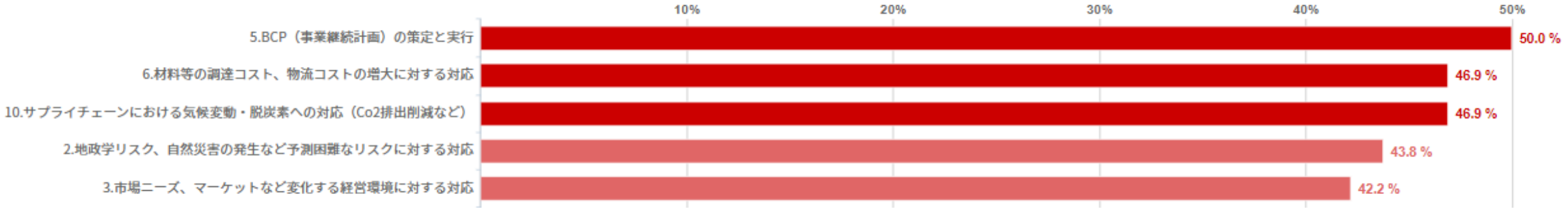


（３）サプライチェーン

Q12. 貴社におけるサプライチェーン上の**課題**は何ですか。（規模別；上位５）

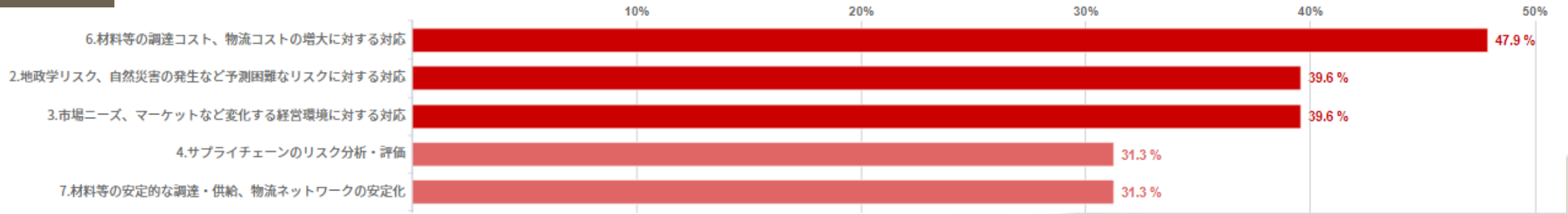
大企業

（N＝64）



中小企業

（N＝48）



（３）サプライチェーン

Q13. 貴社はサプライチェーンの強靭化に向けて以下の**取り組み**を行っていますか。

1.サプライチェーンの可視化

全体	22.8 %	33.3 %	36.8 %	7.0 %	（N＝114）
大企業	31.3 %	31.3 %	29.7 %	7.8 %	（N＝64）
中小企業	12.5 %	37.5 %	47.9 %	2.1 %	（N＝48）

2.地政学リスク、自然災害の発生など予測困難なリスクに対する対応

全体	25.4 %	36.0 %	32.5 %	6.1 %
大企業	35.9 %	32.8 %	25.0 %	6.3 %
中小企業	12.5 %	41.7 %	43.8 %	2.1 %

3.市場ニーズ、マーケットなど変化する経営環境に対する対応

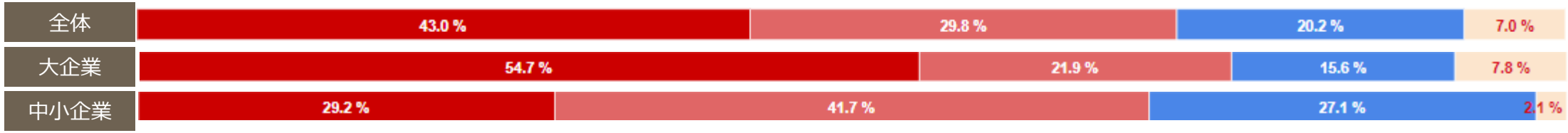
全体	24.6 %	43.0 %	24.6 %	7.9 %
大企業	31.3 %	37.5 %	21.9 %	9.4 %
中小企業	16.7 %	52.1 %	29.2 %	2.1 %

4.サプライチェーンのリスク分析・評価

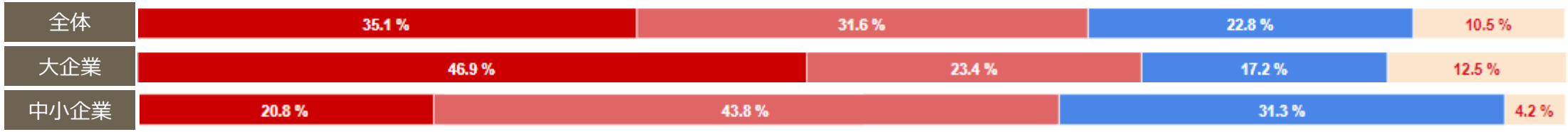
全体	19.3 %	37.7 %	33.3 %	9.6 %
大企業	28.1 %	39.1 %	21.9 %	10.9 %
中小企業	8.3 %	37.5 %	50.0 %	4.2 %

（３）サプライチェーン

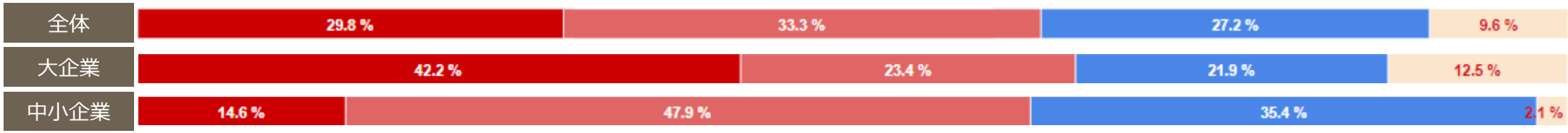
5.BCP（事業継続計画）の策定と実行



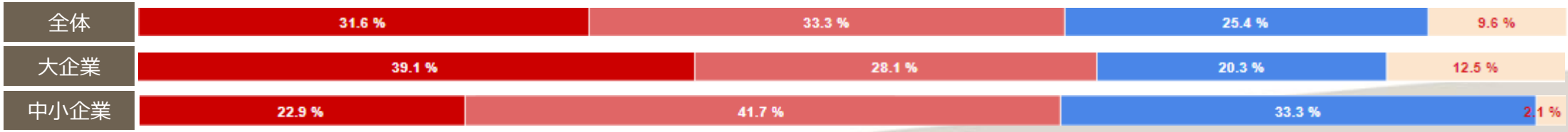
6.材料等の調達コスト、物流コストの増大に対する対応



7.材料等の安定的な調達・供給、物流ネットワークの安定化

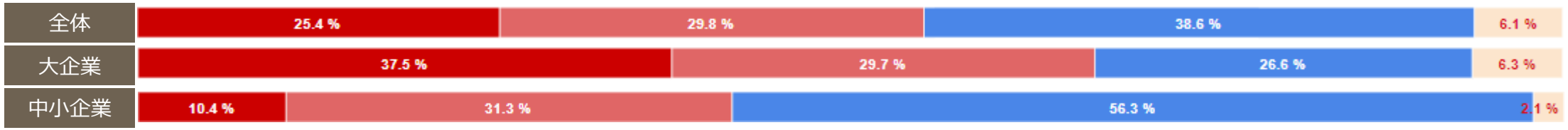


8.調達先・販売先の多様化、分散化

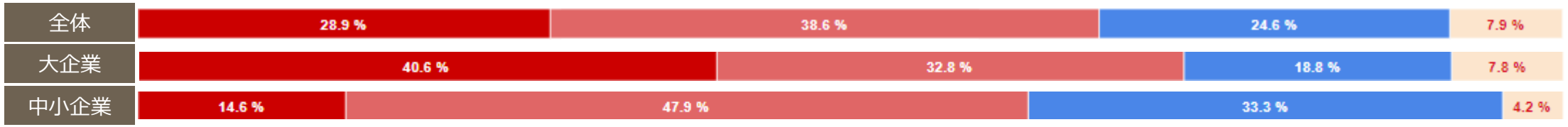


（３）サプライチェーン

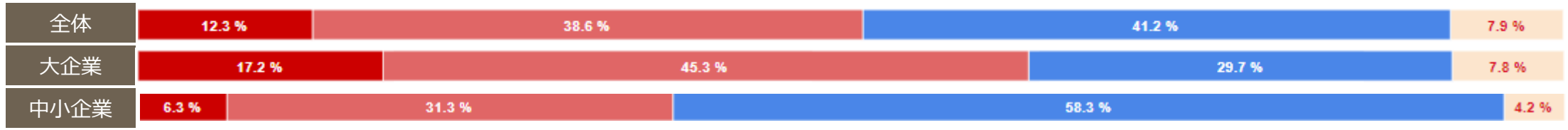
9.ビジネスと人権への対応（人権デューデリジェンス）



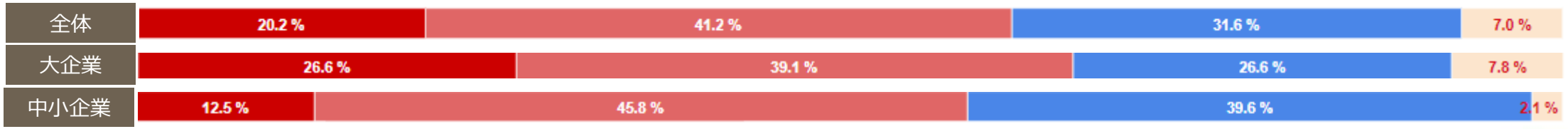
10.サプライチェーンにおける気候変動・脱炭素への対応（Co2排出削減など）



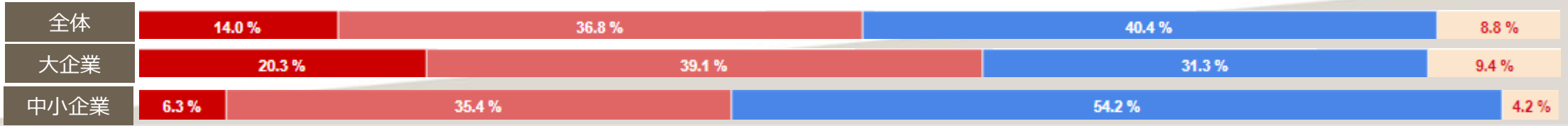
11.サプライチェーンの最適化を担う人材の確保・育成



12.サプライチェーンの強靭化に向けたデジタル化の推進



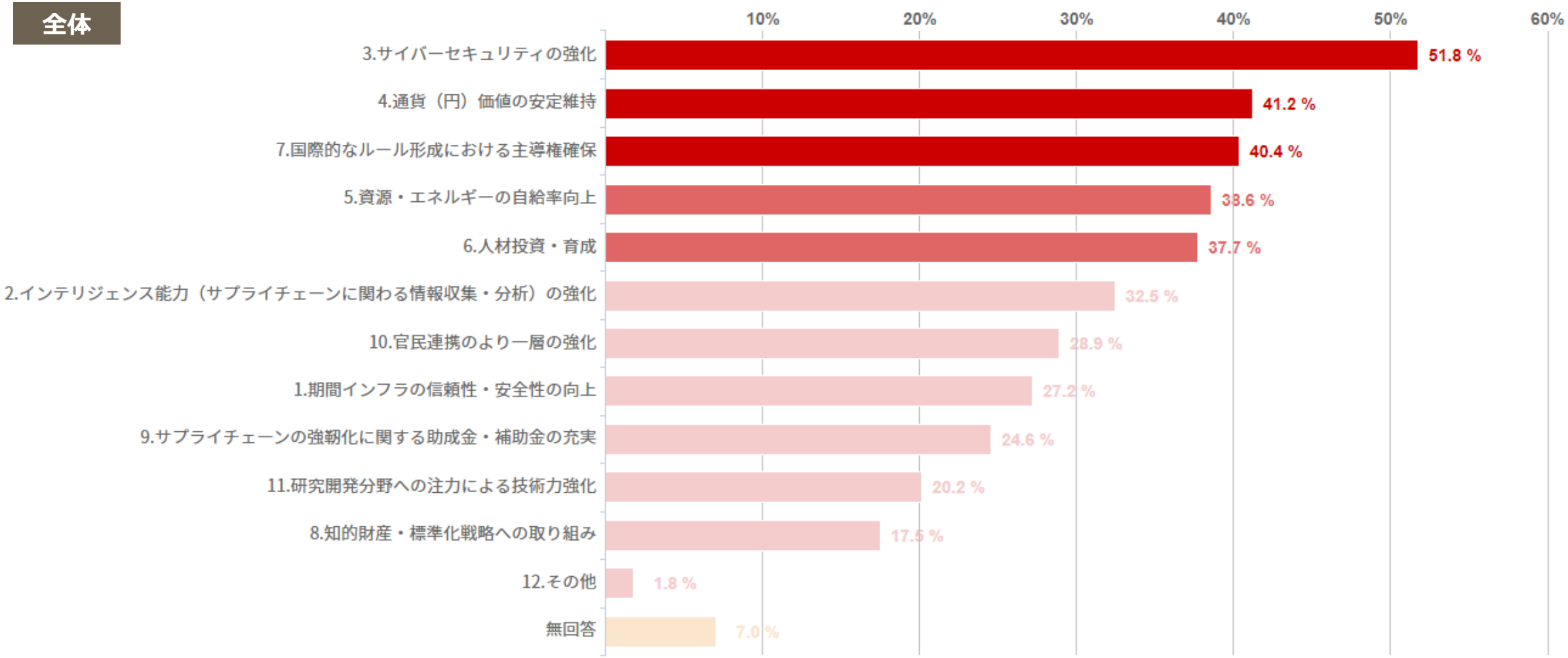
13.サプライチェーンの強靭化に資する他企業との連携体制の強化



（３）サプライチェーン

Q14. 貴社の属するサプライチェーンのレジリエンス（外部のショックや変動に対して強く、迅速且つ効果的に回復できる能力）の維持・向上を図る上で、**政府への要望**としてどういったことがあげられますか。（N＝114）

全体

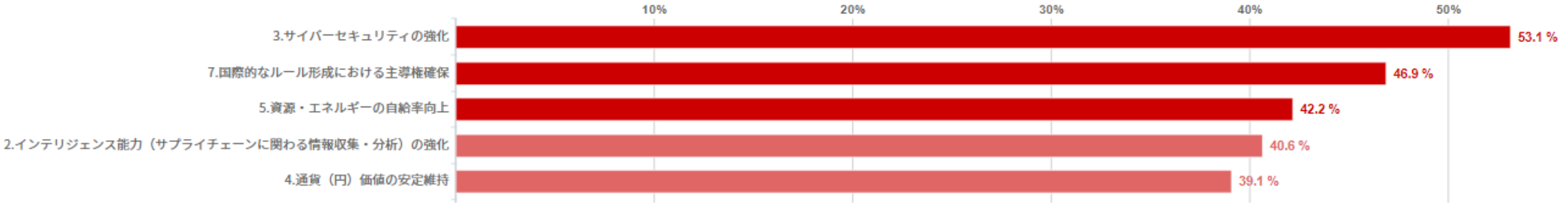


（３）サプライチェーン

Q14. 貴社の属するサプライチェーンのレジリエンス（外部のショックや変動に対して強く、迅速且つ効果的に回復できる能力）の維持・向上を図る上で、**政府への要望**としてどういったことがあげられますか。（規模別；上位５）

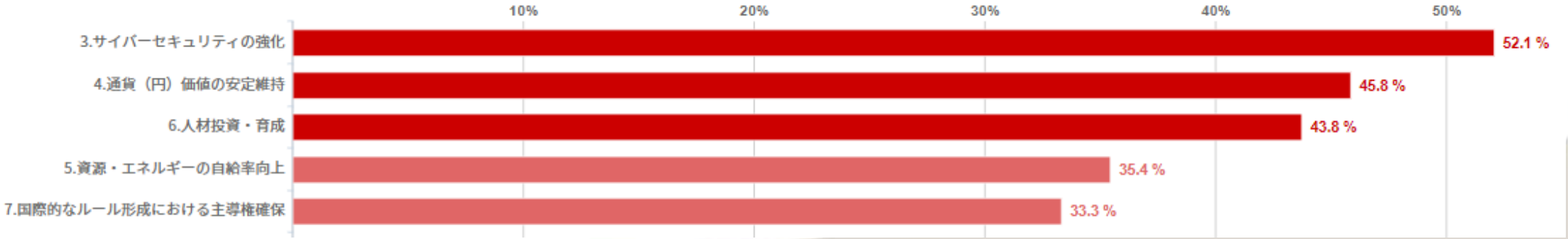
大企業

（N＝64）



中小企業

（N＝48）

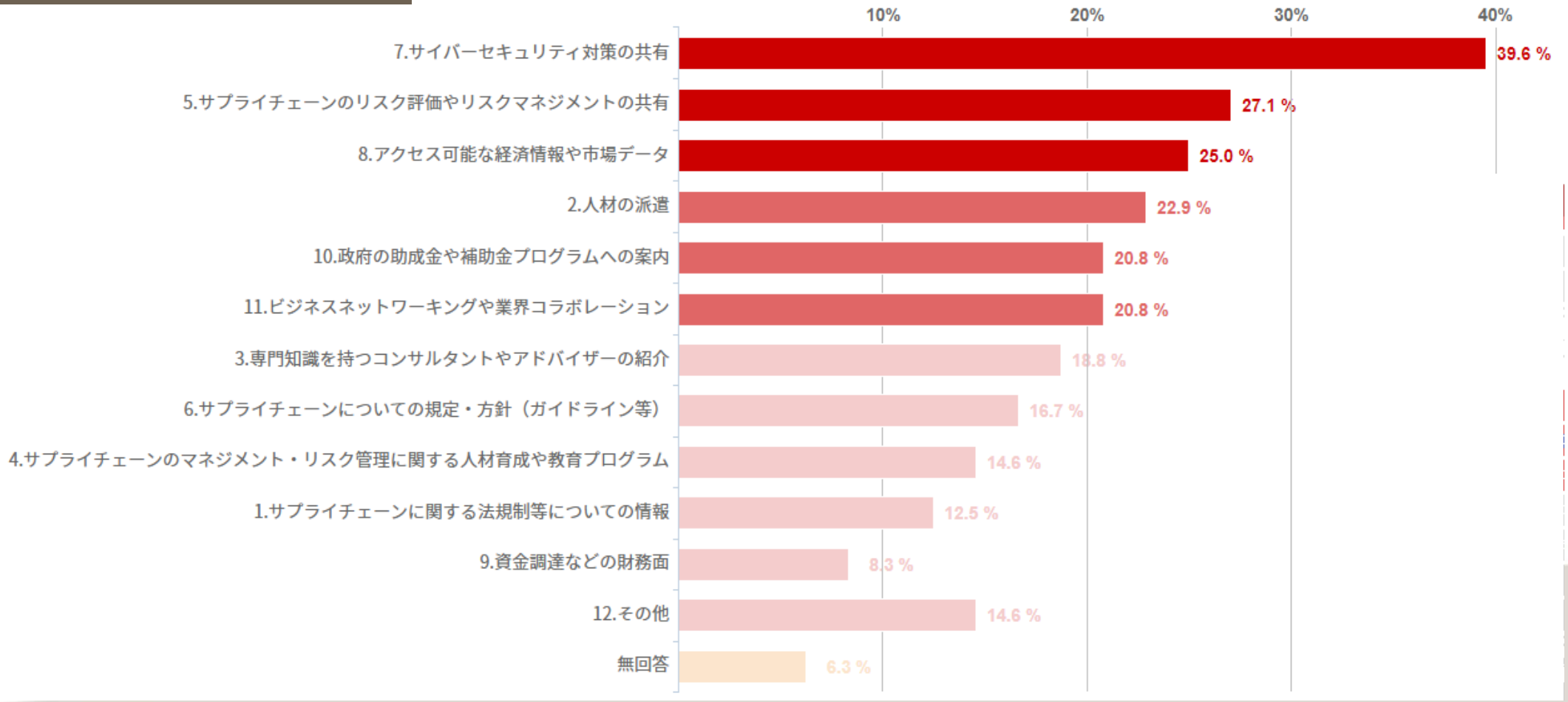


（３）サプライチェーン

Q15. **中小企業、大企業**それぞれの立場で回答してください。
（中小企業の回答者）貴社の属するサプライチェーンのレジリエンスの維持・向上のために、大企業に対してどんなことを求めますか。
（大企業の回答者）貴社の属するサプライチェーンのレジリエンスの維持・向上のために、中小企業に対してどんなことを求めますか。

中小企業から大企業に求めること

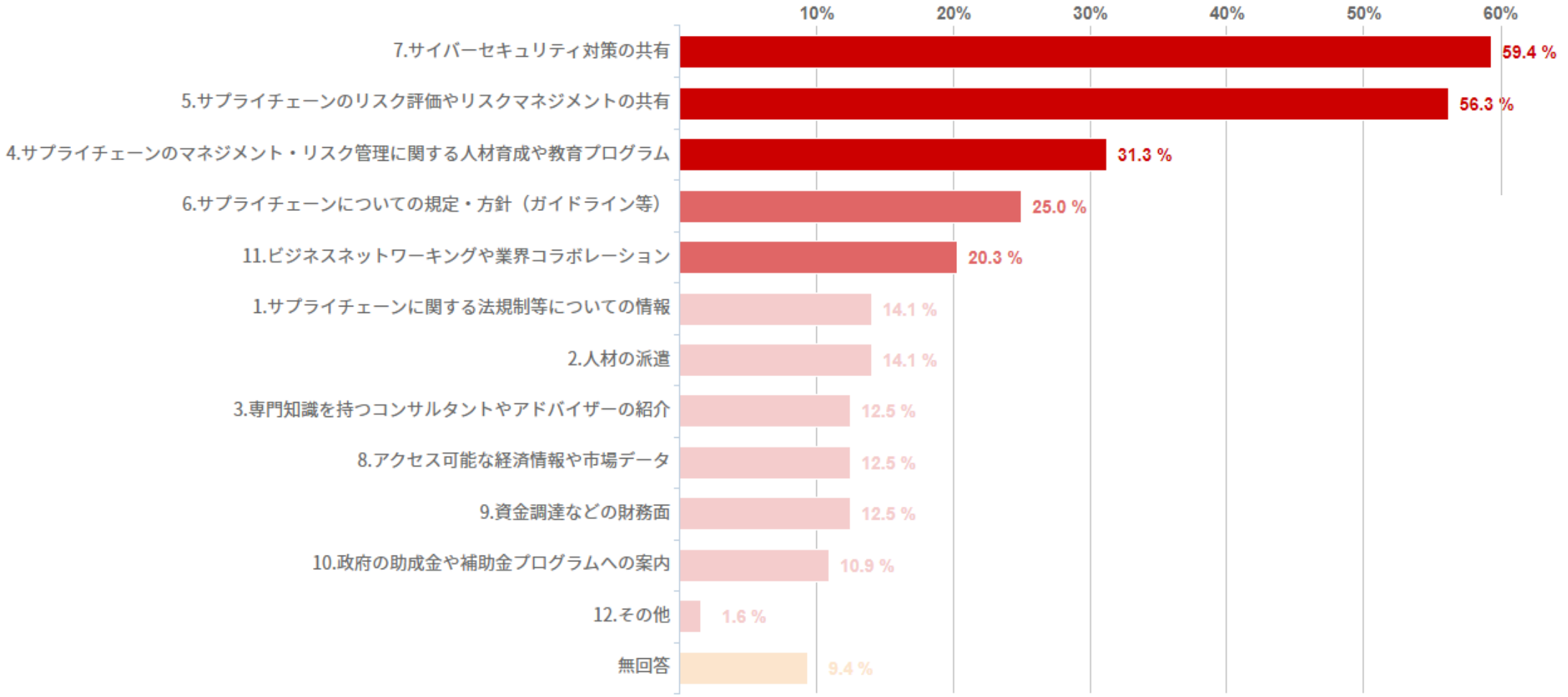
（N＝48）



（３）サプライチェーン

大企業から中小企業に求めること

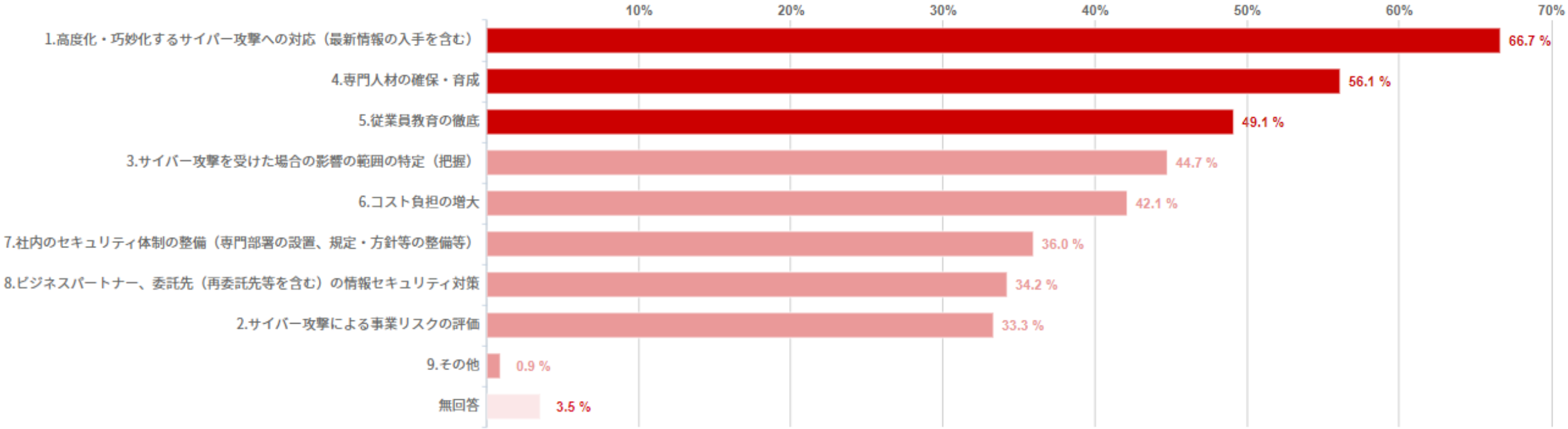
（N＝64）



（４）サイバーセキュリティ

Q16. 貴社におけるサイバーセキュリティ対策を行う上での**課題**は何ですか。（N＝114）

全体

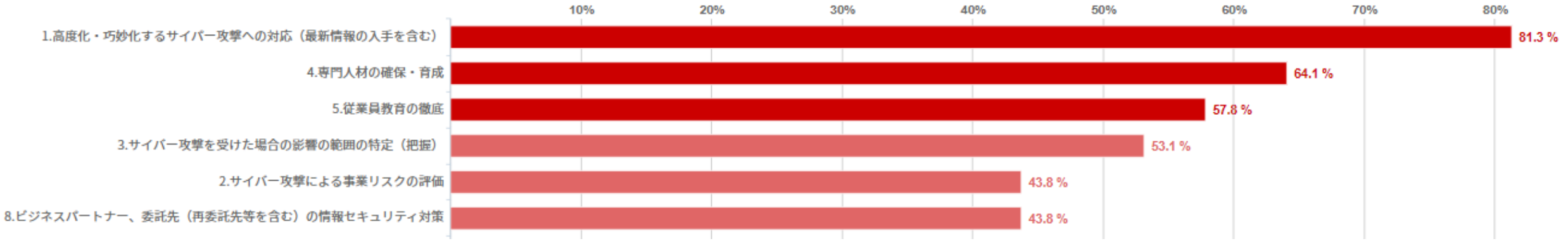


（４）サイバーセキュリティ

Q16. 貴社におけるサイバーセキュリティ対策を行う上での**課題**は何ですか。（規模別；上位５）

大企業

（N＝64）



中小企業

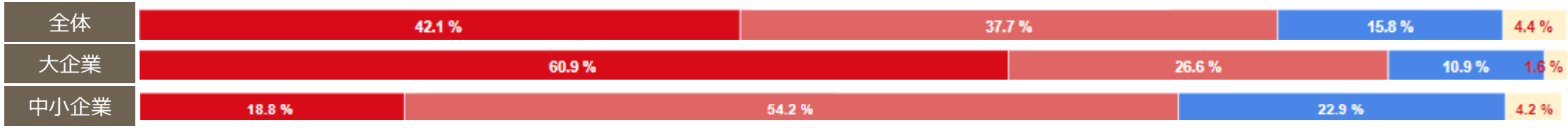
（N＝48）

（４）サイバーセキュリティ

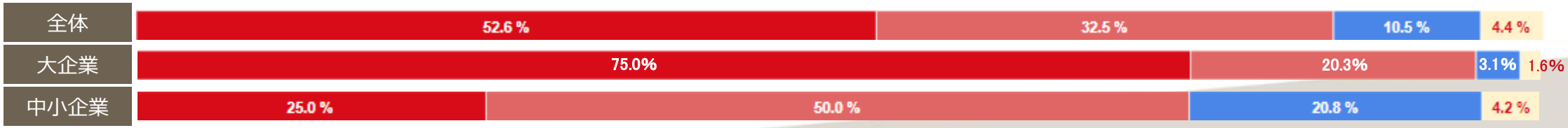
Q17. 以下は、経済産業省、独立行政法人情報処理推進機構が取りまとめた「サイバーセキュリティ経営ガイドライン Ver3.0」における「経営者が認識すべき3原則」及び「サイバーセキュリティ経営の重要10項目」に掲げられているチェック項目です。貴社はそれぞれについて**取り組み**を行っていますか。

（原則1）サイバーセキュリティリスクを経営者が責任を負うべき経営リスクとして認識し、組織全体としての対応方針（セキュリティポリシー）を策定している。

（原則2）サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先等、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要であることを認識している。

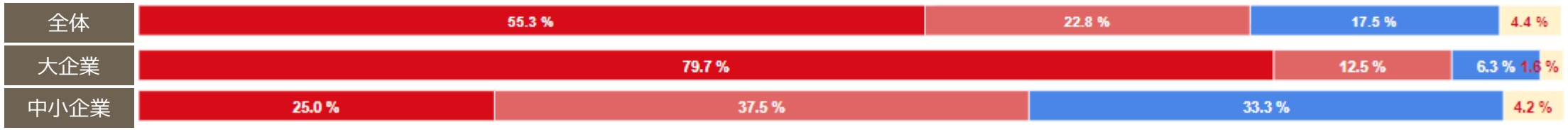


（原則3）平時及び緊急時のいずれにおいても、サイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要であることを認識している。

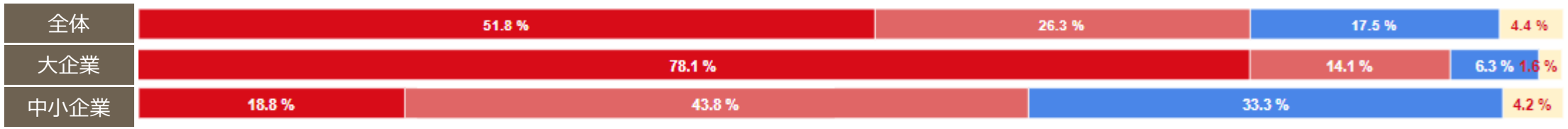


（４）サイバーセキュリティ

（重要事項1）サイバーセキュリティリスクを経営者が責任を負うべき経営リスクとして認識し、組織全体としての対応方針（セキュリティポリシー）を策定している。



（重要事項2）サイバーセキュリティリスクの管理に関する各関係者の役割と責任を明確にした上で、リスク管理体制を構築している。



（重要事項3）サイバーセキュリティに関する残存リスクを許容範囲以下に抑制するための方策を検討し、その実施に必要となる資源（予算、人材等）を確保した上で、具体的な対策に取り組んでいる。

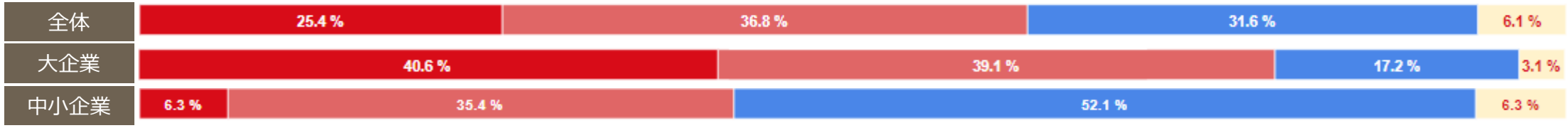
（重要事項4）事業に用いるデジタル環境、サービス・情報を特定し、それらに対するサイバー攻撃（過失や内部不正を含む）の脅威や影響度から、自組織や自ら提供する製品・サービスにおけるサイバーセキュリティリスクを識別している。

（重要事項5）サイバーセキュリティリスクに対応するための保護対策として、防御・検知・分析の各機能を実現する仕組みを構築している。

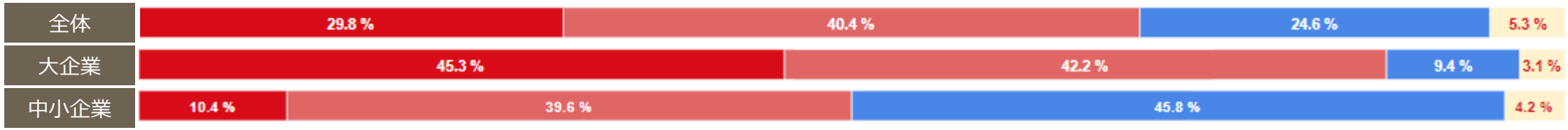
（４）サイバーセキュリティ

（重要事項6）リスクの変化に対応し、組織や事業におけるリスク対応を継続的に改善するため、サイバーセキュリティリスクの特徴を踏まえたPDCA サイクルを運用している。

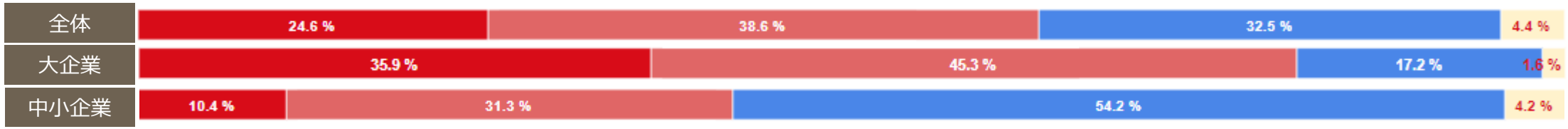
（重要事項7）影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を適時に実施するため、制御系を含むサプライチェーン全体のインシデントに対応可能な体制を整備している。



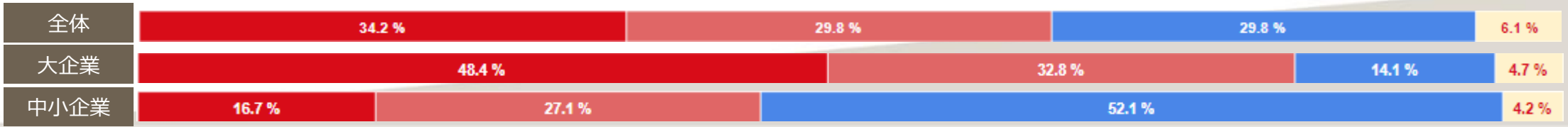
（重要事項8）インシデントにより業務停止等に至った場合、企業経営への影響を考慮して、いつまでに復旧すべきかを特定し、復旧に向けた手順書策定や、復旧対応体制の整備をしている。



（重要事項9）サプライチェーン全体にわたって適切なサイバーセキュリティ対策が講じられるよう、国内外の拠点、ビジネスパートナーやシステム管理の運用委託先等を含めた対策状況を把握している。



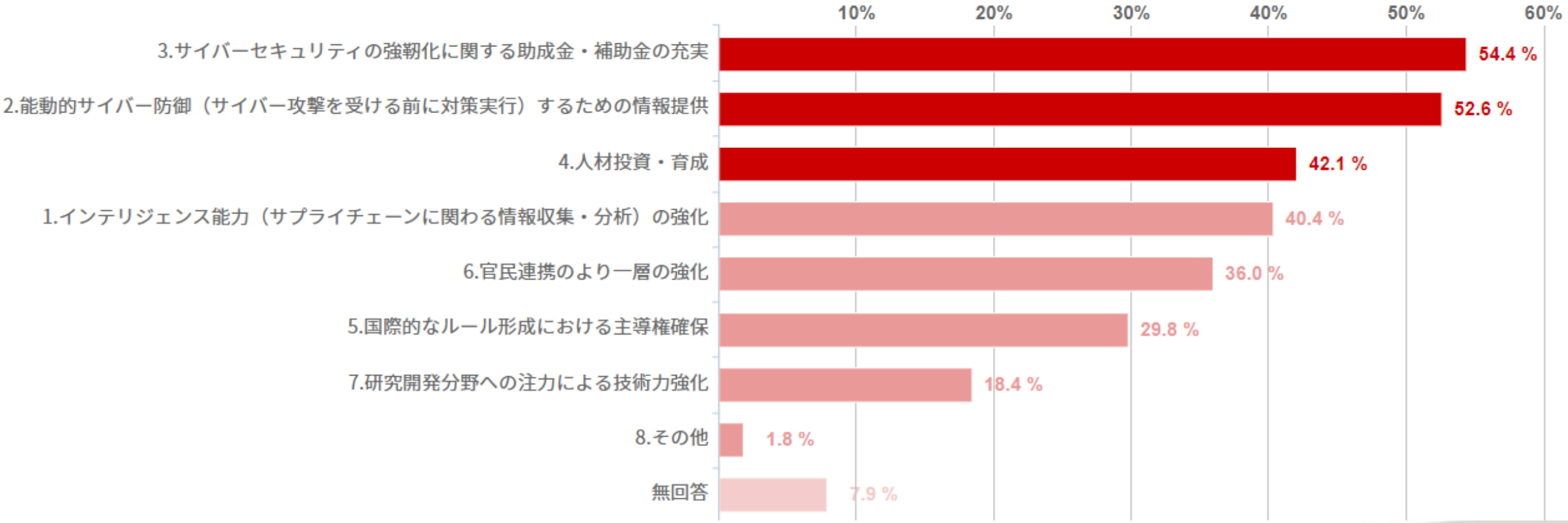
（重要事項10）有益な情報を得るには自ら適切な情報提供を行う必要があるとの自覚のもと、サイバー攻撃や対策に関する情報共有を行う関係の構築及び被害の報告・公表への備えをしている。



（４）サイバーセキュリティ

Q18. サイバーセキュリティ対策の充実を図る上で、**政府への要望**としてどういったことがあげられますか。（N＝114）

全体

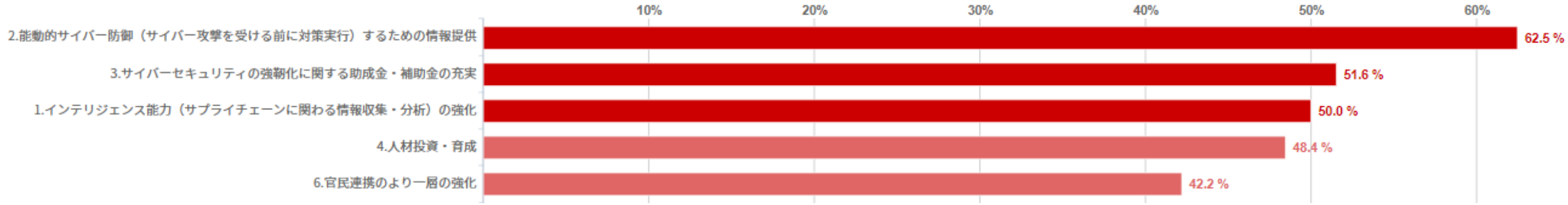


（４）サイバーセキュリティ

Q18. サイバーセキュリティ対策の充実を図る上で、**政府への要望**としてどういったことがあげられますか。（規模別；上位5）

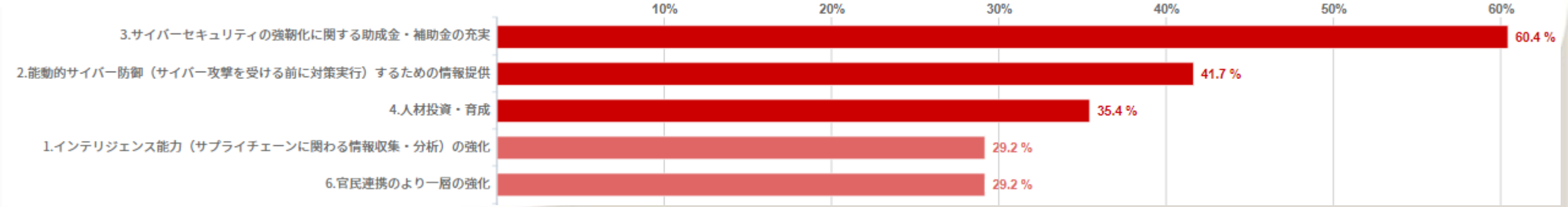
大企業

（N＝64）



中小企業

（N＝48）

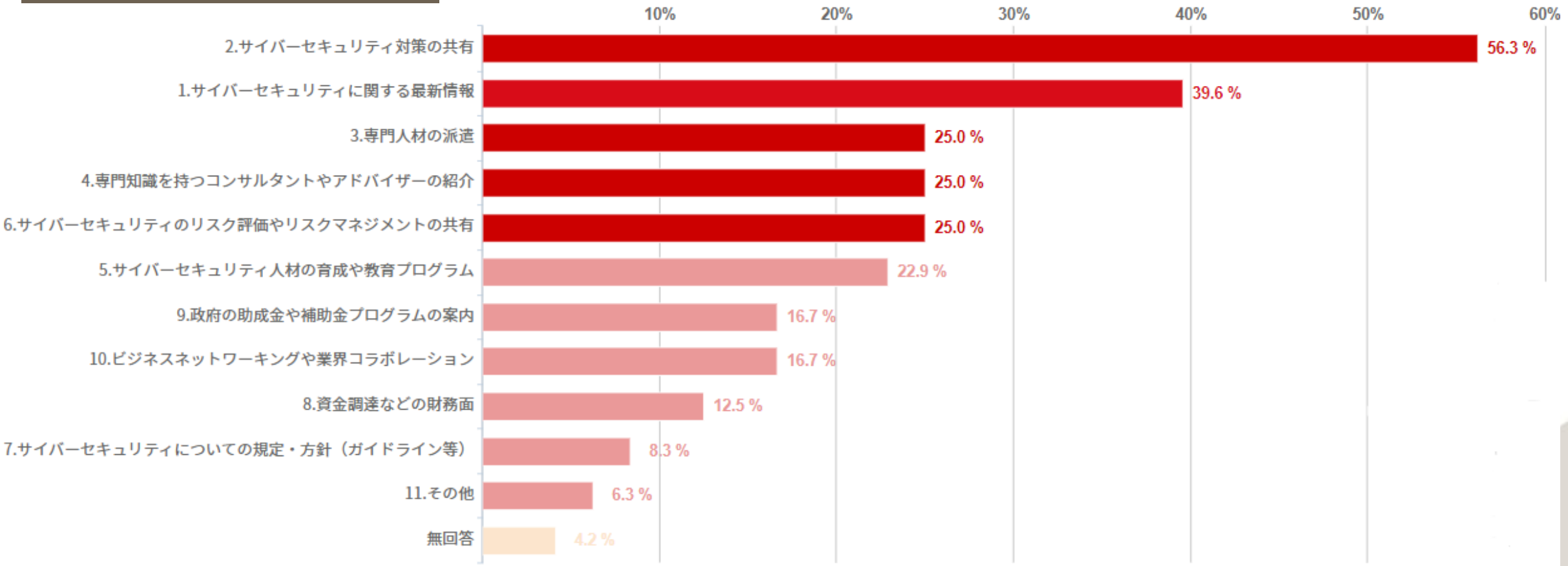


（４）サイバーセキュリティ

Q19. サプライチェーン全体で情報保全体制の確立が求められる中、ますます中小企業と大企業の連携が不可欠となっています。
中小企業、大企業それぞれの立場で回答してください。
（中小企業の回答者）サイバーセキュリティ対策の強化を図る上で、大企業に対してどんなことを求めますか。
（大企業の回答者）サイバーセキュリティ対策の強化を図る上で、取引を行っている中小企業に対してどんなことを求めますか。

中小企業から大企業に求めること

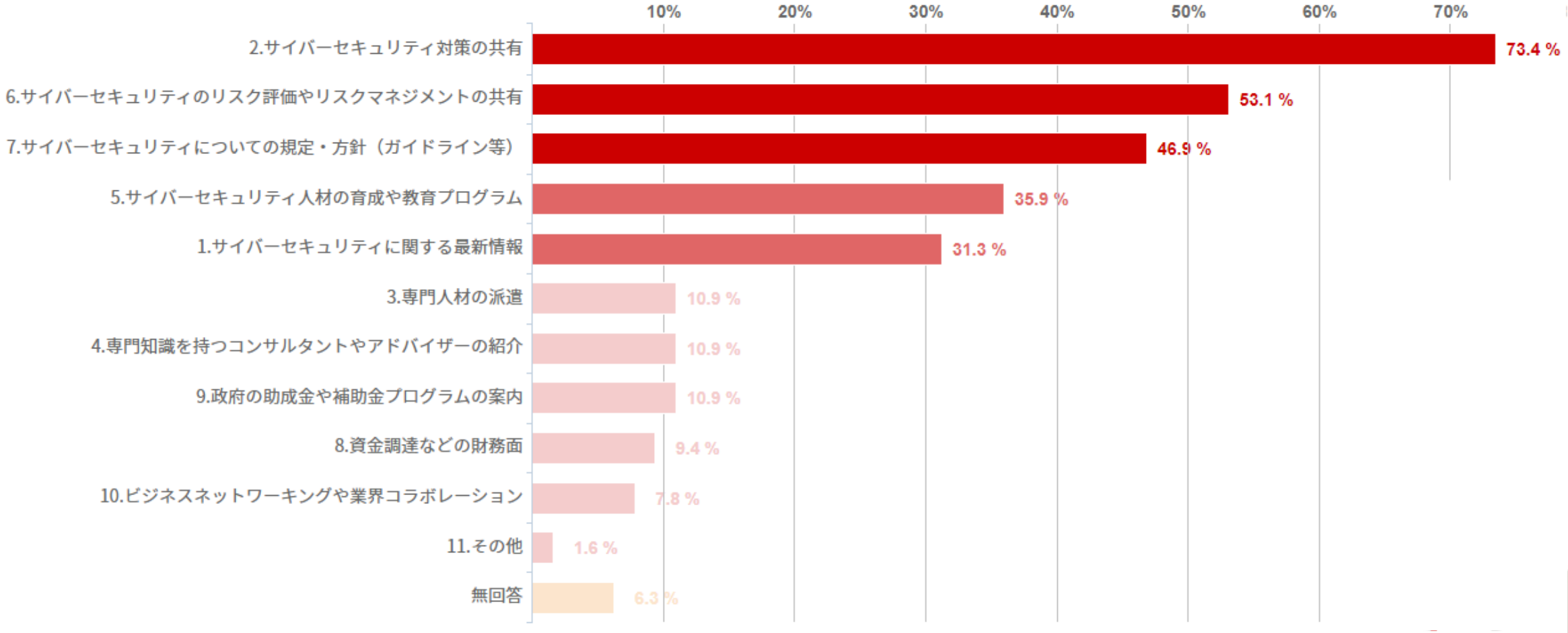
（N＝48）



（４）サイバーセキュリティ

大企業から中小企業に求めること

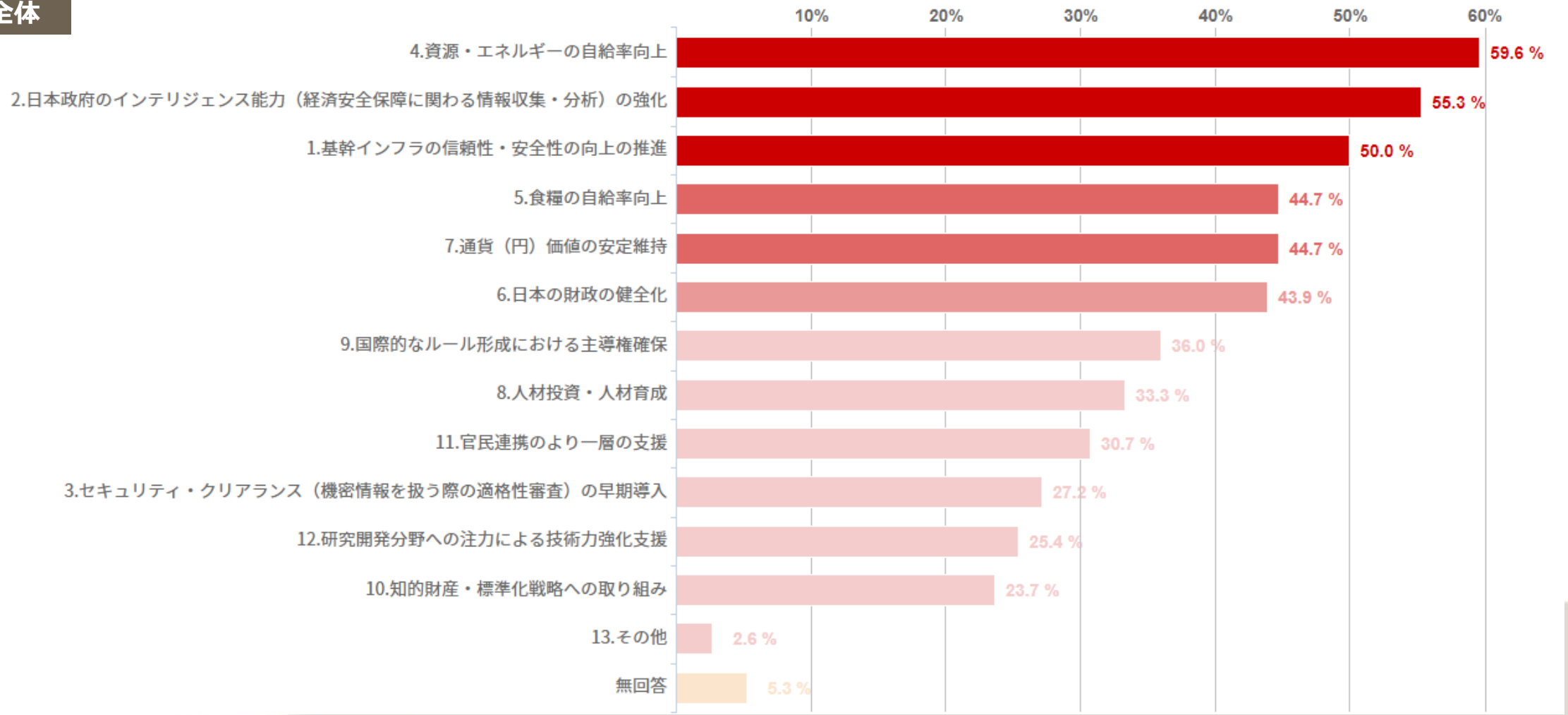
（N＝64）



（５）その他（政府への要望）

Q20. これまでの設問でお尋ねしたサプライチェーン・サイバーセキュリティ以外で、経済安全保障全般を通じて、**政府への要望**としてどういったことがあげられますか。（N＝114）

全体

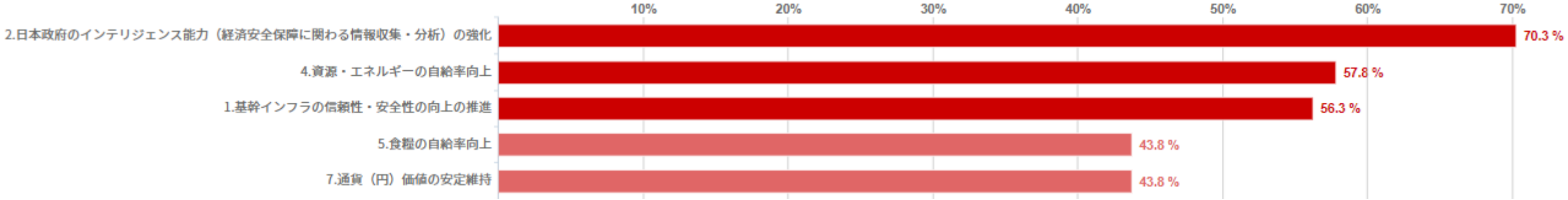


（５）その他（政府への要望）

Q20. これまでの設問でお尋ねしたサプライチェーン・サイバーセキュリティ以外で、経済安全保障全般を通じて、**政府への要望**としてどういったことがあげられますか。（規模別；上位5）

大企業

（N＝64）



中小企業

（N＝48）