

電通PRコンサルティング「危機管理広報力、およびサイバーインシデント対応実態調査2026」

サイバー対応体制は8割超が整備。**しかし、エスカレーションルールを明確に定めている企業は4割。**～危機管理広報力が高い企業ほど経営層のサイバーリスク意識も高い傾向～

株式会社電通PRコンサルティング（代表取締役社長執行役員：山口恭正、所在地：東京都港区）は、従業員数1,000人以上の企業に勤務し、コンプライアンス・リスク管理の選定または最終決裁に関わる500人を対象に、「危機管理広報力、およびサイバーインシデント対応実態調査2026」を実施しました。

調査の結果、これら大企業において危機管理における意思決定の一元化ルール整備は大半の企業で進んでいました。一方、**規定を定期的に見直し、社内の理解にまで至っているのは半数程度**にとどまっており、実効性を高める段階に移っています。

また、サイバー攻撃については85.2%が経営上のリスクとして認識し、83.0%がCSIRT※やシステム担当者などの対応体制を設置している一方、経営層・広報・法務・人事などコーポレート部門まで含めた連携・エスカレーションルールを明確に定めている企業は48.2%（n=415）、全回答者ベースでは40.0%にとどまっています。

さらに、今後**優先して対応を進めるべきリスクとして「生成AI利用に伴うリスク」が最多**となり、企業の危機管理が従来型の事故・不祥事対応だけでなく、**生成AI、風評被害、サイバー攻撃などの新たな経営リスクへの対応の必要性**も浮き彫りになりました。

※ CSIRT (Computer Security Incident Response Team) はサイバーセキュリティに関するインシデント発生時の対応を行う専門チーム

調査結果ポイント**1 意思決定の一元化ルールは大半が整備、社内理解までは約5割**

- 重大危機発生時の意思決定ルール・仕組みの規定について「整備されており、見直しの機会を定期的に設け社内も理解している」としたのは全体の49.8%で約半数を占めています。
- 「整備されているが、定期的な見直しはしていない」（34.0%）、「整備されているが、社内の理解も含めてまだ不十分だと思う」（13.0%）を合わせると、96.8%となり、大半が全社的な意思決定のルールを規定しています。

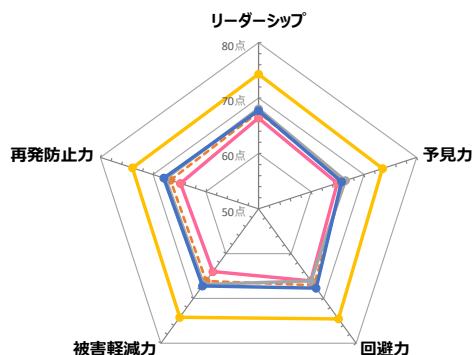
**2 サイバーリスクは85.2%が認識、83.0%が対応体制を設置。
しかしCSIRTとの「全社連携」は約4割と、社内連携がカギに**

- サイバー攻撃について、「優先度の高いリスクと捉えている」「ある程度リスクがあると捉えている」と回答した企業は合わせて85.2%に達しました。
- 一方、サイバー攻撃発生時に向けた「CSIRTの設置」は42.8%、「システム担当者を常設」を合わせると83.0%が設置。
- しかし、CSIRTから経営層、広報、法務、人事などへ情報を伝達する「連携体制・エスカレーションルール」がリスク管理規定等に明確に定められている企業は、48.2%（サンプル500での換算だと40.0%）にとどまりました。
- IT・システム部門だけでなく、経営層・広報・法務などを巻き込んだ「全社危機管理としてのサイバー対応」における連携は、今後の重要課題といえます。

3

危機管理広報力を業種別にみると情報通信・ITが相対的に高い

- 企業の危機管理への取り組みを業種別で見る（サンプル40社以上を抽出）と、1位が「情報通信・IT」、2位「金融・保険」3位「建設・不動産」と続いています。



	リーダシップ	予見力	回避力	被害軽減力	再発防止力
全体 (n=500)	67.4	66.1	67.1	66.1	66.7
製造業 (n=157)	66.4	64.9	66.1	64.0	64.8
建設・不動産 (n=44)	68.1	66.5	66.1	66.9	67.6
情報通信・IT (n=75)	74.3	73.5	74.6	74.2	73.9
金融・保険 (n=64)	67.7	65.8	67.7	67.2	68.0

- 全体 (n=500) - 製造業 (n=157) - 建設・不動産 (n=44)
 - 情報通信・IT (n=75) - 金融・保険 (n=64)

4

サイバーインシデントにおいては、経営層の意識が重要。 リーダシップ力は上位層と下位層に開きあり

- 「自社の経営幹部がサイバー攻撃によるインシデント発生をどの程度のリスクとして位置付けているか」を聞いたところ、危機管理広報力のリーダシップ上位層では96.1%がリスクとして認識したのに対し、下位層では74.0%となり、22.1ポイントの差が見られました。
- 危機管理広報力が高い企業群ほど、経営層におけるサイバーリスク認識も高い傾向がみられました。この結果は、サイバー対応をIT部門だけの課題とせず、経営課題として認識することの重要性を示唆しています。

5

危機管理体制における課題は「リスク洗い出し」「部門連携」「規定・マニュアル整備」

- 危機管理体制の課題としては、1位「リスクの洗い出し」、2位「部門連携」、3位「規定・マニュアル整備」、4位「訓練・教育」、5位「経営層の関与」などが上位を占めました。

6

自社にとって優先的に進めなくてはならないリスク事象は 1位「生成AIリスク」、2位「風評被害」、3位「サイバー攻撃」

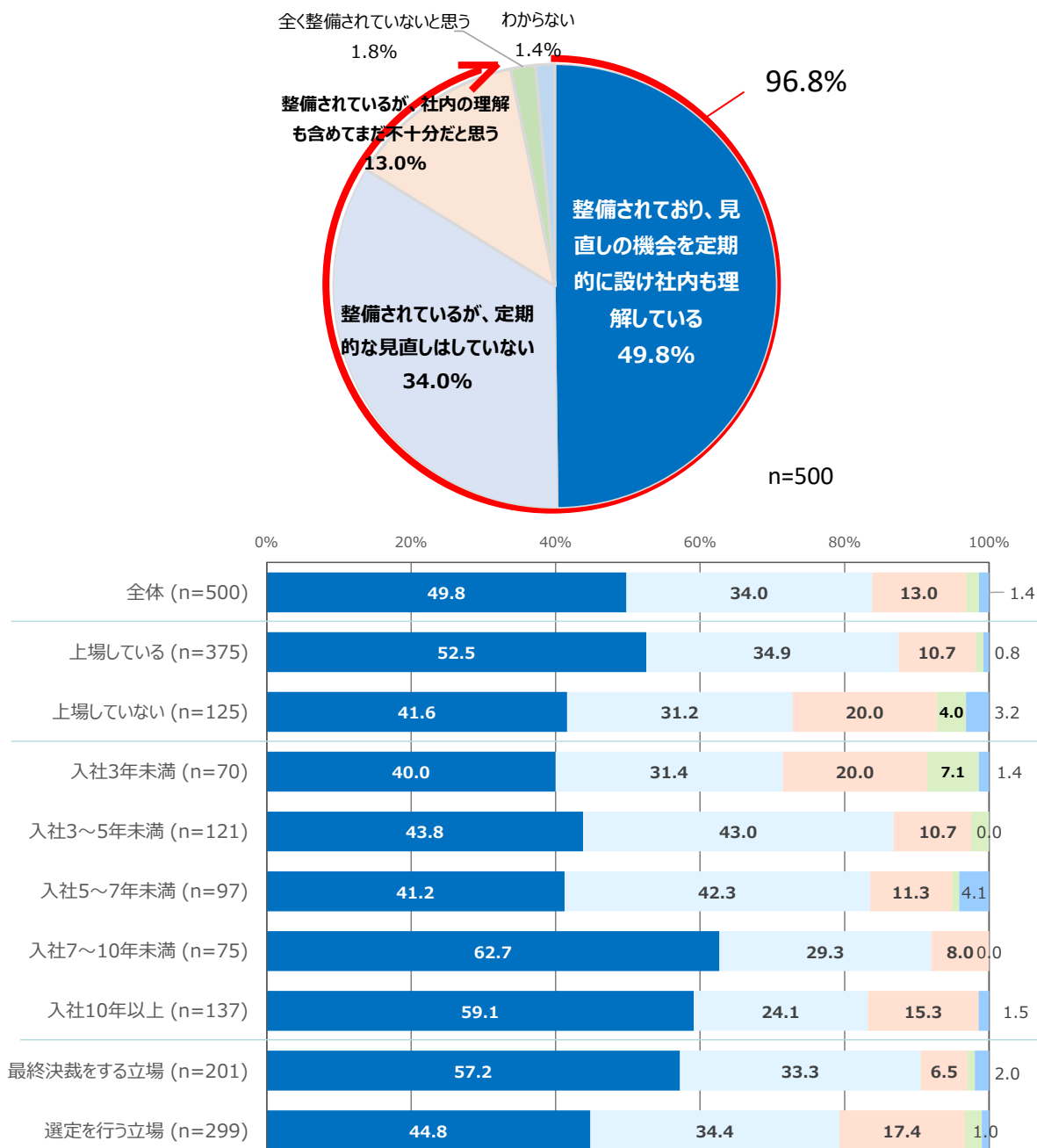
- 自社にとって優先的に進めなくてはならないリスク事象は、1位「生成AI利用に伴うリスク」、2位「風評被害」、3位「サイバー攻撃」とTOP3を占めました。
- 対応策の実施状況をみると、サイバー攻撃に対しては51.0%にとどまりました。

1

意思決定の一元化ルールは大半が整備、社内理解までは約5割

- 重大危機発生時の意思決定ルール・仕組みの規定について「整備されており、見直しの機会を定期的に設け社内も理解している」としたのは全体の49.8%で約半数を占めています。
- 「整備されているが、定期的な見直しはしていない」（34.0%）、「整備されているが、社内の理解も含めてまだ不十分だと思う」（13.0%）を合わせると、96.8%となり、大半が全社的な意思決定のルールを規定しています。

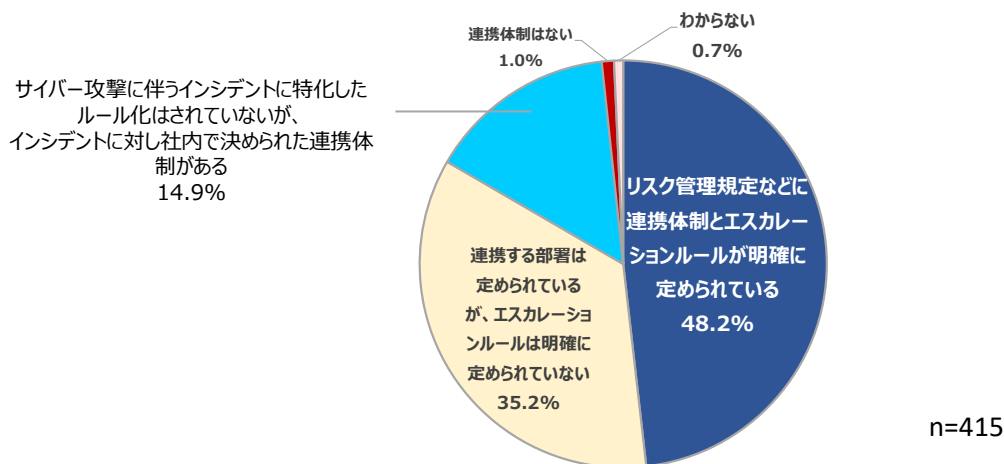
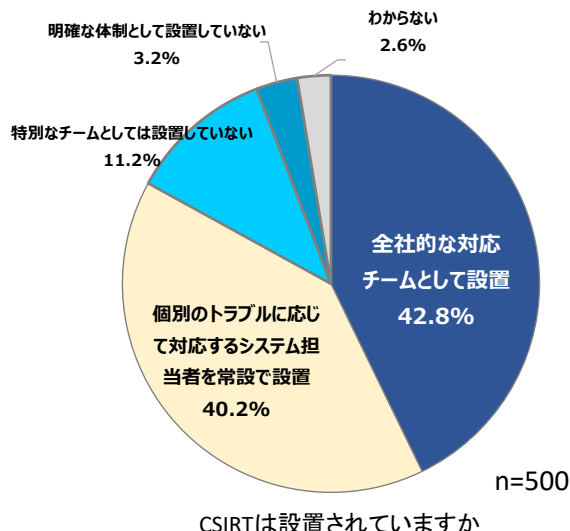
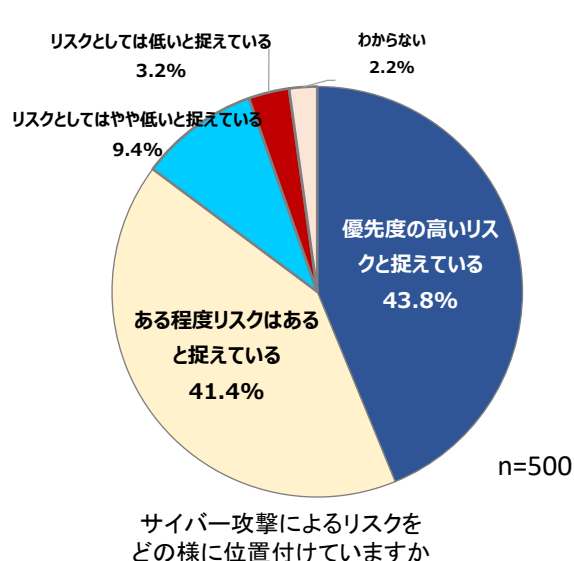
重大な危機が発生した場合、緊急対策本部など経営層が迅速に意思決定するための一元化ルール、全社的な意思決定する仕組みがリスク管理規定で整備されていますか



2

サイバーリスクは85.2%が認識、83.0%が対応体制を設置。 しかしCSIRTとの「全社連携」は約4割と、社内連携がカギに

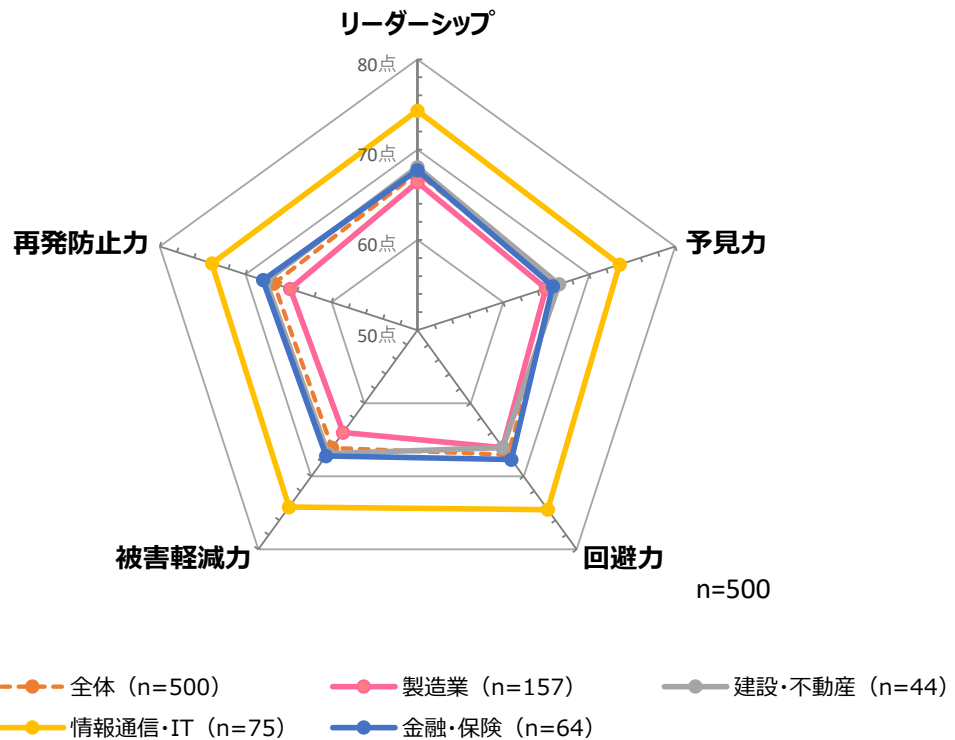
- サイバー攻撃について、「優先度の高いリスクと捉えている」「ある程度リスクがあると捉えている」と回答した企業は合わせて85.2%に達しました。
- 一方、サイバー攻撃発生時に向けた「CSIRTの設置」は42.8%、「システム担当者を常設」を合わせると83.0%が設置。
- しかし、CSIRTから経営層、広報、法務、人事などへ情報を伝達する「連携体制・エスカレーションルール」がリスク管理規定等に明確に定められている企業は、48.2%（サンプル500での換算だと40.0%）にとどまりました。
- IT・システム部門だけでなく、経営層・広報・法務などを巻き込んだ「全社危機管理としてのサイバー対応」における連携は、今後の重要課題といえます。



3

危機管理広報力を業種別にみると情報通信・ITが相対的に高い

- 企業の危機管理への取り組みを業種別で見る（サンプル40社以上を抽出）と、1位が「情報通信・IT」、2位「金融・保険」3位「建設・不動産」と続いています。



(100点満点スコア、単位: 点)

	リーダーシップ	予見力	回避力	被害軽減力	再発防止力
全体 (n=500)	67.4	66.1	67.1	66.1	66.7
製造業 (n=157)	66.4	64.9	66.1	64.0	64.8
建設・不動産 (n=44)	68.1	66.5	66.1	66.9	67.6
情報通信・IT (n=75)	74.3	73.5	74.6	74.2	73.9
金融・保険 (n=64)	67.7	65.8	67.7	67.2	68.0

■ 4業種中最も数値が高いもの
 ■ 4業種中2番目に数値が高いもの

4 サイバーインシデントにおいては、経営層の意識が重要。 リーダーシップ力は上位層と下位層に開きあり

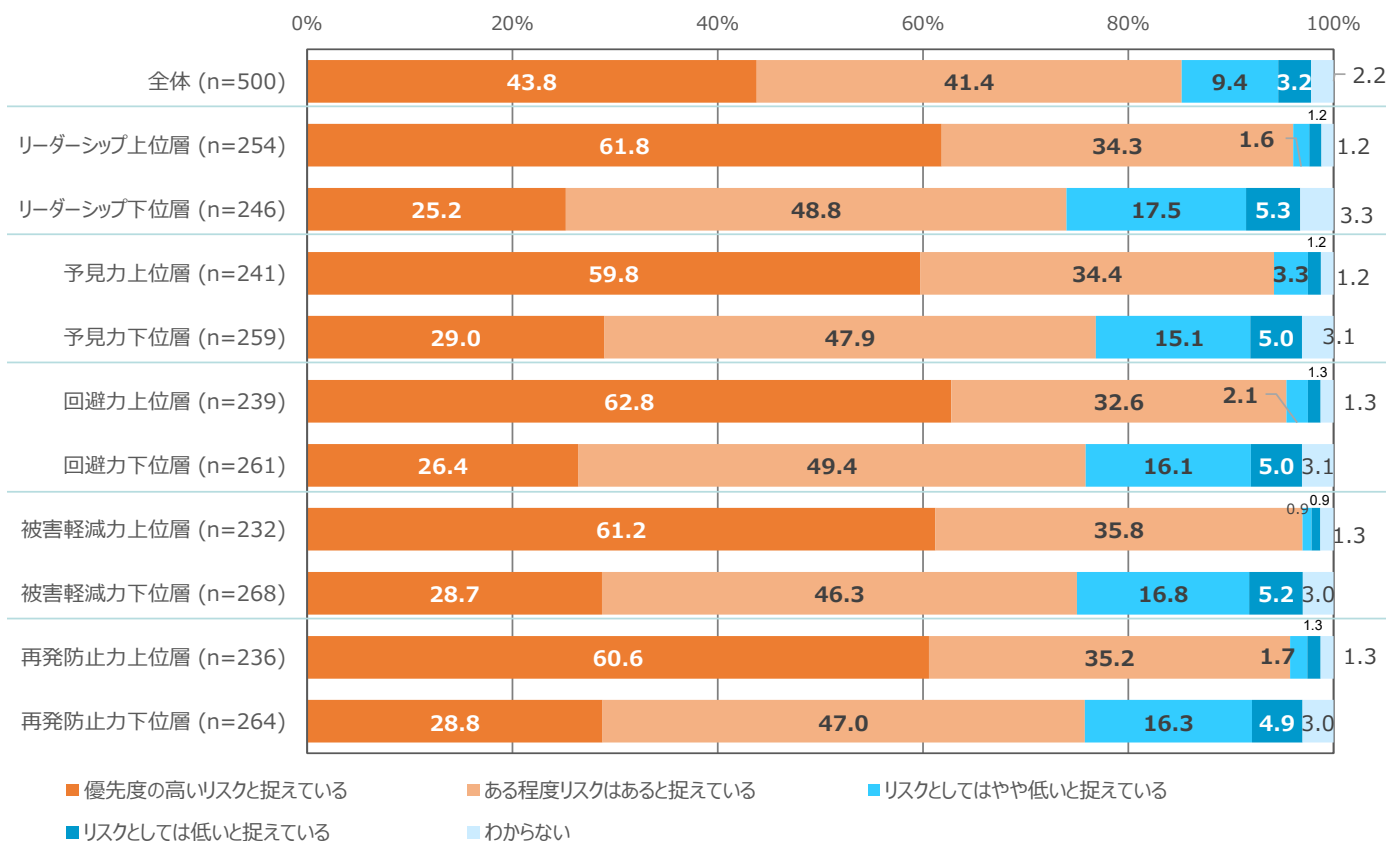
「自社の経営幹部がサイバー攻撃によるインシデント発生をどの程度リスクとして位置付けているか」を聞いたところ、危機管理広報力のリーダーシップ上位層では96.1%がリスクとして認識したのに対し、下位層では74.0%となり、22.1ポイントの差が見られました。

上位層：61.8 + 34.3 = 96.1%

下位層：25.2 + 48.8 = 74.0%

- 危機管理広報力が高い企業群ほど、経営層におけるサイバーリスク認識も高い傾向がみられました。この結果は、サイバー対応をIT部門だけの課題とせず、経営課題として認識することの重要性を示唆しています。

自社の経営幹部がサイバー攻撃によるインシデント発生をどの程度リスクとして位置付けているか。（SA）

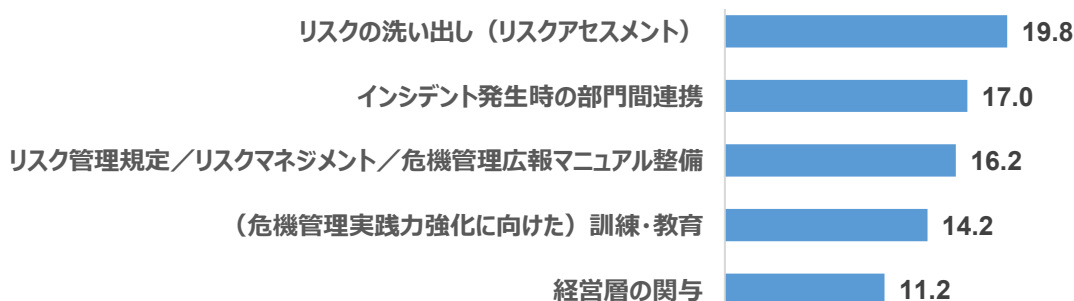


n=500

5 危機管理体制における課題は「リスク洗い出し」「部門連携」「規定・マニュアル整備」

- 危機管理体制の課題としては、1位「リスクの洗い出し」、2位「部門連携」、3位「規定・マニュアル整備」、4位「訓練・教育」、5位「経営層の関与」などが上位を占めました。

危機管理体制において最も課題が大きいと感じること TOP5



n=500
(単位: %)

6 自社にとって優先的に進めなくてはならないリスク事象は 1位「生成AIリスク」、2位「風評被害」、3位「サイバー攻撃」

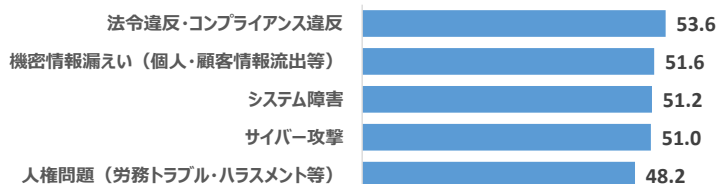
- 自社にとって優先的に進めなくてはならないリスク事象は、1位「生成AI利用に伴うリスク」、2位「風評被害」、3位「サイバー攻撃」とTOP3を占めました。
- 対応策の実施状況をみると、サイバー攻撃に対しては51.0%にとどまりました。

自社にとって
最も優先的に進めなくてはならないリスク事象
上位5項目

リスク事象	全体 (1~3位計)
生成AI利用に伴うリスク（著作権侵害等）	18.4
風評被害	17.0
サイバー攻撃	16.0
SNS炎上	14.8
海外情勢・地政学リスク（サプライチェーンリスク、現地の法人拘束など）	14.4

n=500
(単位: %)

自社にとって起こりうるリスクとして
対応策を実施している危機事象
上位5項目



n=500
(単位: %)

【危機管理広報力、およびサイバーインシデント対応実態調査2026】

■ 調査対象：計500サンプル

従業員数1000名以上の企業に勤めており、コンプライアンス・リスク管理の選定や最終決裁に関わっている500人

■ 調査方法：インターネット調査

■ 調査期間：2026年8月6日～8月7日

■ 設問内容：危機管理広報に関する取り組み・体制、サイバー攻撃によるインシデント発生に対する対策・認識

危機管理広報力調査とは

企業広報戦略研究所（電通PRコンサルティング内）が2015年に構築した「危機管理ペタゴンモデル」に基づき、危機管理広報力をリーダーシップ、予見力、回避力、被害軽減力、再発防止力の5つに分類し、各10項目を設定しています。2026年度に項目を改めて見直し、この5つを軸に強化すべき危機管理対策を把握できる設計としています。平時から自社の危機管理について現状を客観的に把握し、課題を抽出、具体的な施策を講じておくことで緊急時の初動を含めた対応力強化に活用することができます。



<お願い>

本調査内容を転載・引用する場合、転載者・引用者の責任で行うとともに、当社の調査結果である旨を明示してください。

【本件に関するお問い合わせ先】

株式会社 電通PRコンサルティング
〒105-7001 東京都港区東新橋1-8-1
E-mail: info@dentsuprc.co.jp
<http://www.dentsuprc.co.jp/>