アンケート調査結果

２０２３．７．２７
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

～ サイバー攻撃を受けた経験がある企業は 32.5%
～ サイバーリスク対策を「実施していない」企業は 22.6%

近年、不正な方法でシステムに侵入し、危害を加えるサイバー攻撃の被害が拡大傾向にある。そうした中、サプライチェーンを構成する中小企業においては、取引先企業への攻撃の足掛かりとされる懸念もあり、早急に対策をとる必要性が高まっている。一般に、中小企業は大企業に比べデジタル化が遅れているとされるが、サイバーリスクへの備えはどうであろうか、サイバー被害の実態とあわせてアンケート調査で探ってみた。

■ 調査時点：2023 年 7 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　：　1,370 社
有効回答率　：　97.9%
■ 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	121 社	234 社	53 社	26 社	434 社	31.6 %
卸 売 業	71	81	10	6	168	12.3 %
小 売 業	111	40	13	5	169	12.3 %
建 設 業	95	126	16	4	241	17.6 %
運 輸 業	9	48	24	6	87	6.4 %
サービス業	143	92	25	11	271	19.8 %
計	550	621	141	58	1,370	100.0 %
構成比	40.1%	45.4%	10.3%	4.2%	100.0%	―

1．サイバーリスクの認識

はじめに、すべての企業に対し、自社のサーバやパソコンなどのコンピュータシステム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 22.2%と2割程度にとどまった。これに対し、「②可能性はあまりない」とした企業が 38.5%、「③可能性はほとんどない」とした企業が 39.3%で、これらを合計した「可能性は低い（②+③）」と認識している企業は 77.8%に及ぶ。このように、中小企業ではサイバーリスクを明確に認識している企業は少ないようである。

業種別でみると、「可能性は低い（②+③）」と答えた企業割合は小売業（88.8%）でとくに高くなっている。

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 12.9%であるのに対し、50 人以上では 58.6%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	23.5	39.9	36.6	100.0	76.5
	卸　売　業	25.0	44.6	30.4	100.0	75.0
	小　売　業	11.2	23.1	65.7	100.0	88.8
	建　設　業	23.7	36.9	39.4	100.0	76.3
	運　輸　業	24.1	50.6	25.3	100.0	75.9
	サービス業	23.2	39.5	37.3	100.0	76.8
規模別	5 人未満	12.9	31.6	55.5	100.0	87.1
	5～19 人	23.3	45.0	31.7	100.0	76.7
	20～49 人	38.3	41.8	19.9	100.0	61.7
	50 人以上	58.6	25.9	15.5	100.0	41.4
全　体		**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

近年のサイバー攻撃による被害は、大手企業のみならず中小企業まで広がっている。そこで、これまでにサイバー攻撃を受けた経験があるか、すべての企業に聞いた結果が**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 32.5%でおよそ3社に1社である。これに対し、「②サイバー攻撃を受けた経験がない」とした企業は 67.5%と多い。ただし、サイバー攻撃の手口は日々巧妙化しており、回答企業において、サイバー攻撃を受けているにも関わらず、気づいていない可能性も否定できない。

業種別でみると、「①サイバー攻撃を受けた経験がある」と答えた企業割合は、運輸業が 42.5%で最も高いのに対し、小売業が 21.3%で最低となった。

第 2 表－(1)　サイバー攻撃の有無　　(%)

区分＼項目		①サイバー攻撃を受けた経験がある	②サイバー攻撃を受けた経験がない	計
業種別	製　造　業	33.6	66.4	100.0
	卸　売　業	36.3	63.7	100.0
	小　売　業	21.3	78.7	100.0
	建　設　業	29.0	71.0	100.0
	運　輸　業	42.5	57.5	100.0
	サービス業	35.1	64.9	100.0
規模別	5 人未満	26.9	73.1	100.0
	5～19 人	33.5	66.5	100.0
	20～49 人	46.1	53.9	100.0
	50 人以上	41.4	58.6	100.0
全　　体		**32.5**	**67.5**	**100.0**

（２）攻撃の種類

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 32.5%、445 社）に対し、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-(2)**である。

全体でみると、「①不審メール（なりすまし、詐欺メール等）」と答えた企業が 94.8%で圧倒的に多い。次いで、「②ウイルス感染」が 18.7%、「③パソコンやサーバ内のデータ漏洩や破壊」が 5.2%と続いている。以下、「④（サーバに負荷をかける）DDos攻撃」（3.4%）、「⑤ランサムウェア」（1.6%）、「⑥Web サイト等の改竄」（0.7%）などとなっている。

業種別でみると、すべての業種で「①不審メール」と答えた企業割合の高さが目立つ。

第 2 表－(2) 攻撃の種類　　（複数回答、%）

区分＼項目		①不審メール	②ウイルス感染	③データ漏洩・破壊	④DDos攻撃	⑤ランサムウェア	⑥サイトの改竄
業種別	製造業	97.3	16.4	3.4	2.7	0	0.7
	卸売業	96.7	16.4	3.3	1.6	0	0
	小売業	94.4	13.9	5.6	5.6	2.8	2.8
	建設業	90.0	22.9	8.6	1.4	5.7	0
	運輸業	97.3	13.5	2.7	2.7	2.7	0
	サービス業	92.6	24.2	7.4	6.3	1.1	1.1
規模別	5人未満	95.3	15.5	4.7	3.4	1.4	0
	5～19人	94.2	19.7	6.3	2.9	1.0	0.5
	20～49人	96.9	16.9	1.5	4.6	1.5	1.5
	50人以上	91.7	33.3	8.3	4.2	8.3	4.2
全体		**94.8**	**18.7**	**5.2**	**3.4**	**1.6**	**0.7**

（３）直近の被害時期

同じく、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 32.5%、445 社）に対し、サイバー攻撃を受けた直近の時期について聞いた結果が**第 2 表－(3)**である。

全体でみると、「①半年以内」と答えた企業が 40.5%で最も多い。これに、「②半年超1年以内」とする企業が 29.9%で続いている。両者を合わせると、直近「1年以内」にサイバー攻撃を受けた企業が 70.4%と7割に及ぶ。同割合は、「③1 年超3年以内」(26.9%)、「④3年超前」(2.9%)と比較して各段に高く、サイバー攻撃の脅威が身近に迫っていることがうかがえる。

業種別でみると、すべての業種において「①半年以内」とする企業割合が最も高くなっている。

第 2 表－(3) 直近の被害時期 (%)

区分＼項目		①半年以内	②半年超 1年以内	③1年超 3年以内	④3年超前	計
業種別	製　造　業	39.0	28.8	29.5	2.7	100.0
	卸　売　業	44.3	24.6	29.5	1.6	100.0
	小　売　業	41.7	30.5	27.8	0	100.0
	建　設　業	39.9	38.6	18.6	2.9	100.0
	運　輸　業	43.3	32.4	18.9	5.4	100.0
	サービス業	38.9	27.4	29.5	4.2	100.0
規模別	5 人未満	41.2	28.4	27.0	3.4	100.0
	5～19 人	41.8	30.3	25.5	2.4	100.0
	20～49 人	36.9	30.8	29.2	3.1	100.0
	50 人以上	33.3	33.3	29.2	4.2	100.0
全　　体		**40.5**	**29.9**	**26.7**	**2.9**	**100.0**

（４）サイバー攻撃による経営上の不利益

同じく、**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 32.5%、445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－(4)**である。

全体でみると、「⑤特に不利益はなかった」と答えた企業は 55.1%で過半を占めた。これに対し、不利益を受けた企業（44.9%、200 社）の具体的な内容では、「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 36.9%で最も多い。次いで、「②営業機会の逸失や生産停止による売上減」とした企業が 10.6%となっており、企業活動に直接的な被害が生じた企業も1割程度あった。このほか、「③自社の信用力評価が低下した」が 5.8%、「④顧客からの損害賠償請求」が 0.9%であった。

第 2 表－(4) サイバー攻撃による経営上の不利益　（複数回答、%）

区分＼項目		①事故対応等に費用がかかった	②営業機会逸失や生産停止による売上減	③信用力評価の低下	④顧客からの損害賠償請求	⑤特に不利益なし
業種別	製　造　業	37.0	13.0	5.5	0.7	55.5
	卸　売　業	34.4	13.1	4.9	0	55.7
	小　売　業	27.8	5.6	8.3	0	63.9
	建　設　業	38.6	11.4	2.9	0	55.7
	運　輸　業	35.1	2.7	8.1	2.7	54.1
	サービス業	41.1	9.5	7.4	2.1	50.5
規模別	5 人未満	29.7	8.1	8.1	0	60.8
	5～19 人	37.5	11.0	4.3	1.0	55.8
	20～49 人	38.5	12.3	7.7	3.1	49.2
	50 人以上	70.8	16.7	0	0	29.2
全　　体		**36.9**	**10.6**	**5.8**	**0.9**	**55.1**

3．セキュリティ対策について

（１）対策の内容

次に、すべての企業に対し、サイバーリスクを意識して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 67.1％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 40.9％で続いており、情報機器の利用に最低限必要な対策が上位を占めた。

以下、「③社員教育や訓練の実施」（14.9％）、「④専門部署の設置」（2.6％）、「⑤セキュリティベンダー等とのコンサルタント契約」（2.4％）と続くが、いずれも少数であるうえ、「⑥対策を実施していない」とする企業も 22.6％と2割を超えており、中小企業のサイバーセキュリティに対する備えは十分とは言い難い。

従業員規模別でみると、ほぼすべての対策項目において、規模が大きくなるほど実施割合が高くなっている。一方、「⑥対策を実施していない」とする企業は規模が小さくなるほど多い。

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	69.8	43.5	15.7	2.5	3.0	20.5
	卸　売　業	69.6	48.8	16.1	2.4	1.8	19.6
	小　売　業	40.2	22.5	9.5	1.8	2.4	46.7
	建　設　業	73.4	38.6	13.7	2.5	0.8	17.4
	運　輸　業	75.9	42.5	21.8	1.1	1.1	14.9
	サービス業	69.4	44.6	15.1	4.1	3.7	19.9
規模別	5 人未満	56.7	31.8	7.3	1.3	2.2	33.1
	5～19 人	71.5	44.9	17.6	2.9	1.6	17.6
	20～49 人	82.3	50.4	24.8	2.1	4.3	10.6
	50 人以上	81.0	60.3	34.5	13.8	8.6	6.9
全　体		**67.1**	**40.9**	**14.9**	**2.6**	**2.4**	**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、「対策を実施していない」と答えた企業（全体の22.6%、310 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サイバーリスクが発生する可能性は低いから」と答えた企業が 39.3%で最も多くなっている。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思い込んでいる企業が少なくないようである。

次いで、「②優先順位が低いから」とする企業が 27.3%で多く、対策の必要性は理解していても、他に優先すべき経営課題があるため、対策が後回しになっている現状がうかがえる。以下、「③対策法がわからないから」(25.3%)、「④忙しくて手が回らないから」(17.5%)、「⑤対策費用がかかるから」(14.9%)などとなっており、人材不足やコスト面での課題を挙げる企業も一定数みられた。

第 3 表－(2) 未対策の理由　　（複数回答、%）

区分＼項目		①リスク発生の可能性低い	②優先順位が低い	③対策法がわからない	④忙しくて手が回らない	⑤対策費が重荷	⑥その他
業種別	製　造　業	43.2	21.6	28.4	21.6	15.9	3.4
	卸　売　業	50.0	34.4	21.9	12.5	12.5	3.1
	小　売　業	36.7	29.1	15.2	13.9	13.9	6.3
	建　設　業	38.1	21.4	33.3	26.2	14.3	4.8
	運　輸　業	46.2	23.1	30.8	7.7	7.7	0
	サービス業	29.6	35.2	29.6	14.8	18.5	1.9
規模別	5 人未満	38.7	27.6	22.1	18.2	13.8	5.5
	5～19 人	38.9	27.8	31.5	15.7	17.6	0.9
	20～49 人	46.7	20.0	20.0	20.0	13.3	6.7
	50 人以上	50.0	25.0	25.0	25.0	0	0
全　　体		**39.3**	**27.3**	**25.3**	**17.5**	**14.9**	**3.9**

（３）支援制度の活用について

最後に、政府は中小企業のサイバーセキュリティ対策を促すため、国の補助で安価にセキュリティを導入できるサービスなどを実施しているが、こうした支援制度を活用する意向があるか、すべての企業に聞いた結果が**第３表－(3)**である。

全体でみると、「①すでに活用している」と答えた企業はわずか 3.1％である。一方、「③(活用しておらず)今後も活用するつもりはない」とした企業が 16.6％となっており、現状では支援制度への関心は低調である。ただ、「②今後、活用の意向あり」とした企業が 34.1％あり、潜在的な需要は少なくないと考えられる。

さらに、「④支援制度を認知していなかった」とする企業が 46.2％と5割近くを占めていることから、今後認知度が高まれば、中小企業のサイバーセキュリティ対策が進む可能性が期待できよう。

第３表－(3) 支援制度の活用について　　（％）

区分＼項目		①活用している	②今後活用の意向あり	③活用するつもりはない	④認知していなかった	計
業種別	製造業	3.0	39.4	15.2	42.4	100.0
	卸売業	3.0	35.7	11.9	49.4	100.0
	小売業	3.0	14.8	22.5	59.7	100.0
	建設業	2.1	33.6	17.0	47.3	100.0
	運輸業	2.3	42.5	13.8	41.4	100.0
	サービス業	4.4	34.3	18.5	42.8	100.0
規模別	5人未満	2.7	21.6	19.5	56.2	100.0
	5～19人	2.6	38.3	14.8	44.3	100.0
	20～49人	2.8	55.3	14.9	27.0	100.0
	50人以上	12.1	55.1	12.1	20.7	100.0
全体		**3.1**	**34.1**	**16.6**	**46.2**	**100.0**