NEWS RELEASE

アンケート調査結果

２０２５．５．１５
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「対策なし」企業が 20.5%
～ 未対策の理由「対策法がわからない」(36.0%)が最多

近年、サプライチェーンの脆弱性を狙ったサイバー攻撃が深刻な脅威となっている。そのため、情報セキュリティ対策が十分でない中小企業が標的となる可能性が高く、対策を強化することが重要な課題となっている。
そこで、中小企業におけるサイバーリスクへの対応状況はどうか、アンケート調査で探ってみた。

■ 調査時点：2025 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
■ 依頼先数 ： 1,400 社
有効回答数 ： 1,274 社
有効回答率 ： 91.0%
■ 有効回答内訳：下表のとおり

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	114 社	197 社	52 社	18 社	381 社	29.9 %
卸 売 業	60	66	13	3	142	11.1 %
小 売 業	100	39	6	6	151	11.9 %
建 設 業	94	114	11	6	225	17.7 %
運輸・通信業	13	54	14	11	92	7.2 %
サービス業	146	86	28	23	283	22.2 %
計	527	556	124	67	1,274	100.0 %
構成比	41.4%	43.6%	9.7%	5.3%	100.0%	―

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ることにより、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」と認識している企業は 29.0%である。これに対し、「②可能性はあまりない」とした企業が 39.1%、「③可能性はほとんどない」とした企業が 31.9%で、これら「可能性は低い(②+③)」と認識している企業の合計は 71.0%にのぼる。

これを 23 年調査と比較すると、「①可能性は十分ある」とした企業は 6.8 ポイント増加し、認識の向上がみられた。しかし、依然として3割未満の低い水準にとどまっており、全体として危機意識が十分に醸成されているとは言い難い。

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(7.9%)で極めて低くなっている。

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 15.4%であるのに対し、50 人以上では 59.7%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	32.3	40.9	26.8	100.0	67.7
	卸　売　業	40.1	34.5	25.4	100.0	59.9
	小　売　業	7.9	31.1	61.0	100.0	92.1
	建　設　業	28.4	42.3	29.3	100.0	71.6
	運輸・通信業	38.0	42.4	19.6	100.0	62.0
	サービス業	27.6	39.5	32.9	100.0	72.4
規模別	5 人未満	15.4	36.2	48.4	100.0	84.6
	5～19 人	34.5	41.9	23.6	100.0	65.5
	20～49 人	45.2	41.9	12.9	100.0	54.8
	50 人以上	59.7	32.8	7.5	100.0	40.3
全　　体		**29.0**	**39.1**	**31.9**	**100.0**	**71.0**
2023 年 7 月		22.2	38.5	39.3	100.0	77.8

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種類

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、複数回答で聞いた結果が**第 2 表−1** である。

全体でみると、「(1)サイバー攻撃を受けた経験がある」と答えた企業は 14.4%であるのに対し、「(2)攻撃を受けていない」とする企業が 85.6%と圧倒的に多い。この背景には、企業の防衛力が向上していることが考えられる。しかし一方で、近年のサイバー攻撃はより巧妙になっており、気づかないうちに軽微な攻撃を受けている可能性も否定できない。

サイバー攻撃の種類をみると、「①不審メール(なりすまし、詐欺メール)」が 95.0%で最も多い。次いで、「②ウイルス感染(パソコンの乗っ取り)」が 22.1%で多く、以下、「③サーバに負荷をかける(DDos攻撃)」(7.7%)、「④データの漏洩・破壊」(3.9%)、「⑤ランサムウェア」(1.7%)などとなっている。

従業者規模別でみると、「(1)攻撃を受けた経験がある」と答えた企業割合は、規模が大きくなるほど高くなっている。

第 2 表－1　サイバー攻撃の有無と種類　　(%)

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)攻撃を受けていない
			①不審メール	②ウイルス感染	③DDos攻撃	④データ漏洩・破壊	⑤ランサムウェア	
業種別	製　造　業	16.5	95.2	24.2	8.1	3.2	0	83.5
	卸　売　業	21.1	86.7	23.3	6.7	6.7	3.3	78.9
	小　売　業	4.6	100.0	0	0	0	0	95.4
	建　設　業	12.9	96.6	17.2	10.3	0	0	87.1
	運輸・通信業	20.7	94.7	21.1	10.5	0	0	79.3
	サービス業	12.7	100.0	25.7	5.7	8.6	5.7	87.3
規模別	5 人未満	8.7	95.5	25.0	6.8	4.5	0	91.3
	5～19 人	16.5	95.6	18.7	5.5	2.2	2.2	83.5
	20～49 人	18.5	91.3	21.7	8.7	4.3	4.3	81.5
	50 人以上	34.3	95.7	30.4	17.4	8.7	0	65.7
全　　体		**14.4**	**95.0**	**22.1**	**7.7**	**3.9**	**1.7**	**85.6**
2024 年 7 月		27.9	92.3	15.9	4.9	3.0	3.3	72.1

（２）サイバー攻撃による不利益

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 14.4%、184 社）に対し、サイバー攻撃を受けたことにより、自社の経営においてどのような不利益が生じたか、複数回答で聞いた結果が**第 2 表－2** である。

全体でみると、サイバー攻撃による不利益の内容としては、「①原因調査や事故対応等に費用がかかった」と答えた企業が 23.6%で最も多い。次いで、「②納期遅れや営業機会の逸失」とした企業が 8.8%となっており、以下、「③生産・サービス停止による売上減」（2.2%）、「④企業の信用力の低下」（1.6%）などとなっている。

一方、「⑥特に不利益はなかった」と答えた企業が 70.3%と 7 割を占めている。つまり、多くの企業がサイバー攻撃を受けても被害はなかったと判断しているが、実際には目に見えにくい被害が十分に把握されていない懸念もある。

第 2 表－2　サイバー攻撃による不利益　　（複数回答、%）

区分＼項目		①調査費用等の発生	②営業機会の逸失等	③生産停止による売上減	④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	27.4	11.3	6.5	1.6	0	67.7
	卸　売　業	23.3	13.3	0	0	0	73.3
	小　売　業	0	0	0	0	0	100.0
	建　設　業	17.2	6.9	0	0	0	75.9
	運輸・通信業	36.8	5.3	0	0	0	57.9
	サービス業	19.4	5.6	0	5.6	2.8	69.4
規模別	5 人未満	20.0	8.9	0	0	2.2	68.9
	5～19 人	18.7	7.7	3.3	3.3	0	74.7
	20～49 人	30.4	13.0	4.3	0	0	69.6
	50 人以上	43.5	8.7	0	0	0	56.5
全　体		**23.6**	**8.8**	**2.2**	**1.6**	**0.5**	**70.3**
2024 年 7 月		**39.8**	**10.2**	**4.1**	**4.7**	**0.3**	**49.5**

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 70.1％で最も多い。次いで、「②データの保護（バックアップや暗号化等）」とする企業が 45.5％で多く、技術的な対策が主となっている。また、「③社員教育・訓練の実施」とする企業は 20.8％であるが、24 年調査（7.8％）を 13.0 ポイント上回っており、人的な対策に注力する企業も増えていることがうかがえる。以下、「④専門部署の設置」（5.1％）、「⑤セキュリティベンダー等とのコンサルタント契約」（2.0％）となった。なお、「⑥対策していない」とする企業は 20.5％で、2割程度となっている。

従業員規模別でみると、「⑥対策していない」とする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－1　対策の内容　　（複数回答、％）

区分＼項目		①セキュリティソフト導入	②データの保護	③社員教育・訓練実施	④専門部署の設置	⑤コンサルタント契約	⑥対策なし
業種別	製　造　業	74.2	52.1	20.5	4.5	2.1	15.0
	卸　売　業	76.1	49.3	23.2	7.0	2.8	17.6
	小　売　業	41.3	21.3	12.0	4.0	0	48.0
	建　設　業	76.4	51.1	24.0	4.4	1.3	13.8
	運輸・通信業	78.3	47.8	30.4	5.4	1.1	12.0
	サービス業	69.0	42.3	18.9	6.0	3.2	22.8
規模別	5 人未満	57.7	34.6	7.6	2.9	1.0	32.3
	5～19 人	76.4	49.5	27.2	4.7	1.1	14.2
	20～49 人	82.3	62.9	36.3	5.6	8.1	7.3
	50 人以上	91.0	65.7	41.8	25.4	6.0	4.5
全　体		**70.1**	**45.5**	**20.8**	**5.1**	**2.0**	**20.5**
2024 年 7 月		67.9	42.6	7.8	2.3	2.0	22.6

（２）未対策の理由

前項3－(1)で、サイバーリスクについて、「対策していない」と答えた企業（全体の 20.5%、260 社）に対し、未対策の理由について複数回答で聞いた結果が**第 3 表－2** である。

全体でみると、「①対策法がわからないから」と答えた企業が 36.0%で最も多い。専門知識を持つ人材がいない企業では、セキュリティ対策の重要性は理解していても、具体的な対策の進め方が分からず、結果として未対策のままになるケースが少なくないようだ。

次いで、「②優先順位が低いから」とする企業が 31.6%、「③忙しくて手が回らないから」が22.9%となっている。中小企業は取り扱うデータ量が少ないため、サイバー攻撃の標的にならないとの思い込みから対策が後回しになっている現状がうかがえる。

以下、「④効果がみえないから」(19.0%)、「⑤対策費用が重荷だから」(17.0%)などとなっている。

第 3 表－2　未対策の理由　　（複数回答、%）

区分＼項目		①対策法がわからない	②優先順位が低い	③忙しくて手が回らない	④効果がみえない	⑤対策費が重荷	⑥その他
業種別	製　造　業	35.7	39.3	28.6	21.4	16.1	1.8
	卸　売　業	45.8	12.5	20.8	20.8	20.8	12.5
	小　売　業	35.7	28.6	14.3	28.6	11.4	1.4
	建　設　業	27.6	31.0	37.9	13.8	17.2	0
	運輸・通信業	45.5	27.3	27.3	9.1	9.1	9.1
	サービス業	34.9	36.5	20.6	9.5	23.8	3.2
規模別	5 人未満	37.6	32.7	20.6	18.2	16.4	2.4
	5～19 人	32.9	30.3	27.6	21.1	18.4	5.3
	20～49 人	33.3	22.2	22.2	22.2	11.1	0
	50 人以上	33.3	33.3	33.3	0	33.3	0
全　体		**36.0**	**31.6**	**22.9**	**19.0**	**17.0**	**3.2**

4．今後の取り組み方針

最後に、サイバーリスク対策への今後の取り組み方針について、すべての企業に聞いた結果が**第 4 表**である。

全体でみると、「①重要課題として取り組む」と答えた企業は 9.7%と1割未満にとどまり、「②(取引先からの要請など)必要があれば取り組む」とした企業が 67.8%で最も多くなっている。一方、「③取り組む予定なし」とした企業は 22.5%であった。

このように、中小企業では積極的な取り組み方針をもつ企業はまだ少ないのが現状である。しかしながら、近年では企業間取引において、相応のセキュリティ対策が求められる傾向が強まっている。そのため、事業の継続性を守るためにも、サイバーリスク対策を経営戦略の一環として取り入れる必要性が今後さらに高まると考えられる。

業種別でみると、「②必要があれば取り組む」とした企業割合は建設業(76.9%)や運輸・通信業(71.7%)で比較的高い。

従業者規模別でみると、「①重要課題として取り組む」企業割合は規模が大きくなるほど高くなっている。

第 4 表　今後の取り組み方針　　(%)

区分＼項目		①重要課題として取り組む	②必要があれば取り組む	③取り組む予定なし	計
業種別	製　造　業	10.8	69.8	19.4	100.0
	卸　売　業	12.7	68.3	19.0	100.0
	小　売　業	2.0	49.0	49.0	100.0
	建　設　業	7.1	76.9	16.0	100.0
	運輸・通信業	10.9	71.7	17.4	100.0
	サービス業	12.4	66.4	21.2	100.0
規模別	5 人未満	4.7	61.1	34.2	100.0
	5～19 人	10.1	73.5	16.4	100.0
	20～49 人	21.8	69.3	8.9	100.0
	50 人以上	22.4	70.1	7.5	100.0
全　　体		**9.7**	**67.8**	**22.5**	**100.0**

以　上