NEWS RELEASE

アンケート調査結果

２０２６．５．１５
大阪シティ信用金庫

中小企業におけるサイバーリスクへの対応状況

～「サイバーリスクを深刻な脅威として捉えていない」が 71.4%
サイバーリスクへの「対策なし」（17.6%）が 6 社に 1 社
対応の障壁は「専任担当者が不在」（41.3%）が最多 ～

近年、デジタル化の進展に伴い、企業を標的としたサイバー攻撃は巧妙化・多様化の一途を辿っている。ひとたび、情報漏洩やシステム停止が発生すると、自社のみならず、サプライチェーン全体に多大な影響を及ぼすリスクがあるため、中小企業においても組織的な対策の強化が急務となっている。

そうした状況を踏まえ、サイバーリスク対策の実態や課題などについて、当金庫の取引先中小企業を対象にアンケート調査を実施した。

■ 調査時点：2026 年 4 月上旬
■ 調査対象：大阪シティ信用金庫取引先企業 （大阪府内）
■ 調査方法：聞き取り法
■ 調査依頼先数： 1,400 社
有効回答数 ： 1,249 社
有効回答率 ： 89.2%

業種＼従業者	5 人未満	5～19 人	20～49 人	50 人以上	計	構成比
製 造 業	107 社	227 社	59 社	18 社	411 社	32.9 %
卸 売 業	47	69	11	5	132	10.6 %
小 売 業	93	38	9	6	146	11.7 %
建 設 業	93	101	14	7	215	17.2 %
運輸・通信業	7	51	18	13	89	7.1 %
サービス業	153	73	19	11	256	20.5 %
計	500	559	130	60	1,249	100.0 %
構成比	40.0%	44.8%	10.4%	4.8%	100.0%	―

（注） 小売業には「飲食店」、サービス業には「不動産業」を含みます。

信頼で地域とつながる
大阪シティ信用金庫

１．サイバーリスクの認識

はじめに、すべての企業に対し、自社がサイバー攻撃を受け、企業活動を妨害される可能性について、どのように認識しているか聞いた結果が**第 1 表**である。

全体でみると、「①可能性は十分ある」と答えた企業は 28.6％にとどまっている。これに対し、「②可能性はあまりない」が 43.9％、「③可能性はほとんどない」が 27.5％となっており、これら「可能性は低い（②＋③）」と認識している企業の合計（71.4％）は7割を超えている。

前年（2025 年）の調査結果と比較すると、「①可能性は十分ある」とする企業は 0.4 ポイント減とほぼ横ばいである。また、「③可能性はほとんどない」は 4.4 ポイント減少した一方、「②可能性はあまりない」が 4.8 ポイント増加した。これらの結果から、中小企業ではサイバーリスクの存在自体は認識されつつあるものの、多くの企業は依然として深刻な脅威とは捉えておらず、危機意識はなお低い水準にあるといえよう。

業種別でみると、「①可能性は十分ある」と答えた企業割合は小売業（13.0％）で最も低い。

従業者規模別でみると、「①可能性は十分ある」と答えた企業割合は規模が大きくなるほど高くなっており、5 人未満では 16.4％であるのに対し、50 人以上では 53.3％と大きな差がみられた。

第 1 表　サイバーリスクの認識　　（％）

区分＼項目		①可能性は十分ある	②可能性はあまりない	③可能性はほとんどない	計	可能性低い ②＋③
業種別	製　造　業	32.6	47.0	20.4	100.0	67.4
	卸　売　業	32.6	48.5	18.9	100.0	67.4
	小　売　業	13.0	37.0	50.0	100.0	87.0
	建　設　業	22.8	44.6	32.6	100.0	77.2
	運輸・通信業	39.3	41.6	19.1	100.0	60.7
	サービス業	30.1	40.6	29.3	100.0	69.9
規模別	5 人未満	16.4	41.6	42.0	100.0	83.6
	5～19 人	32.0	47.1	20.9	100.0	68.0
	20～49 人	49.2	43.1	7.7	100.0	50.8
	50 人以上	53.3	35.0	11.7	100.0	46.7
全　　体		**28.6**	**43.9**	**27.5**	**100.0**	**71.4**
2025 年 4 月		29.0	39.1	31.9	100.0	71.0

２．サイバー攻撃による被害の実態

（１）サイバー攻撃の有無と内容

すべての企業に対し、これまでにサイバー攻撃を受けた経験があるか、またどのような攻撃を受けたのか聞いた結果（複数回答）が**第 2 表-1** である。

全体でみると、「(1)攻撃を受けた経験がある」と答えた企業は 14.7%である。一方、「(2)攻撃を受けた経験なし」とする企業は 85.3%となり、被害を認識していない企業が大多数を占めた。

また、サイバー攻撃の内容については、「①不審メール（なりすまし、詐欺メール）」が 96.2%と突出して多く、メールを介して人の不注意を突く手口が最大の脅威となっている。このほか、「②ウイルス感染（パソコンの乗っ取り）」が 10.3%と続き、「③サーバに負荷をかける DDoS 攻撃」(1.6%)、「④ランサムウェア」(1.6%)、「⑤Webサイト等の改ざん」(0.5%)などは少数にとどまっている。

第 2 表－1　サイバー攻撃の有無と内容　　(%)

区分＼項目		(1)攻撃を受けた経験がある（内訳①～⑤、複数回答）						(2)攻撃を受けた経験なし
			①不審メール	②ウイルス感染	③DDoS攻撃	④ランサムウェア	⑤Web サイト等の改ざん	
業種別	製　造　業	14.4	93.2	15.3	0	0	0	85.6
	卸　売　業	15.2	100.0	5.0	0	0	0	84.8
	小　売　業	11.0	93.8	18.8	12.5	6.3	6.3	89.0
	建　設　業	16.7	100.0	5.6	2.8	0	0	83.3
	運輸・通信業	14.6	92.3	15.4	0	0	0	85.4
	サービス業	15.6	97.5	5.0	0	5.0	0	84.4
規模別	5 人未満	9.6	95.8	10.4	0	0	2.1	90.4
	5～19 人	17.5	95.9	12.2	2.0	2.0	0	82.5
	20～49 人	21.5	96.4	7.1	3.6	3.6	0	78.5
	50 人以上	16.7	100.0	0	0	0	0	83.3
全　　体		**14.7**	**96.2**	**10.3**	**1.6**	**1.6**	**0.5**	**85.3**
2025 年 4 月		14.4	95.0	22.1	7.7	1.7	－	85.6

（２）サイバー攻撃による被害内容

前項２－（１）で、「サイバー攻撃を受けた経験がある」と答えた企業（全体の 14.7%、184 社）に対し、サイバー攻撃により、自社の経営においてどのような被害が生じたかを聞いた結果（複数回答）が**第 2 表－2** である。

全体でみると、「①従業員の負担増」と答えた企業が 31.1%で最も多く、復旧作業や顧客対応などが現場に大きなストレスと追加業務を生んでいる実態が浮き彫りになった。次いで、「②調査費用等の発生」とした企業が 14.2%となっており、専門業者への依頼に伴うコストの発生が一定数みられた。このほか、「③業務停止による売上減」（1.6%）、「④企業の信用力の低下」（0.5%）などの影響も少数ながらあった。

一方、被害について「⑥特になし」と答えた企業は 63.9%で半数以上を占めている。直接的な被害を免れている企業は多いものの、前年（2025 年）調査と比較すると、6.4 ポイント減少しており、中小企業にとってサイバー攻撃がより現実的な脅威となりつつあることがうかがえる。

第 2 表－2 サイバー攻撃による被害内容　　（複数回答、%）

区分＼項目		①従業員の負担増	②調査費用等の発生	③業務停止による売上減	④企業の信用力の低下	⑤顧客から損害賠償請求	⑥特になし
業種別	製造業	27.6	19.0	3.4	0	0	63.8
	卸売業	25.0	5.0	0	0	0	75.0
	小売業	31.3	25.0	0	6.3	0	56.3
	建設業	36.1	16.7	0	0	0	58.3
	運輸・通信業	38.5	7.7	0	0	0	61.5
	サービス業	32.5	7.5	2.5	0	0	67.5
規模別	5 人未満	20.8	14.6	0	2.1	0	70.8
	5～19 人	37.1	12.4	2.1	0	0	59.8
	20～49 人	28.6	17.9	3.6	0	0	64.3
	50 人以上	30.0	20.0	0	0	0	70.0
全体		**31.1**	**14.2**	**1.6**	**0.5**	**0**	**63.9**
2025 年 4 月		－	**23.6**	**2.2**	**1.6**	**0.5**	**70.3**

3．サイバーリスク対策について

（１）対策の内容

次に、すべての企業に対し、サイバー攻撃の脅威から自社を守るため、どのような対策を実施しているか聞いた結果（複数回答）が**第 3 表－1** である。

全体でみると、「①セキュリティソフトの導入」と答えた企業が 66.8％で最も多い。これに、「②データの保護（バックアップや暗号化等）」とする企業が 52.4％で続いており、多くの企業がシステムなどの技術的な対策を優先していることがうかがえる。一方、「③社員教育・訓練の実施」は 22.4％、「④専門部署の設置」は 8.0％にとどまり、人的・組織的な対策はまだ十分とはいえない状況である。

また、「⑥対策なし」とした企業は 17.6％で、およそ 6 社に 1 社がサイバー攻撃に対し無防備な状態となっている。

業種別でみると、「⑥対策なし」とした企業割合は、小売業（37.7％）で4割近くに達し、対策の遅れが目立つ結果となった。

第 3 表－1　対策の内容　　（複数回答、％）

区分＼項目		①セキュリティソフトの導入	②データの保護	③社員教育・訓練の実施	④専門部署の設置	⑤ポリシー・ルール策定	⑥対策なし
業種別	製　造　業	68.0	57.8	20.5	8.3	4.1	15.9
	卸　売　業	75.0	59.1	26.5	13.6	6.1	9.8
	小　売　業	46.6	32.2	19.2	7.5	3.4	37.7
	建　設　業	69.2	50.0	20.6	6.5	1.9	15.0
	運輸・通信業	74.2	48.3	25.8	6.7	4.5	14.6
	サービス業	67.6	55.5	25.4	6.6	3.9	16.4
規模別	5 人未満	51.4	41.2	13.8	5.4	2.4	31.8
	5～19 人	74.9	57.5	24.4	7.4	3.9	10.1
	20～49 人	84.6	68.5	39.2	13.8	5.4	2.3
	50 人以上	81.7	65.0	38.3	23.3	11.7	3.3
全　体		**66.8**	**52.4**	**22.4**	**8.0**	**3.8**	**17.6**
2025 年 4 月		70.1	45.5	20.8	5.1	2.0	20.5

（２）自社対応における障壁

すべての企業に対し、サイバーリスク対策を進める上で障壁となっていることについて聞いた結果（複数回答）が**第 3 表－2** である。

全体でみると、「①専任担当者が不在」と答えた企業が 41.3％で最も多く、「②対策費が重荷」とする企業（40.2％）が僅差で続いている。中小企業にとって、人材不足とコスト負担が取り組みを遅らせる主な要因となっていることがうかがえる。

次いで、「③技術的な対策や運用が困難」が 33.7％、「④何を優先すべきか分からない」が 24.7％あり、専門知識やノウハウの不足が対策を阻んでいる実態が浮き彫りとなった。このほか、「⑤従業員教育が不十分」が 17.3％となっている。

業種別でみると、「①専任担当者が不在」とした企業割合は、卸売業（52.7％）や製造業（46.5％）で比較的高い。

従業者規模別でみると、「④何を優先すべきか分からない」とした企業割合は、規模が小さくなるほど高い傾向にある

第 3 表－2　自社対応における障壁　　（複数回答、％）

区分＼項目		①専任担当者が不在	②対策費が重荷	③技術的対策や運用が困難	④何を優先すべきか分からない	⑤従業員教育が不十分
業種別	製　造　業	46.5	40.1	38.6	23.7	18.6
	卸　売　業	52.7	42.0	32.1	21.4	22.1
	小　売　業	26.7	30.8	17.8	26.0	11.6
	建　設　業	43.5	40.7	36.0	24.3	15.9
	運輸・通信業	39.3	43.8	38.2	24.7	24.7
	サービス業	34.5	43.1	32.2	27.5	14.5
規模別	5 人未満	29.1	33.7	25.5	25.7	9.6
	5～19 人	48.7	44.2	37.7	26.4	19.9
	20～49 人	53.8	43.1	46.2	19.2	29.2
	50 人以上	47.5	50.8	37.3	11.9	30.5
全　　体		**41.3**	**40.2**	**33.7**	**24.7**	**17.3**

４．今後の取り組み方針

最後に、今後のサイバーリスク対策として、特に重要と考える取り組みは何か、すべての企業に対し複数回答で聞いた結果が**第 4 表**である。

全体でみると、「①（OS・ソフトウェアの更新など）基本的な技術対策の徹底」（59.2%）と「②セキュリティ製品の導入・強化」（56.2%）がいずれも5割を超えており、多くの企業が技術的な防御力の底上げを優先すべき課題としていることが明らかになった。続いて、「③従業員教育の充実」（46.6%）が半数近くに上り、システムのみならずリテラシー向上への意識も高まりつつある。以下、「④復旧手順の整備」が 35.3%、「⑤予算の確保」が 11.2%となった。

業種別でみると、「①基本的な技術対策の徹底」とした企業割合は製造業（63.7%）や卸売業（62.8%）で比較的高い。

従業者規模別でみると、「③従業員教育の充実」とした企業割合は規模が大きくなるほど高い傾向にある。

第 4 表　今後の取り組み方針　　（複数回答、%）

区分＼項目		①基本的な技術対策の徹底	②セキュリティ製品の導入・強化	③従業員教育の充実	④復旧手順の整備	⑤予算の確保
業種別	製　造　業	63.7	60.5	42.5	37.5	12.6
	卸　売　業	62.8	59.7	52.7	44.2	17.8
	小　売　業	49.6	44.6	47.5	20.9	8.6
	建　設　業	56.6	59.0	43.4	33.5	11.3
	運輸・通信業	56.8	56.8	59.1	34.1	4.5
	サービス業	58.3	51.6	48.0	37.3	9.1
規模別	5 人未満	56.4	49.8	33.8	30.1	9.8
	5～19 人	61.6	60.8	53.4	37.0	11.4
	20～49 人	58.5	60.8	57.7	41.5	11.5
	50 人以上	61.0	55.9	62.7	49.2	20.3
全　　体		**59.2**	**56.2**	**46.6**	**35.3**	**11.2**

以　上