2020年12月

国内企業のサイバーリスク意識・対策実態調査2020

集計報告書

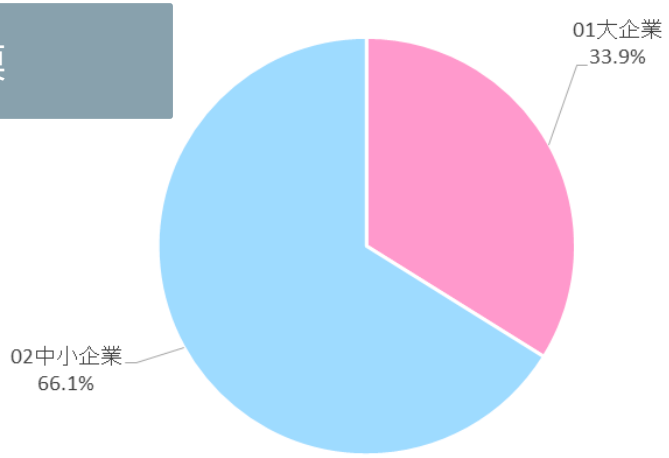
一般社団法人　日本損害保険協会

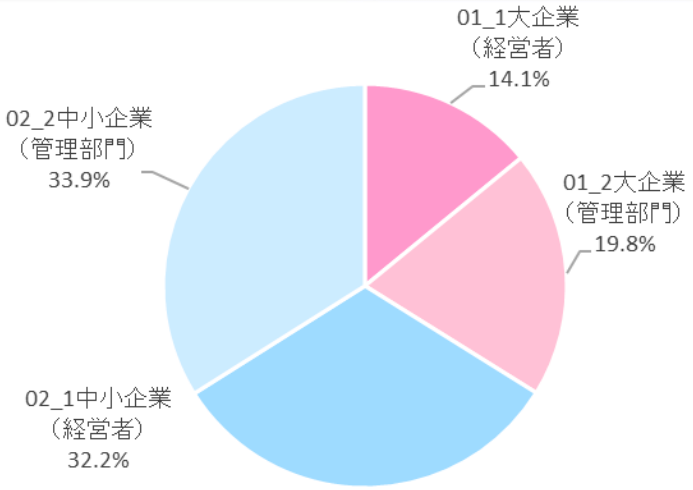
Ⅰ．調査概要

調査対象	調査実施機関の企業モニター調査の登録企業（4,000 社）
回答率	**1,535件／4,000件（38.4%）** ※回答はいずれかの質問に1つでも回答があった企業をカウントしております。 ※集計については、各設問の回答数を母数として行っております。
調査方法	インターネット調査
調査実施機関	株式会社帝国データバンク
調査実施期間	2020年10月1日（木）～2020年10月19日（月）
集計にあたって	・複数回答の回答比率は各項目における回答社数に占める各選択肢の回答件数を表します。 ・不明、回答拒否など回答を得られなかった場合、無回答として設問ごとの集計から除外しています。 ・ｎ：各設問の回答数、SA：単一回答、MA：複数回答

Ⅱ．回答企業属性

企業規模





企業規模2区分	件数	構成比
Q1_全体	1,535	100.0%
01大企業	520	33.9%
02中小企業	1,015	66.1%

企業規模4区分	件数	構成比
全体	1,535	100.0%
01_1大企業（経営者）	216	14.1%
01_2大企業（管理部門）	304	19.8%
02_1中小企業（経営者）	494	32.2%
02_2中小企業（管理部門）	521	33.9%

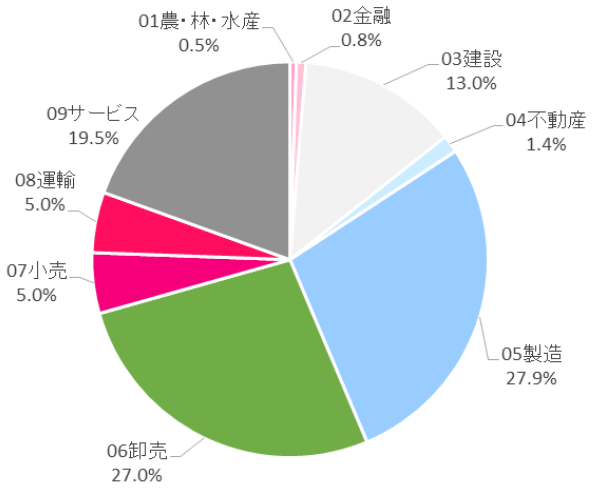
【企業規模区分】

業界	大企業	中小企業（小規模企業を含む）	小規模企業
製造業その他の業界	「資本金3億円を超える」 かつ 「従業員数300人を超える」	「資本金3億円以下」 または 「従業員300人以下」	「従業員20人以下」
卸売業	「資本金1億円を超える」 かつ 「従業員数100人を超える」	「資本金１億円以下」 または 「従業員数100人以下」	「従業員5人以下」
小売業	「資本金5千万円を超える」 かつ 「従業員50人を超える」	「資本金5千万円以下」 または 「従業員50人以下」	「従業員5人以下」
サービス業	「資本金5千万円を超える」 かつ 「従業員100人を超える」	「資本金5千万円以下」 または 「従業員100人以下」	「従業員5人以下」

注1：中小企業基本法で小規模企業を除く中小企業に分類される企業のなかで、業種別の全国売上高ランキングが上位3%の企業を大企業として区分
注2：中小企業基本法で中小企業に分類されない企業のなかで、業種別の全国売上高ランキングが下位50%の企業を中小企業として区分
注3：上記の業種別の全国売上高ランキングは、調査実施機関の産業分類（1,359業種）によるランキング

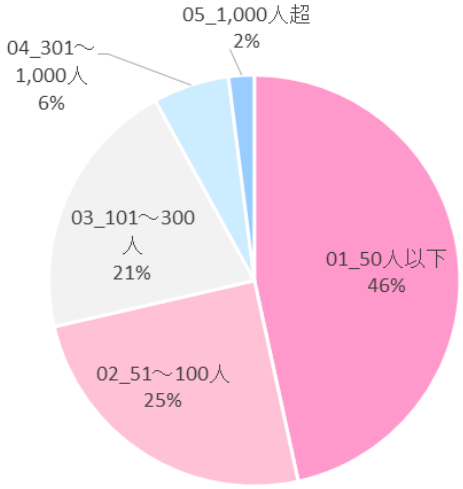
Ⅱ．回答企業属性

業種



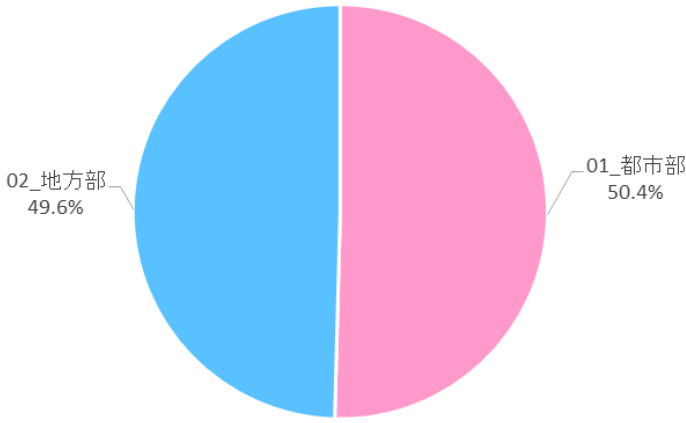
業種10区分	件数	構成比
全体	1535	100.0%
01農・林・水産	8	0.5%
02金融	12	0.8%
03建設	200	13.0%
04不動産	22	1.4%
05製造	428	27.9%
06卸売	414	27.0%
07小売	76	5.0%
08運輸	76	5.0%
09サービス	299	19.5%

従業員数



従業員数	件数	構成比
全体	1,535	100%
01_50人以下	715	46.6%
02_51～100人	381	24.8%
03_101～300人	316	20.6%
04_301～1,000人	92	6.0%
05_1,000人超	31	2.0%

地域



地域別	件数	構成比
全体	1,535	100.0%
01_都市部	774	50.4%
02_地方部	761	49.6%

都市部：埼玉県、千葉県、東京都、神奈川県、
愛知県、大阪府、福岡県
地方部：上記以外の道府県

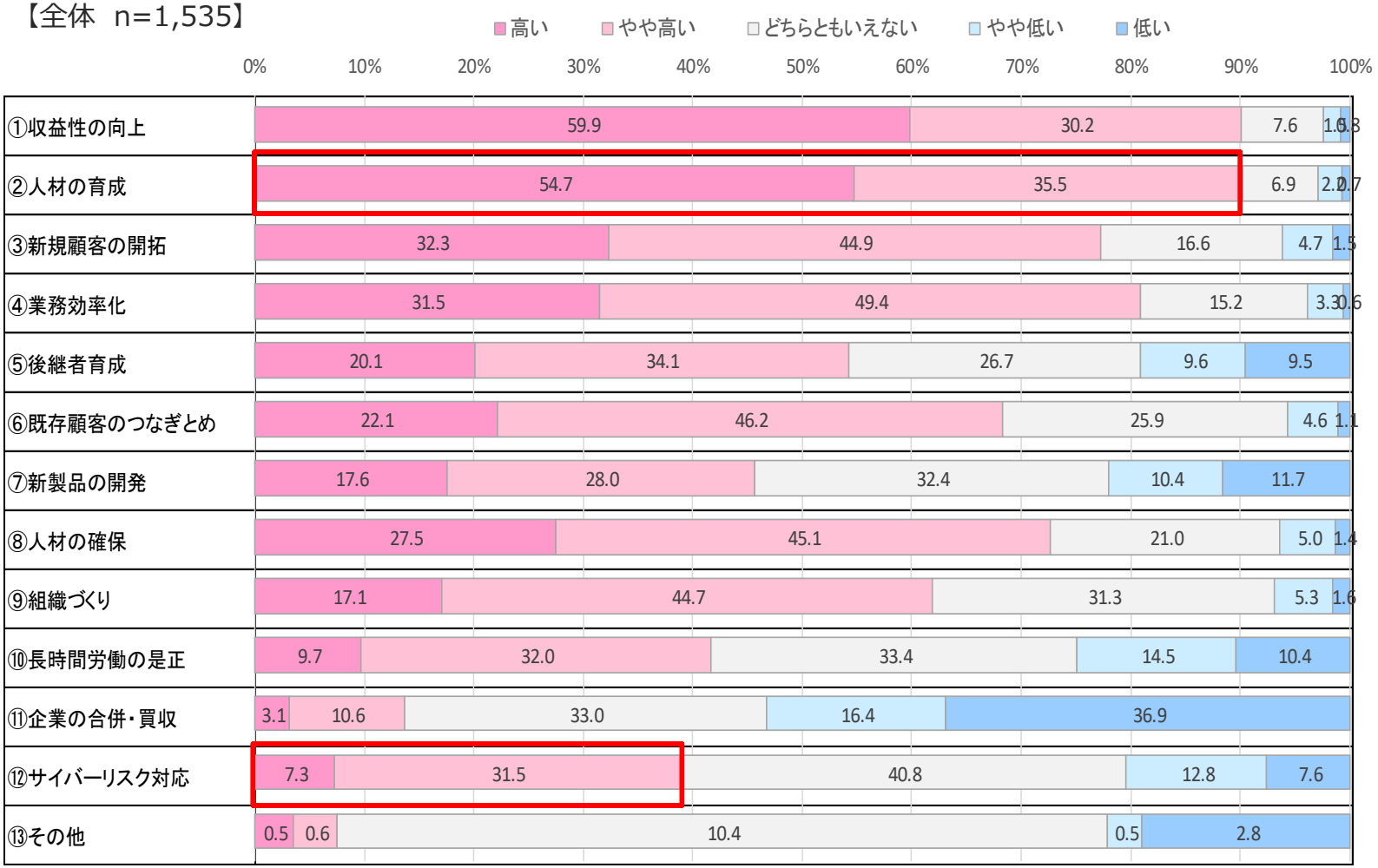
Ⅲ．集計結果

Ⅲ．集計結果（１）回答企業に関する設問
問1．それぞれ経営課題としての優先度を教えてください。(SA)

■優先度が高い経営課題として、9割が、「人材の育成」（90.2%）「収益性の向上」（90.1%）を挙げている。

■「サイバーリスクへの対応」の優先度が高いと認識している企業は4割（38.8%）にとどまっている。

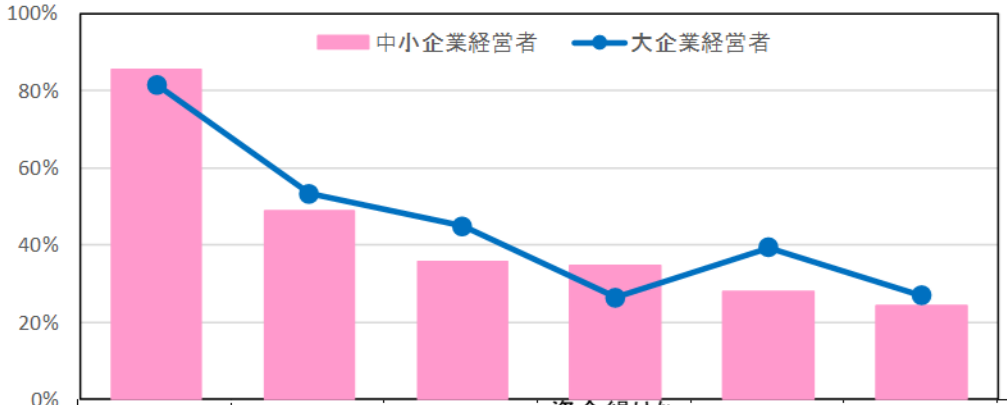
【全体　n=1,535】



Ⅲ．集計結果（１）回答企業に関する設問
問2．経営上の重大リスクと考えるものをすべてお選びください。(MA)

■8割以上（83.1%）が「経済環境の変化」を経営上の重大リスクと認識しており、企業規模別に見ると、中小企業の方が比率が高くなっている（大企業経営者81.5%、中小企業経営者85.6%）。

■「サイバーリスク」を経営上の重大リスクと認識している企業は少なく、全体では25.0%だが、従業員数が1,000名以上の企業では35.5%となっている。



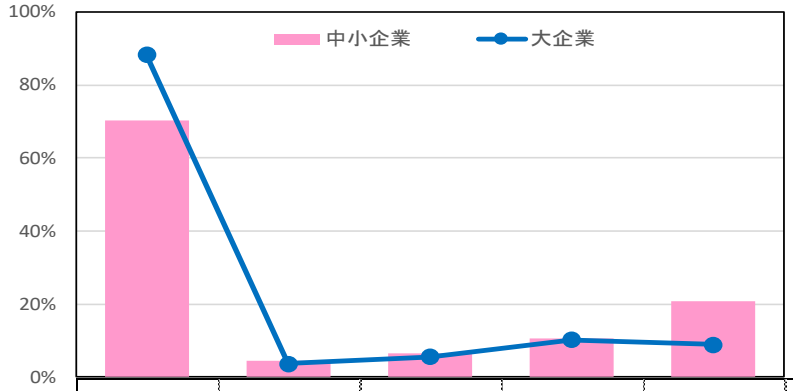
		n=	経済環境の変化	自然災害の発生	人材流出リスク	資金繰りなどの財務リスク	法令順守違反	サイバーリスク	その他	わからない
全体		(1535)	83.1%	49.4%	37.6%	32.8%	35.4%	25.0%	1.4%	1.4%
業種別	01_製造業	(428)	86.2%	50.2%	29.7%	34.3%	29.7%	23.4%	1.4%	1.9%
	02_非製造業	(1107)	81.9%	49.1%	40.7%	32.2%	37.6%	25.6%	1.4%	1.2%
企業規模別	01_1大企業（経営者）	(216)	81.5%	53.2%	44.9%	26.4%	39.4%	26.9%	1.9%	1.4%
	02_1中小企業（経営者）	(494)	85.6%	49.0%	35.6%	34.8%	28.1%	24.3%	1.2%	0.4%
所在地別	01_都市部	(774)	83.6%	50.0%	36.2%	33.7%	34.5%	27.5%	1.0%	1.2%
	02_地方部	(761)	82.7%	48.9%	39.0%	31.8%	36.3%	22.3%	1.7%	1.6%
従業員数別	01_50人以下	(715)	80.4%	49.4%	37.2%	38.0%	30.5%	22.9%	2.0%	1.5%
	02_51～100人	(381)	84.3%	47.8%	38.8%	31.2%	35.7%	23.6%	0.5%	0.8%
	03_101～300人	(316)	86.7%	48.1%	37.3%	25.0%	41.1%	29.1%	0.9%	0.9%
	04_301～1,000人	(92)	83.7%	60.9%	37.0%	27.2%	46.7%	28.3%	2.2%	3.3%
	05_1,000人超	(31)	93.5%	51.6%	35.5%	25.8%	51.6%	35.5%	0.0%	3.2%

※複数回答の為、構成比の合計は100%にならない場合がございます。

Ⅲ．集計結果（１）回答企業に関する設問
問３．貴社におけるテレワークやWEB会議の活用状況について、当てはまるものをすべてお選びください。(MA)

■76.3%がテレワークやWEB会議の両方またはいずれかを活用している。

■大企業は9割（88.3%）、中小企業でも7割（70.1%）が、テレワークやWEB会議の両方またはいずれかを活用している。



		n=	テレワークやWEB会議の両方もしくは片方を活用している	今後両方活用する予定	今後テレワークを活用する予定	今後WEB会議を活用する予定	現在も今後も活用する予定はない	その他	わからない
全体		（1535）	76.3%	4.2%	6.2%	10.4%	16.7%	1.4%	2.7%
業種別	01_製造業	（428）	78.3%	4.0%	5.1%	9.1%	15.2%	1.2%	2.8%
	02_非製造業	（1107）	75.5%	4.2%	6.6%	10.9%	17.3%	1.4%	2.6%
企業規模別	01大企業	（520）	88.3%	3.7%	5.6%	10.2%	8.8%	0.4%	1.2%
	02中小企業	（1015）	70.1%	4.4%	6.5%	10.5%	20.7%	1.9%	3.4%
所在地別	01_都市部	（774）	85.4%	4.4%	5.8%	7.5%	12.3%	1.7%	2.1%
	02_地方部	（761）	67.0%	3.9%	6.6%	13.4%	21.2%	1.1%	3.3%
従業員数別	01_50人以下	（715）	63.4%	4.6%	7.0%	10.8%	25.7%	2.2%	4.1%
	02_51～100人	（381）	79.3%	5.8%	7.3%	13.9%	11.8%	0.5%	1.8%
	03_101～300人	（316）	92.7%	2.2%	3.5%	8.5%	8.2%	0.9%	0.9%
	04_301～1,000人	（92）	100.0%	1.1%	4.3%	3.3%	1.1%	0.0%	2.2%
	05_1,000人超	（31）	100.0%	3.2%	6.5%	0.0%	0.0%	0.0%	0.0%

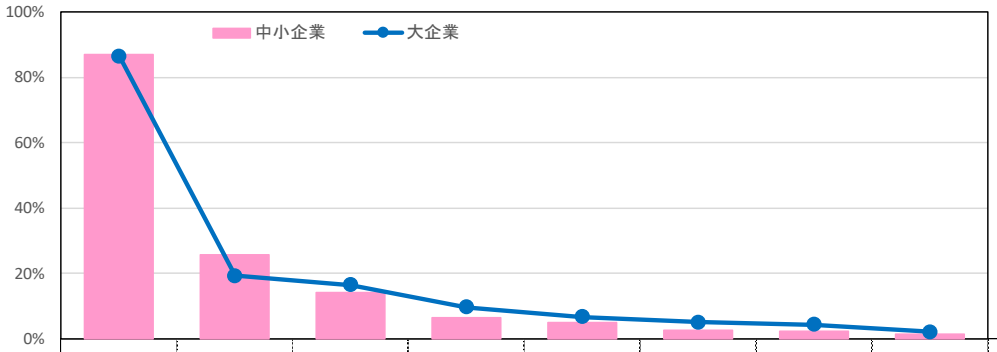
※複数回答の為、構成比の合計は100%にならない場合がございます。

Ⅲ．集計結果（１）回答企業に関する設問

【問３.で『現在も今後も活用する予定はない』『わからない』以外を選択された企業のみ対象】

問４-1．テレワークやWEB会議を活用したきっかけ（活用予定の場合は、検討したきっかけ）について、当てはまるものをすべてお選びください。(MA)

■テレワークやWEB会議を活用したきっかけ（活用予定の場合は、検討したきっかけ）について、「新型コロナウイルス感染症（COVID-19）の影響のため」が86.8%と最も多く、実際にテレワークやWEB会議を活用している企業においては89.3%となっている。



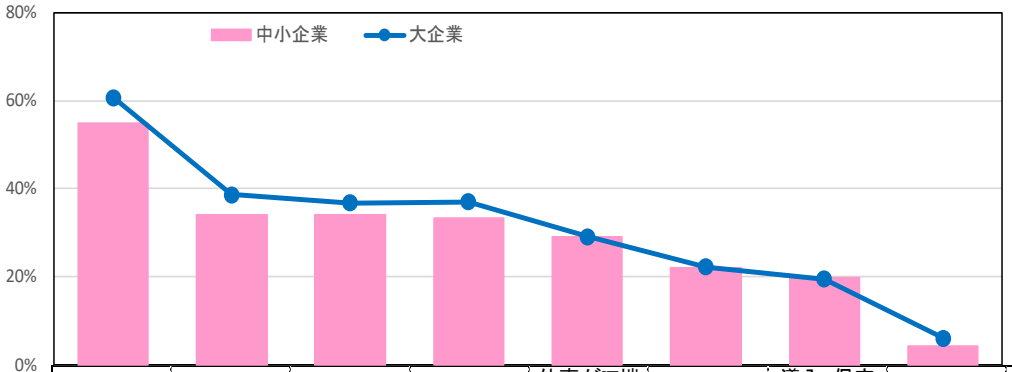
		n=	新型コロナウイルス感染症（COVID-19）の影響のため	取引先からの要請のため	従業員の作業効率やモチベーション向上のため	通勤に対するコストやデメリットの見直しのため	子育てや介護をしながら働き続けたい従業員が増加したため	多様な人材（障がい者、高齢者、外国人）の活用が可能になるため	東京オリンピック・パラリンピックに向けた働き方改革のため	オフィスレイアウト（フリーアドレス）導入のため	その他	わからない
全体		(1242)	86.8%	23.3%	15.1%	7.7%	5.6%	3.6%	3.0%	1.8%	5.7%	1.3%
業種別	01_製造業	(353)	85.8%	30.9%	15.0%	7.9%	5.1%	4.0%	2.3%	1.7%	4.0%	1.1%
	02_非製造業	(889)	87.2%	20.2%	15.1%	7.6%	5.8%	3.5%	3.3%	1.8%	6.4%	1.3%
企業規模別	01大企業	(468)	86.5%	19.2%	16.5%	9.6%	6.6%	5.1%	4.3%	2.1%	5.3%	0.4%
	02中小企業	(774)	87.0%	25.7%	14.2%	6.6%	5.0%	2.7%	2.2%	1.6%	5.9%	1.8%
所在地別	01_都市部	(665)	88.1%	21.1%	14.0%	9.9%	6.6%	3.8%	4.5%	2.6%	4.5%	1.1%
	02_地方部	(577)	85.3%	25.8%	16.3%	5.2%	4.5%	3.5%	1.2%	0.9%	7.1%	1.6%
従業員数別	01_50人以下	(506)	83.4%	25.7%	15.0%	7.5%	4.3%	2.6%	2.2%	1.2%	6.1%	1.8%
	02_51～100人	(329)	89.4%	27.7%	14.6%	8.2%	5.2%	3.6%	2.1%	2.4%	4.9%	1.2%
	03_101～300人	(287)	88.5%	19.5%	15.0%	7.7%	5.6%	3.8%	2.8%	1.7%	4.5%	1.0%
	04_301～1,000人	(89)	88.8%	11.2%	16.9%	7.9%	9.0%	6.7%	6.7%	2.2%	9.0%	0.0%
	05_1,000人超	(31)	93.5%	6.5%	16.1%	6.5%	22.6%	9.7%	16.1%	3.2%	9.7%	0.0%
テレワーク・WEB活用状況	活用している	(1057)	89.3%	22.9%	14.8%	7.9%	6.4%	3.8%	3.4%	2.0%	5.8%	0.6%
	活用予定がある	(294)	84.7%	26.2%	21.1%	10.9%	3.4%	4.1%	0.7%	2.0%	4.4%	2.7%

※複数回答の為、構成比の合計は100%にならない場合がございます。

【問３.で『現在も今後も活用する予定はない』『わからない』以外を選択された企業のみ対象】
問４-2．テレワークやWEB会議の活用によって発生、または懸念している問題について、当てはまるものをすべてお選びください。(MA)

■テレワークやWEB会議の活用によって発生、または懸念している問題として、「従業員間のコミュニケーション不足」（57.0%）が最も多く、次に「情報漏えい等のサイバーリスク」（35.8%）が多かった。

■テレワークやWEB会議の活用を予定している企業の4割（41.2%）が「情報漏えい等のサイバーリスク」を懸念している。



		n=	従業員間のコミュニケーション不足	情報漏えい等のサイバーリスク	勤怠管理の複雑化	セキュリティ対策	仕事がIT端末を用いた業務に限定される	組織力の低下	導入・保守コストなど設備投資の増加	従業員のサービス残業増加	その他	わからない
全体		(1242)	57.0%	35.8%	35.0%	34.7%	29.0%	22.1%	19.6%	4.8%	3.3%	7.4%
業種別	01_製造業	(353)	53.0%	36.3%	33.7%	37.1%	31.4%	17.0%	18.4%	5.4%	3.1%	9.6%
	02_非製造業	(889)	58.6%	35.7%	35.5%	33.7%	28.0%	24.2%	20.1%	4.6%	3.4%	6.5%
企業規模別	01大企業	(468)	60.7%	38.7%	36.8%	37.0%	29.1%	22.2%	19.4%	6.0%	1.9%	5.6%
	02中小企業	(774)	54.8%	34.1%	34.0%	33.3%	28.9%	22.1%	19.8%	4.1%	4.1%	8.5%
所在地別	01_都市部	(665)	61.2%	37.7%	39.2%	36.1%	32.3%	24.7%	18.5%	5.1%	2.7%	5.1%
	02_地方部	(577)	52.2%	33.6%	30.2%	33.1%	25.1%	19.2%	21.0%	4.5%	4.0%	10.1%
従業員数別	01_50人以下	(506)	52.6%	32.6%	33.0%	31.4%	28.9%	20.9%	21.1%	3.8%	4.7%	7.9%
	02_51～100人	(329)	58.4%	38.3%	32.8%	35.3%	29.2%	23.7%	22.8%	4.0%	2.7%	7.6%
	03_101～300人	(287)	60.3%	33.8%	36.6%	36.6%	30.0%	22.6%	13.9%	5.9%	2.4%	8.0%
	04_301～1,000人	(89)	61.8%	47.2%	44.9%	47.2%	24.7%	24.7%	20.2%	11.2%	1.1%	2.2%
	05_1,000人超	(31)	71.0%	48.4%	48.4%	29.0%	32.3%	12.9%	12.9%	3.2%	0.0%	6.5%
テレワーク・WEB活用状況	活用している	(1057)	58.9%	35.7%	35.7%	33.5%	29.9%	22.6%	17.5%	4.8%	3.4%	7.1%
	活用予定がある	(294)	47.6%	41.2%	34.4%	43.2%	33.7%	20.4%	30.3%	5.1%	3.7%	6.5%

※複数回答の為、構成比の合計は100%にならない場合がございます。

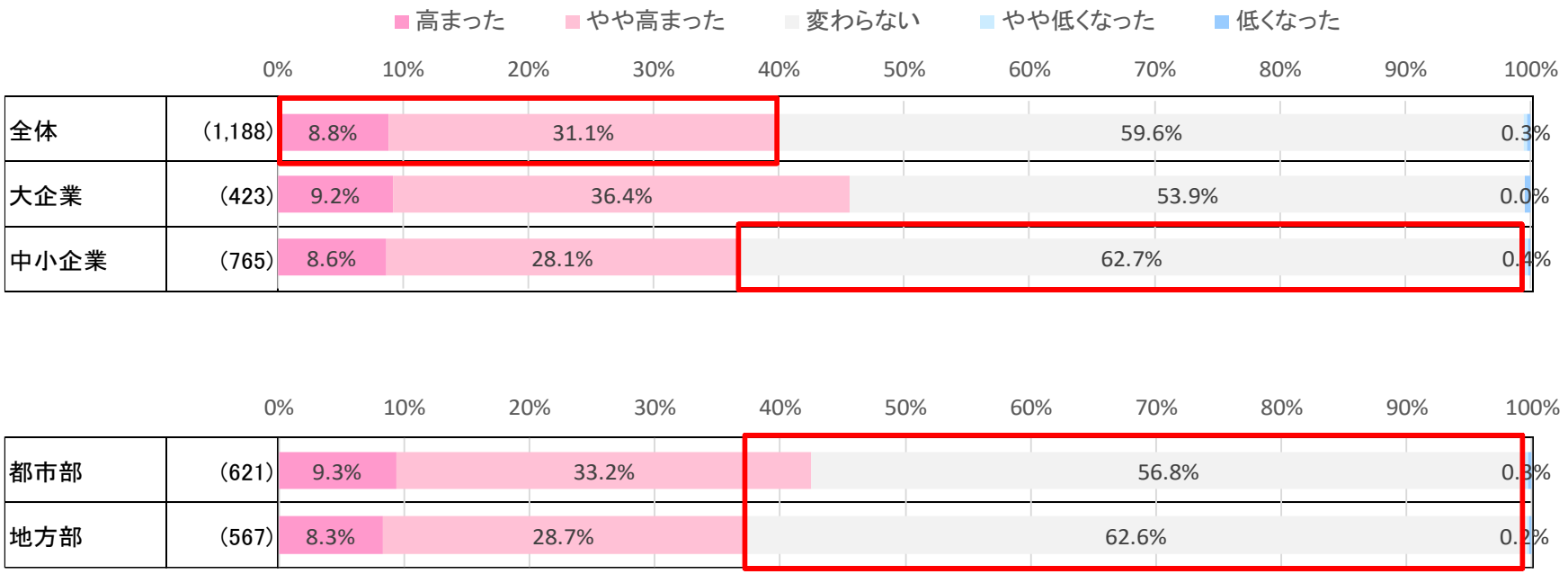
Ⅲ．集計結果（２）サイバーリスク意識・対策実態について

問５．貴社がサイバー攻撃を受ける可能性について、新型コロナウイルスの感染拡大以前と比べてどう思いますか。(SA)

■4割（39.9%）が、新型コロナウイルスの感染拡大以前と比べてサイバー攻撃を受ける可能性が「高まった」、「やや高まった」と認識している。

■一方、半数以上（59.6%）の企業が以前と比べて「変わらない」と認識しており、企業規模別に見ると、中小企業の方がその比率が高くなっている（62.7%）。

■地域別に見ると、地方部の企業の方が「変わらない」と認識している傾向がある。

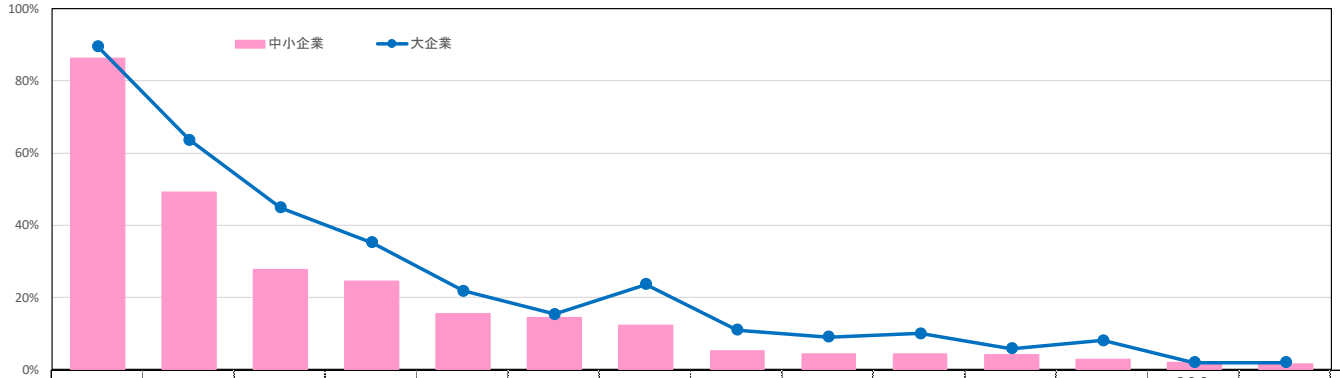


Ⅲ．集計結果（２）サイバーリスク意識･対策実態について

問６．貴社ではどのようなサイバーリスク対策を行っていますか。行っている対策について、当てはまるものをすべてお選びください。(MA)

■9割以上（1,442社、93.9%）が何らかのサイバーリスク対策を行っている。

■具体的な対策として、「ソフトウェア等の脆弱性管理・ウイルス対策ソフトの導入」（87.4%）が最も多く、次に「アクセス権限・ログの管理および制御」（54.1%）、「社員教育（研修・訓練の実施）」（33.5%）が多かった。



		n=	ソフトウェア等の脆弱性管理･ウイルス対策ソフトの導入	アクセス権限･ログの管理および制御	社員教育（研修･訓練の実施）	データ保護（暗号化･DLPなど）	セキュリティ認証の取得	外部専門家からのアドバイス	セキュリティポリシーや事故対応マニュアルの策定	専門人材の雇用･育成	サイバーセキュリティ対策予算の確保	リスクアセスメントの実施	取引先や委託先への対策依頼･義務化	専門部署の設置	SOC（Security Operation Center）による常時監視	EDR（Endpoint Detection & Response）の導入	その他	現在、サイバーリスク対策を行っていない	わからない
全体		(1535)	87.4%	54.1%	33.5%	28.1%	17.7%	14.7%	16.2%	7.1%	6.0%	6.3%	4.6%	4.6%	2.0%	1.6%	1.2%	3.6%	3.3%
業種別	01_製造業	(428)	87.4%	56.1%	31.3%	24.3%	15.2%	12.9%	16.1%	7.9%	7.0%	5.8%	2.8%	4.7%	2.1%	1.6%	0.5%	2.8%	4.4%
	02_非製造業	(1107)	87.4%	53.3%	34.3%	29.6%	18.6%	15.4%	16.2%	6.8%	5.6%	6.5%	5.3%	4.6%	1.9%	1.6%	1.4%	4.0%	2.8%
企業規模別	01大企業	(520)	89.4%	63.7%	44.8%	35.2%	21.7%	15.4%	23.7%	11.0%	9.0%	10.0%	5.8%	8.1%	1.9%	1.9%	0.4%	3.3%	1.9%
	02中小企業	(1015)	86.4%	49.2%	27.7%	24.5%	15.6%	14.4%	12.3%	5.1%	4.4%	4.4%	4.0%	2.9%	2.0%	1.5%	1.6%	3.8%	3.9%
所在地別	01_都市部	(774)	88.1%	58.9%	37.6%	32.9%	19.9%	14.2%	19.9%	7.5%	7.4%	8.5%	5.9%	6.5%	2.6%	1.7%	1.7%	2.7%	3.6%
	02_地方部	(761)	86.7%	49.1%	29.3%	23.3%	15.4%	15.2%	12.4%	6.7%	4.6%	4.1%	3.3%	2.8%	1.3%	1.6%	0.7%	4.6%	2.9%
従業員数別	01_50人以下	(715)	86.2%	42.0%	23.2%	22.7%	13.7%	15.4%	8.0%	3.8%	3.6%	3.1%	4.1%	2.0%	1.8%	1.8%	1.4%	5.0%	3.8%
	02_51～100人	(381)	88.5%	60.4%	32.0%	27.6%	18.4%	13.4%	15.5%	5.8%	5.5%	5.0%	5.0%	5.2%	2.1%	1.0%	1.3%	3.1%	2.9%
	03_101～300人	(316)	88.6%	64.9%	45.9%	30.7%	22.2%	14.9%	26.9%	13.0%	7.6%	10.1%	5.4%	5.7%	0.9%	1.9%	0.9%	2.2%	1.6%
	04_301～1,000人	(92)	87.0%	78.3%	60.9%	54.3%	28.3%	14.1%	31.5%	14.1%	14.1%	17.4%	4.3%	13.0%	3.3%	1.1%	0.0%	1.1%	5.4%
	05_1,000人超	(31)	93.5%	74.2%	80.6%	58.1%	22.6%	16.1%	58.1%	19.4%	25.8%	25.8%	6.5%	22.6%	9.7%	3.2%	0.0%	0.0%	6.5%

※複数回答の為、構成比の合計は100%にならない場合がございます。

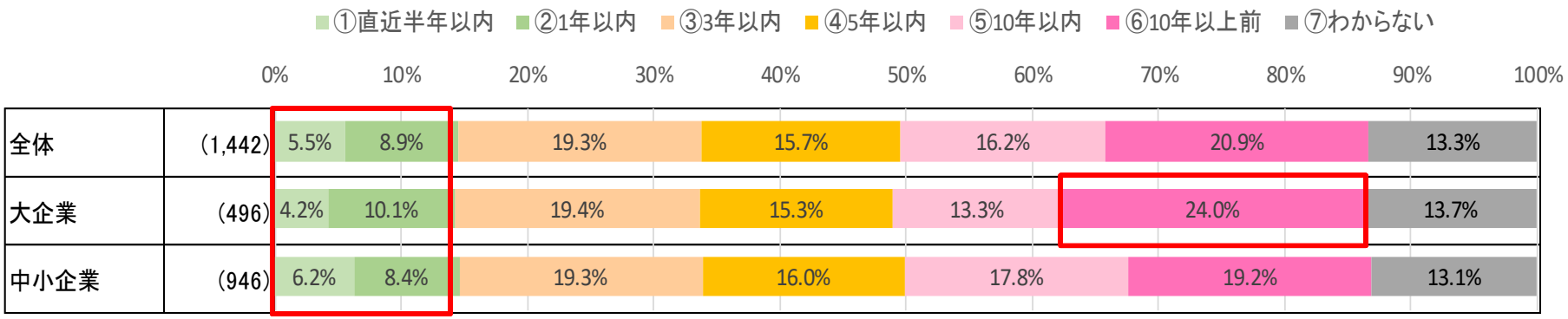
Ⅲ．集計結果（２）サイバーリスク意識・対策実態について

【問６.で『現在、サイバーリスク対策を行っていない』『わからない』以外を選択された企業のみ対象】

問７-１．サイバーリスク対策を開始した時期について教えてください。(SA)

■14.4%が、直近1年以内にサイバーリスク対策を開始している。

■企業規模別で大きな差はないが、「10年以上前」に対策を開始した企業は、大企業の方が比率が高くなっている。



		①直近半年以内	②1年以内	③3年以内	④5年以内	⑤10年以内	⑥10年以上前	⑦わからない
全体	(1,442)	5.5%	8.9%	19.3%	15.7%	16.2%	20.9%	13.3%
大企業	(496)	4.2%	10.1%	19.4%	15.3%	13.3%	24.0%	13.7%
中小企業	(946)	6.2%	8.4%	19.3%	16.0%	17.8%	19.2%	13.1%

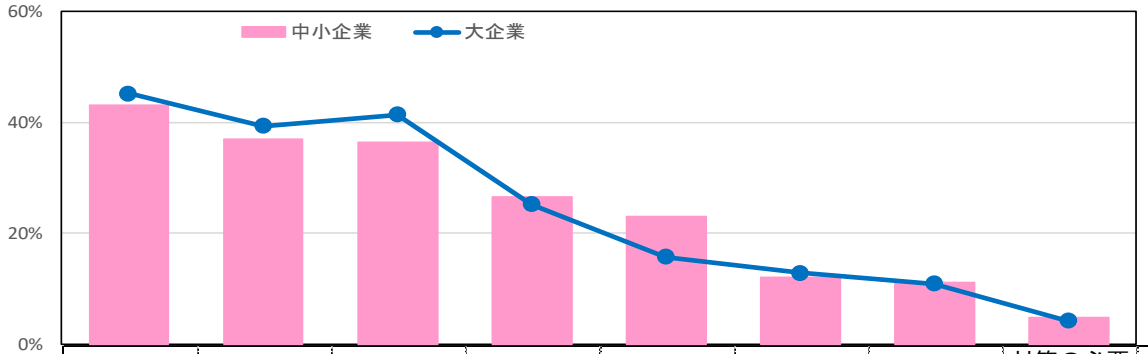
Ⅲ．集計結果（２）サイバーリスク意識・対策実態について

【問６.で『現在、サイバーリスク対策を行っていない』『わからない』以外を選択された企業のみ対象】

問７-２．サイバーリスク対策における貴社の課題について、当てはまるものをすべてお選びください。(MA)

■サイバーリスク対策における課題として、「現在行っている対策が十分なのか分からない」（43.8%）が最も多く、次に「対策をする人手が足りない」（38.1%）、「対策の効果測定が難しい」（37.8%）が多かった。

■「対策をする費用が足りない」は、大企業と比べて中小企業の方が比率が高くなっている（大企業15.7%、中小企業23.0%）。



		n=	現在行っている対策が十分なのか分からない	対策の効果測定が難しい	対策をする人手が足りない	社内や周囲に専門の人材がいない	対策をする費用が足りない	対策をする時間が足りない	特に課題はない	対策の必要性について社内の理解が得られず、十分な予算を獲得・確保できない	その他	わからない
全体		(1442)	43.8%	37.8%	38.1%	26.1%	20.5%	12.4%	11.1%	4.6%	0.6%	3.6%
業種別	01_製造業	(399)	46.6%	41.1%	42.1%	30.1%	23.1%	13.3%	9.0%	5.0%	0.5%	3.3%
	02_非製造業	(1043)	42.7%	36.5%	36.5%	24.6%	19.6%	12.1%	11.9%	4.4%	0.6%	3.7%
企業規模別	01大企業	(496)	45.2%	39.3%	41.3%	25.2%	15.7%	12.9%	10.9%	4.2%	0.4%	4.6%
	02中小企業	(946)	43.0%	37.0%	36.4%	26.6%	23.0%	12.2%	11.2%	4.8%	0.6%	3.1%
所在地別	01_都市部	(730)	41.9%	39.6%	41.4%	25.3%	21.2%	13.8%	11.5%	4.1%	0.4%	2.7%
	02_地方部	(712)	45.6%	36.0%	34.7%	27.0%	19.8%	11.0%	10.7%	5.1%	0.7%	4.5%
従業員数別	01_50人以下	(661)	42.4%	37.8%	33.0%	25.9%	21.9%	11.8%	12.0%	4.7%	0.6%	2.7%
	02_51～100人	(360)	45.0%	38.1%	41.7%	29.2%	21.7%	14.4%	10.3%	4.2%	0.8%	3.6%
	03_101～300人	(305)	43.9%	35.7%	44.3%	25.2%	17.4%	11.8%	11.1%	4.6%	0.3%	3.6%
	04_301～1,000人	(87)	49.4%	43.7%	40.2%	19.5%	16.1%	9.2%	6.9%	3.4%	0.0%	8.0%
	05_1,000人超	(29)	41.4%	37.9%	37.9%	24.1%	20.7%	17.2%	13.8%	10.3%	0.0%	10.3%

※複数回答の為、構成比の合計は100%にならない場合がございます。

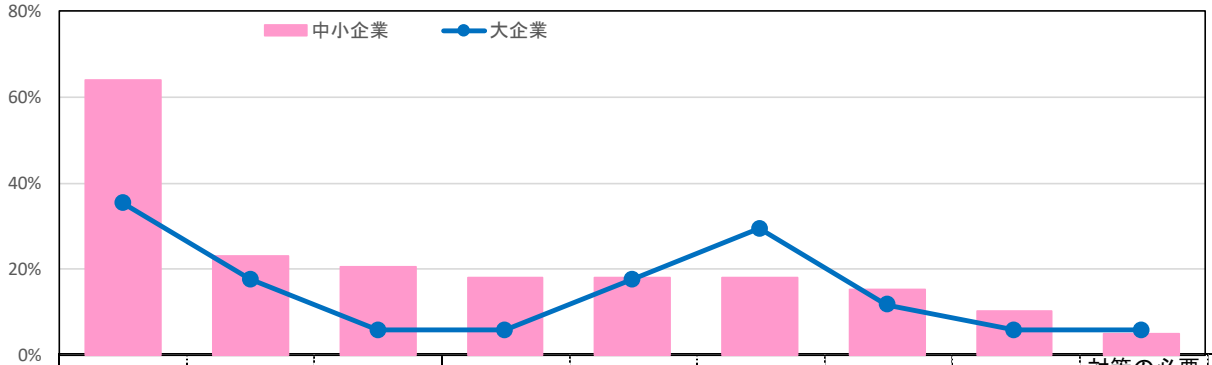
Ⅲ．集計結果（２）サイバーリスク意識・対策実態について

【問６.で『現在、サイバーリスク対策を行っていない』を選択された企業のみ対象】

問８． サイバーリスク対策を行っていない理由について、当てはまるものをすべてお選びください。(MA)

■対策を行っていない理由として、「サイバーリスクが発生する可能性は低いと考えているため」（55.4%）が最も多く、企業規模別に見ると、中小企業の方が比率が高くなっている（大企業35.3%、中小企業64.1%）。

■「対策をする人手に余裕がないため」、「サイバーリスクによって生じる影響・損失がわからないため」、「対策をする費用に余裕がないため」についても、企業規模別で差があり、それぞれ中小企業の方が比率が高くなっている。



		n=	サイバーリスクが発生する可能性は低いと考えているため	対策をする人手に余裕がないため	サイバーリスクによって生じる影響・損失が分からないため	対策をする費用に余裕がないため	他に優先順位の高い経営課題があるため	社内や周囲に専門の人材がいないため	具体的な対策方法がわからないため（相談先がわからない）	対策をする時間に余裕がないため	対策の必要性について社内の理解が得られず、予算を獲得・確保できない	その他	わからない
全体		(56)	55.4%	21.4%	16.1%	14.3%	17.9%	21.4%	14.3%	8.9%	5.4%	0.0%	8.9%
業種別	01_製造業	(12)	66.7%	16.7%	25.0%	16.7%	16.7%	8.3%	16.7%	8.3%	8.3%	0.0%	0.0%
	02_非製造業	(44)	52.3%	22.7%	13.6%	13.6%	18.2%	25.0%	13.6%	9.1%	4.5%	0.0%	11.4%
企業規模別	01大企業	(17)	35.3%	17.6%	5.9%	5.9%	17.6%	29.4%	11.8%	5.9%	5.9%	0.0%	5.9%
	02中小企業	(39)	64.1%	23.1%	20.5%	17.9%	17.9%	17.9%	15.4%	10.3%	5.1%	0.0%	10.3%
所在地別	01_都市部	(21)	47.6%	9.5%	4.8%	19.0%	19.0%	28.6%	4.8%	4.8%	4.8%	0.0%	4.8%
	02_地方部	(35)	60.0%	28.6%	22.9%	11.4%	17.1%	17.1%	20.0%	11.4%	5.7%	0.0%	11.4%
従業員数別	01_50人以下	(36)	55.6%	22.2%	13.9%	11.1%	11.1%	16.7%	11.1%	11.1%	0.0%	0.0%	11.1%
	02_51～100人	(12)	50.0%	25.0%	16.7%	8.3%	16.7%	33.3%	25.0%	0.0%	8.3%	0.0%	8.3%
	03_101～300人	(7)	57.1%	14.3%	14.3%	42.9%	57.1%	28.6%	14.3%	14.3%	28.6%	0.0%	0.0%
	04_301～1,000人	(1)	100.0%	0.0%	100.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
	05_1,000人超	(0)	－	－	－	－	－	－	－	－	－	－	－

※複数回答の為、構成比の合計は100%にならない場合がございます。

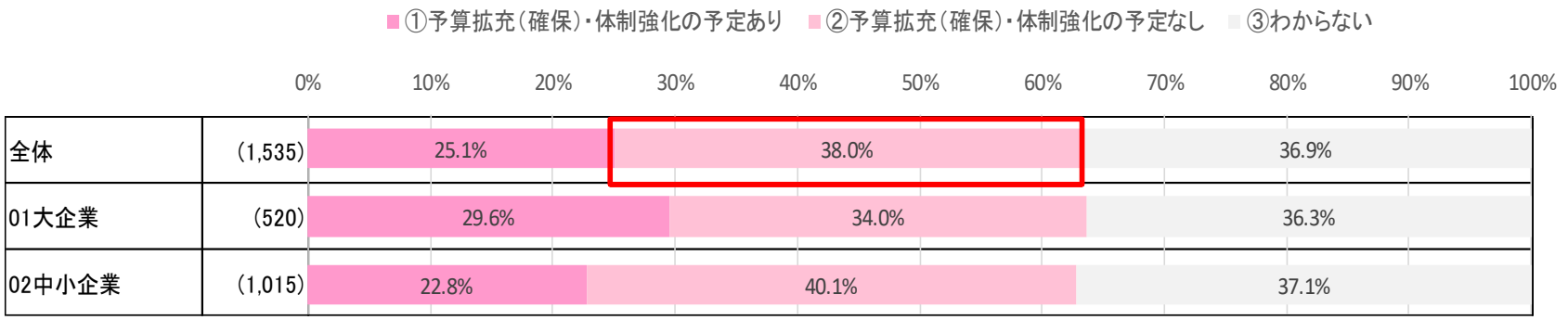
Ⅲ．集計結果（２）サイバーリスク意識・対策実態について

問９．今後、サイバーリスク対策への予算を拡充したり（現在対策を行っていない場合は予算の確保）、体制を強化したりする予定はありますか。(SA)

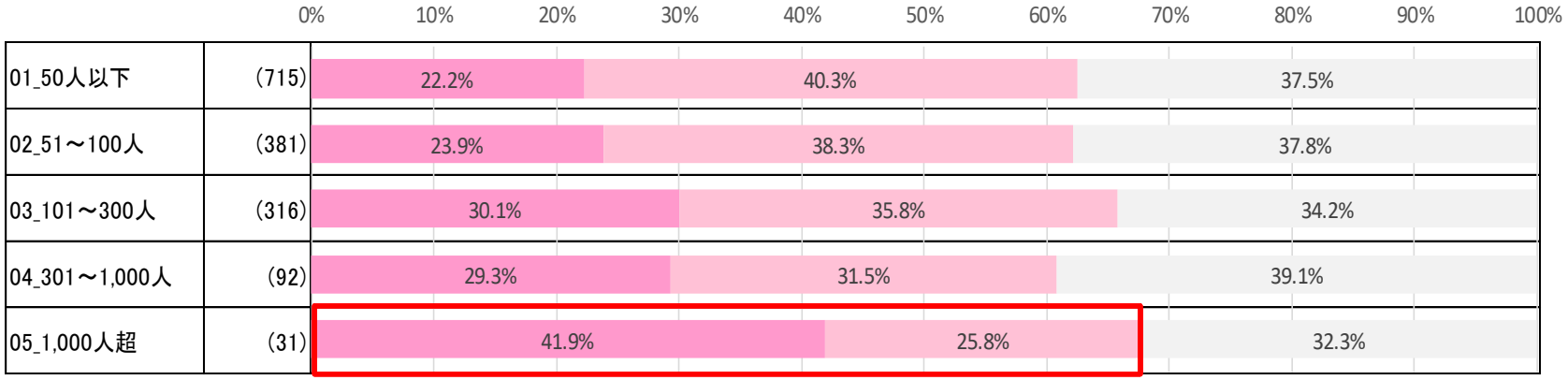
■サイバーリスク対策への予算拡充（確保）や体制強化の予定について、「予定なし」とする企業の方が多かった。

■一方、従業員数が多い企業ほど、予算拡充や体制強化の予定を立てている傾向があり、従業員数が1,000人超の企業では「予定あり」とする企業の方が多かった。

【企業規模別】

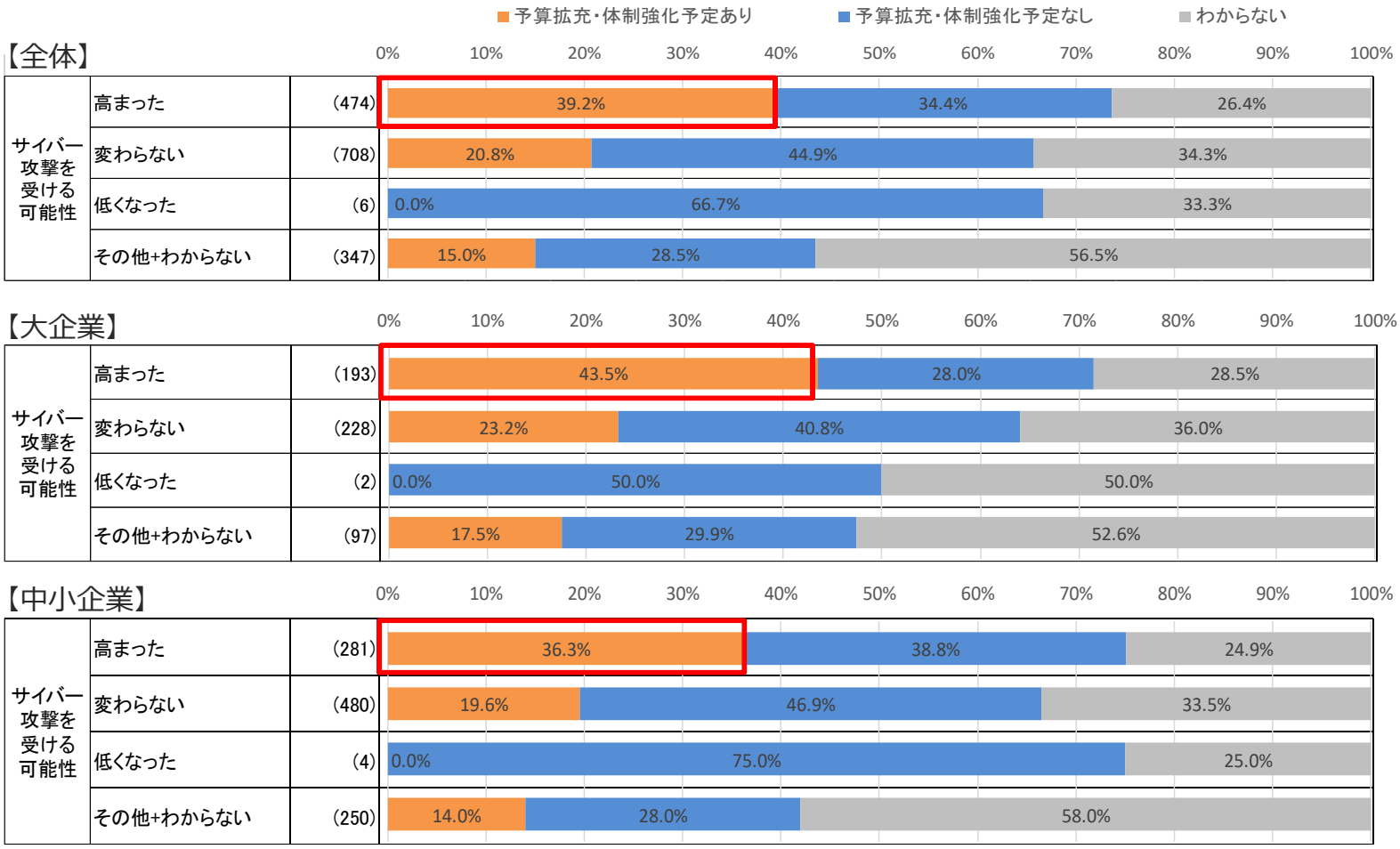


【従業員数別】



Ⅲ．集計結果（２）サイバーリスク意識・対策実態について
参考：サイバー攻撃を受ける可能性の認識（問5）×サイバーリスク対策の予算拡充・体制強化（問9）

■新型コロナウイルスの感染拡大以前と比べてサイバー攻撃を受ける可能性が「高まった」とし、且つ、予算拡充・体制強化の「予定あり」と回答した企業は39.2%であり、企業規模別に見ると、大企業の方が比率が高くなっている（大企業43.5%、中小企業36.3%）。

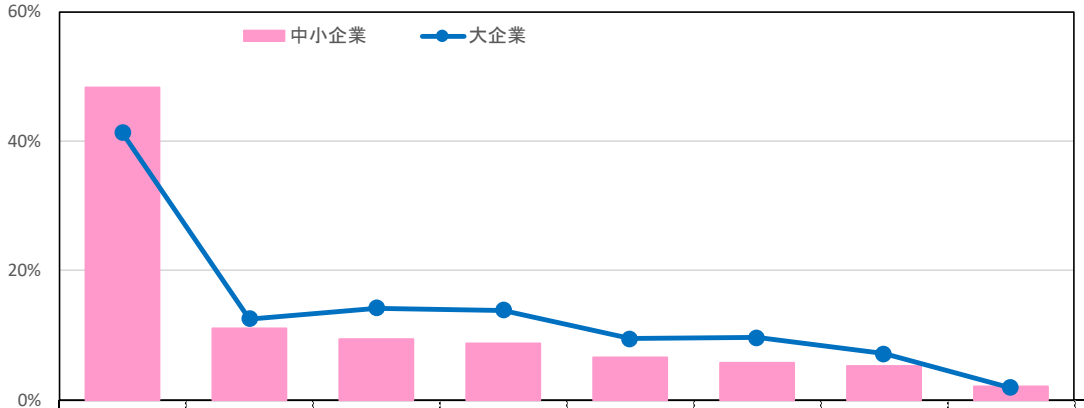


Ⅲ．集計結果（２）サイバーリスク意識･対策実態について

問10．取引先や委託先のサイバーリスク対策について、貴社の管理状況で当てはまるものをすべてお選びください。(MA)

■取引先等へのサイバーリスク対策の管理状況として、「何もしていない」（46.0%）が最も多く、従業員数別に見ると、従業員数が少ない企業ほど比率が高くなっている。

■「何らかのサイバーリスク対策の実施を取引要件にしている」は、従業員数が50人以下の企業では8.4%であったが、1,000人超の企業では25.8%であった。



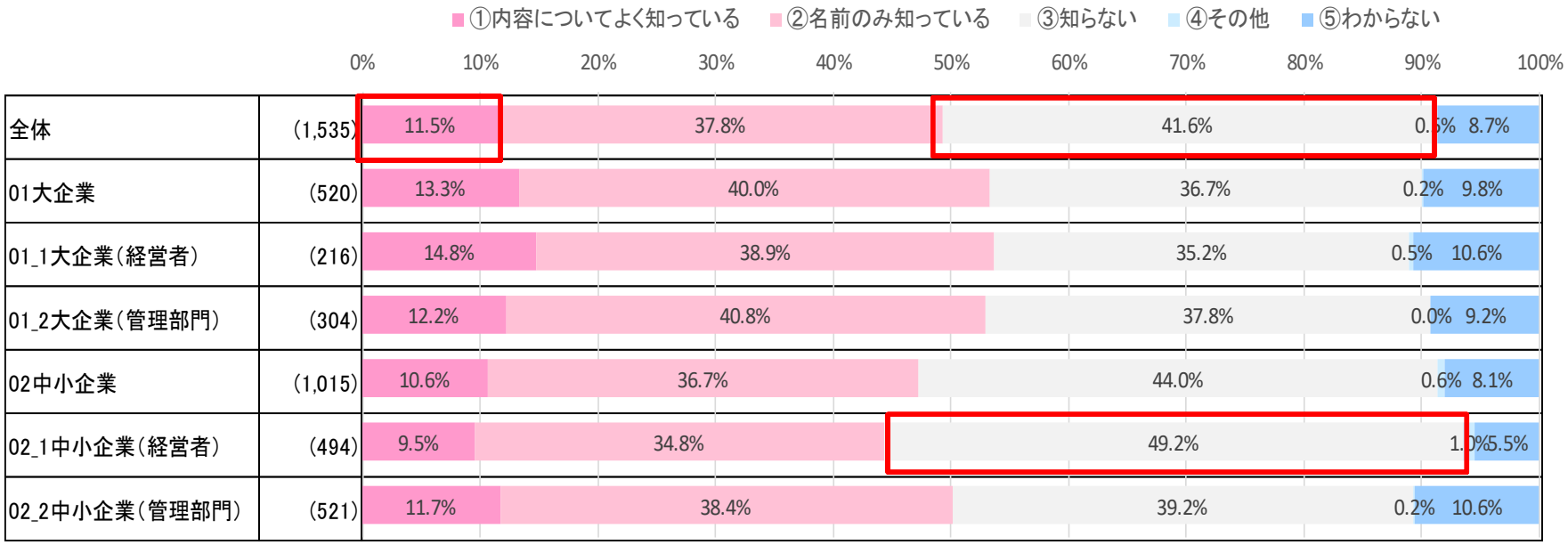
		n=	何もしていない	セキュリティ状況を常時監視している	サイバー被害の発生時に通知を求めている	何らかのサイバーリスク対策の実施を取引要件にしている	セキュリティ認証の取得を依頼または義務付けている	セキュリティ基準等について報告を求めている	サイバー被害に備えた復旧体制を確認している	損害保険の付保を求めている	その他	わからない
全体		(1535)	46.0%	11.6%	11.1%	10.4%	7.6%	7.1%	5.9%	2.1%	1.2%	16.0%
業種別	01_製造業	(428)	47.7%	11.0%	10.7%	10.7%	6.3%	7.0%	5.4%	2.1%	0.7%	17.8%
	02_非製造業	(1107)	45.3%	11.8%	11.2%	10.3%	8.0%	7.1%	6.1%	2.1%	1.4%	15.4%
企業規模別	01大企業	(520)	41.3%	12.5%	14.2%	13.8%	9.4%	9.6%	7.1%	1.9%	1.0%	15.2%
	02中小企業	(1015)	48.4%	11.1%	9.5%	8.7%	6.6%	5.8%	5.2%	2.2%	1.3%	16.5%
所在地別	01_都市部	(774)	43.5%	12.3%	13.4%	12.5%	8.1%	9.6%	6.1%	2.1%	0.9%	14.7%
	02_地方部	(761)	48.5%	10.9%	8.7%	8.3%	7.0%	4.6%	5.7%	2.1%	1.4%	17.3%
従業員数別	01_50人以下	(715)	52.2%	8.5%	10.3%	8.4%	6.0%	4.6%	5.6%	2.7%	1.0%	14.4%
	02_51～100人	(381)	44.4%	15.0%	11.3%	8.4%	7.9%	7.3%	5.2%	1.0%	1.0%	16.5%
	03_101～300人	(316)	41.5%	12.3%	11.7%	14.6%	10.1%	9.8%	6.6%	1.9%	2.2%	15.2%
	04_301～1,000人	(92)	30.4%	18.5%	12.0%	15.2%	9.8%	12.0%	7.6%	3.3%	0.0%	25.0%
	05_1,000人超	(31)	16.1%	12.9%	16.1%	25.8%	6.5%	19.4%	6.5%	0.0%	0.0%	29.0%

※複数回答の為、構成比の合計は100%にならない場合がございます。

Ⅲ．集計結果（３）サイバーリスク保険への加入状況について
問11．サイバーリスク保険についてどの程度知っていますか。(SA)

■サイバーリスク保険の認知度について、「内容についてよく知っている」はわずか11.5%であった。

■「名前のみ知っている」を含むと約半数の企業に認知されているが（49.3%）、4割超（41.6%）が「知らない」と回答しており、特に中小企業の経営者においてその比率が高くなっている（49.2%）。



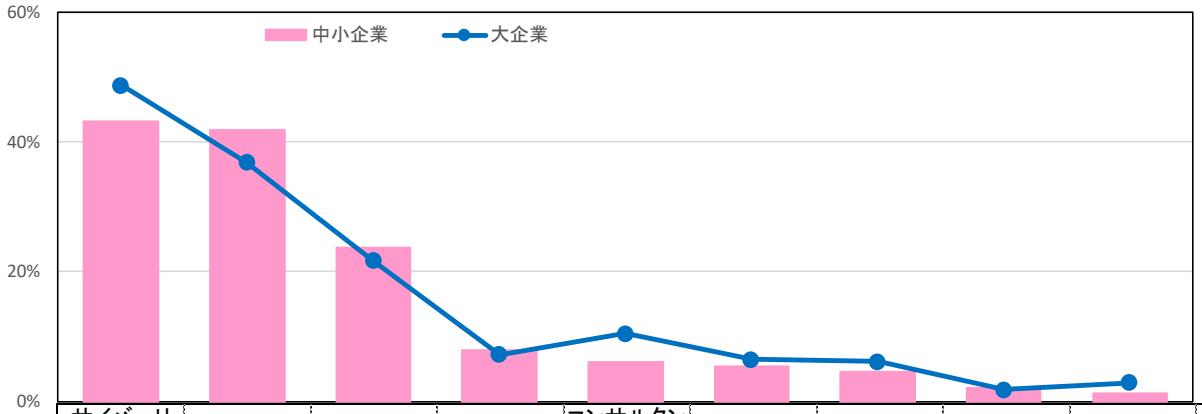
		①内容についてよく知っている	②名前のみ知っている	③知らない	④その他	⑤わからない
全体	(1,535)	11.5%	37.8%	41.6%	0.6%	8.7%
01大企業	(520)	13.3%	40.0%	36.7%	0.2%	9.8%
01_1大企業（経営者）	(216)	14.8%	38.9%	35.2%	0.5%	10.6%
01_2大企業（管理部門）	(304)	12.2%	40.8%	37.8%	0.0%	9.2%
02中小企業	(1,015)	10.6%	36.7%	44.0%	0.6%	8.1%
02_1中小企業（経営者）	(494)	9.5%	34.8%	49.2%	1.0%	5.5%
02_2中小企業（管理部門）	(521)	11.7%	38.4%	39.2%	0.2%	10.6%

Ⅲ．集計結果（３）サイバーリスク保険への加入状況について

【問11.で『内容についてよく知っている』『名前のみ知っている』を選択された企業のみ対象】

問12．サイバーリスク保険を知ったきっかけについて、当てはまるものをすべてお選びください。(MA)

■サイバーリスク保険を知ったきっかけとして、「サイバーリスクに関するニュースや記事で見た」（45.2%）、「保険会社や代理店からの紹介・提案があった」（40.0%）が多かった。



		n=	サイバーリスクに関するニュースや記事で見た	保険会社や代理店からの紹介・提案があった	WEBサイトで見た	セミナーやシンポジウム、勉強会で聞いた	コンサルタントや社外の専門家から説明があった	メールマガジンで見た	公的機関のガイドラインで見た	家族・知人から話を聞いた	SNSで見た	その他	わからない
全体		(757)	45.2%	40.0%	23.0%	7.7%	7.7%	5.8%	5.2%	2.0%	1.8%	1.5%	4.5%
業種別	01_製造業	(204)	43.1%	48.0%	20.1%	8.8%	7.8%	4.4%	5.4%	0.5%	2.0%	0.5%	4.4%
	02_非製造業	(553)	45.9%	37.1%	24.1%	7.2%	7.6%	6.3%	5.1%	2.5%	1.8%	1.8%	4.5%
企業規模別	01大企業	(277)	48.7%	36.8%	21.7%	7.2%	10.5%	6.5%	6.1%	1.8%	2.9%	1.4%	4.3%
	02中小企業	(480)	43.1%	41.9%	23.8%	7.9%	6.0%	5.4%	4.6%	2.1%	1.3%	1.5%	4.6%
所在地別	01_都市部	(405)	44.0%	39.3%	23.7%	7.2%	8.9%	6.4%	4.7%	1.2%	2.0%	1.7%	4.4%
	02_地方部	(352)	46.6%	40.9%	22.2%	8.2%	6.3%	5.1%	5.7%	2.8%	1.7%	1.1%	4.5%
従業員数別	01_50人以下	(334)	43.1%	37.7%	24.3%	8.7%	6.0%	5.4%	5.1%	2.7%	2.4%	2.1%	5.7%
	02_51～100人	(185)	50.8%	41.6%	22.7%	10.3%	8.6%	8.6%	4.9%	2.2%	2.2%	1.1%	3.2%
	03_101～300人	(177)	41.2%	43.5%	23.2%	4.5%	9.0%	5.1%	6.8%	0.6%	0.0%	0.6%	4.0%
	04_301～1,000人	(46)	50.0%	39.1%	19.6%	2.2%	10.9%	0.0%	2.2%	2.2%	0.0%	0.0%	4.3%
	05_1,000人超	(15)	53.3%	33.3%	6.7%	6.7%	6.7%	6.7%	0.0%	0.0%	13.3%	6.7%	0.0%

※複数回答の為、構成比の合計は100%にならない場合がございます。

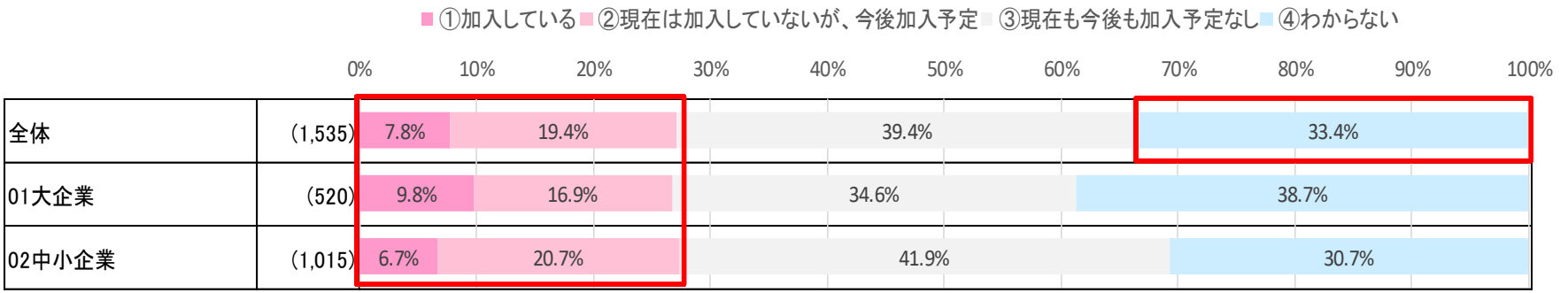
Ⅲ．集計結果（３）サイバーリスク保険への加入状況について
問13．貴社はサイバーリスク保険に加入していますか。(SA)

■サイバーリスク保険に「加入している」と回答した企業は、全体の7.8%であった。

■企業規模別に見ると、大企業は9.8%、中小企業は6.7%であり、中小企業の方が加入が進んでいない。

■一方、2割が「今後加入予定」とし、中小企業の方がその比率が高くなっている（大企業16.9%、中小企業20.7%）。

■自社のサイバーリスク保険の加入状況について、3割超（33.4%）が「わからない」としている。

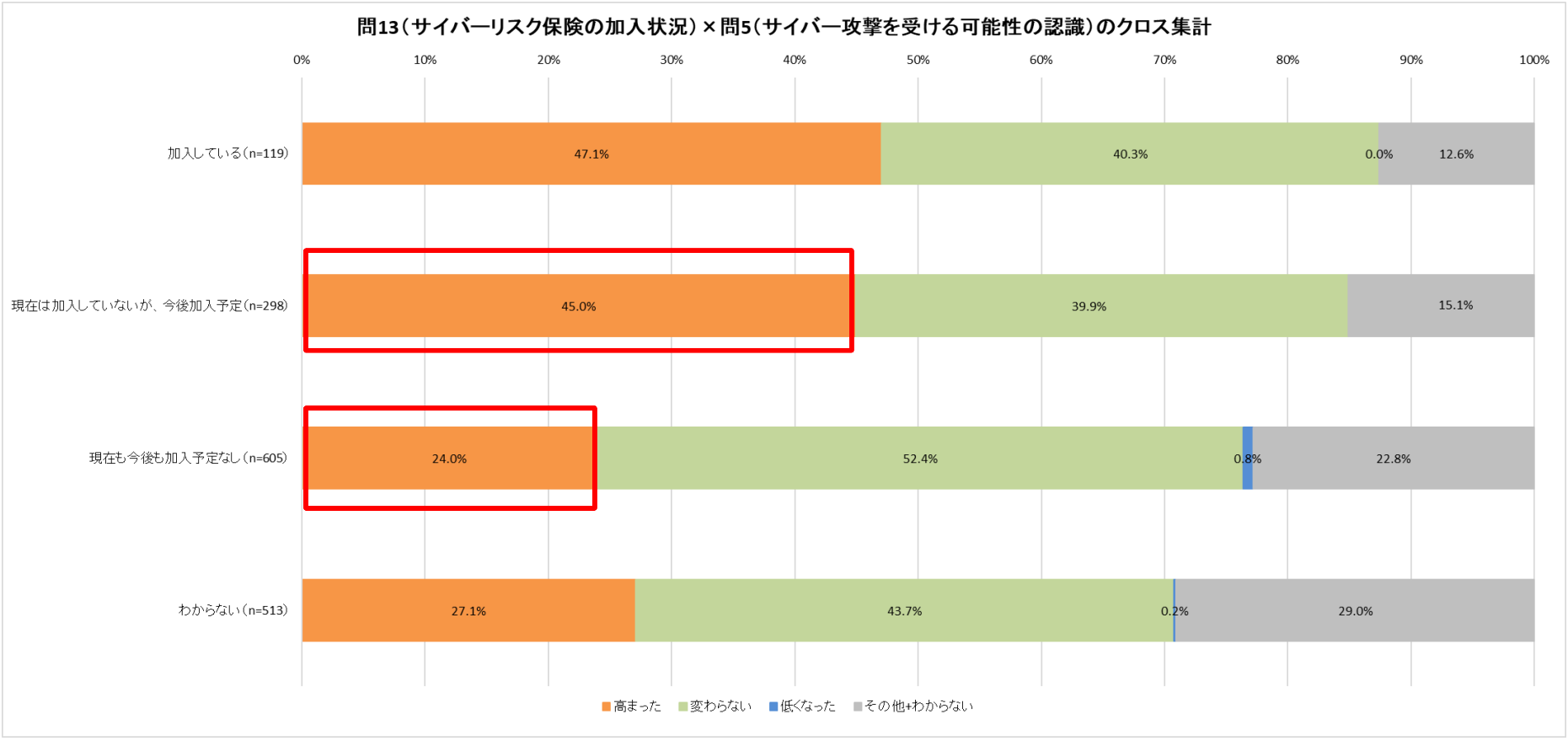


		①加入している	②現在は加入していないが、今後加入予定	③現在も今後も加入予定なし	④わからない
全体	(1,535)	7.8%	19.4%	39.4%	33.4%
01大企業	(520)	9.8%	16.9%	34.6%	38.7%
02中小企業	(1,015)	6.7%	20.7%	41.9%	30.7%

Ⅲ．集計結果（３）サイバーリスク保険への加入状況について
参考：サイバーリスク保険の加入状況（問13）×サイバー攻撃を受ける可能性の認識（問5）

■サイバーリスク保険に「今後加入予定」とした企業の半数が、新型コロナウイルスの感染拡大以前と比べてサイバー攻撃を受ける可能性が「高まった」と認識している（45.0%）。

■一方、サイバー攻撃を受ける可能性が「高まった」と認識しているにもかかわらず、24.0%がサイバーリスク保険に「現在も今後も加入予定なし」としている。



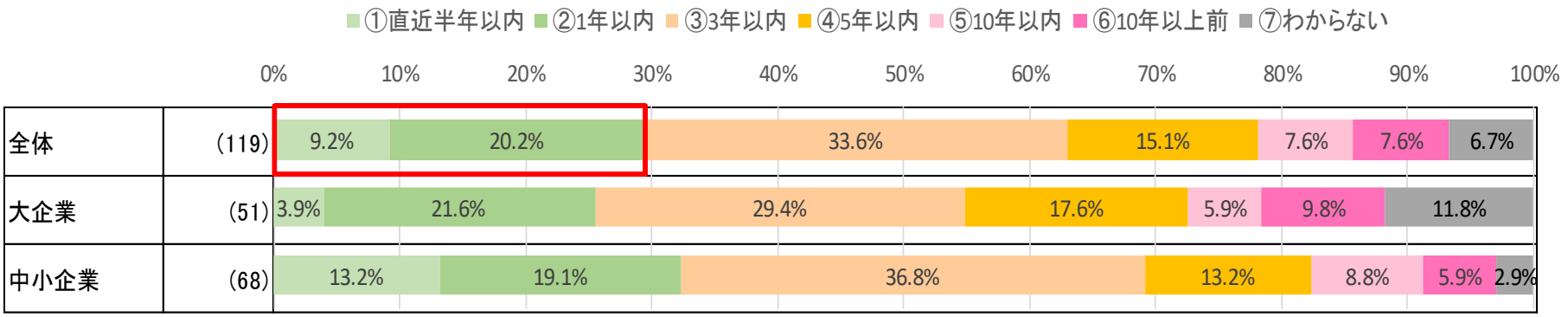
Ⅲ．集計結果（３）サイバーリスク保険への加入状況について

【問13.で『『加入している』を選択された企業のみ対象】

問14-1．サイバーリスク保険の加入時期について教えてください。(SA)

■サイバーリスク保険の加入時期について、3割（29.4%）が直近1年以内に加入している。

■企業規模別に見ると、中小企業の方が直近に加入している傾向がある。



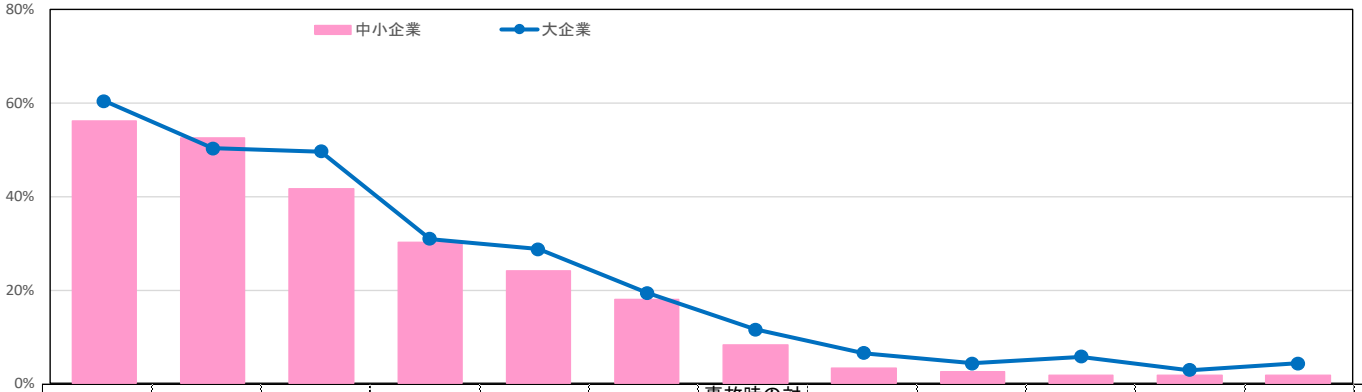
Ⅲ．集計結果（３）サイバーリスク保険への加入状況について

【問13.で『加入している』『現在は加入していないが、今後加入予定』を選択された企業のみ対象】

問14-2．サイバーリスク保険の加入(加入予定含む)理由について、当てはまるものをすべてお選びください。(MA)

■サイバーリスク保険の加入（加入予定含む）理由について、「会社の信用力向上につながるため」（57.6%）が最も多く、次に「完全にサイバー事故を防ぐことはできないため」（51.8%）が多かった。

■サイバーリスク保険に加入している企業では、「完全にサイバー事故を防ぐことはできないため」(51.3%）が最も多いが、加入を予定している企業では、「会社の信用力向上につながるため」（60.4%）が最も多かった。



		n=	会社の信用力向上につながるため	完全にサイバー事故を防ぐことはできないため	ネット上で情報管理する機会が増えてきたため	情報漏えいの事件やニュースを見聞きしたため	損害保険会社・損害保険代理店から提案されたため	いざという時の資金手当てをするため	事故時の対応について、保険会社の支援サービスを利用したいため	取引先や加盟団体から加入を推奨されたため	他社がサイバー被害を受けたことがあったため	親会社から加入を推奨されたため	実際にサイバー被害を受けたことがあるため	補償以外の付帯サービスに魅力を感じたため	その他	わからない
全体		(417)	57.6%	51.8%	44.4%	30.5%	25.7%	18.5%	9.4%	4.3%	3.1%	3.1%	2.2%	2.6%	1.2%	3.4%
業種別	01_製造業	(108)	64.8%	62.0%	45.4%	34.3%	19.4%	15.7%	13.9%	0.0%	3.7%	3.7%	0.9%	0.9%	0.0%	4.6%
	02_非製造業	(309)	55.0%	48.2%	44.0%	29.1%	27.8%	19.4%	7.8%	5.8%	2.9%	2.9%	2.6%	3.2%	1.6%	2.9%
企業規模別	01大企業	(139)	60.4%	50.4%	49.6%	30.9%	28.8%	19.4%	11.5%	6.5%	4.3%	5.8%	2.9%	4.3%	0.0%	1.4%
	02中小企業	(278)	56.1%	52.5%	41.7%	30.2%	24.1%	18.0%	8.3%	3.2%	2.5%	1.8%	1.8%	1.8%	1.8%	4.3%
所在地別	01_都市部	(216)	52.8%	52.8%	48.1%	28.7%	24.5%	19.9%	7.4%	5.6%	4.6%	3.2%	1.9%	1.9%	1.4%	1.9%
	02_地方部	(201)	62.7%	50.7%	40.3%	32.3%	26.9%	16.9%	11.4%	3.0%	1.5%	3.0%	2.5%	3.5%	1.0%	5.0%
従業員数別	01_50人以下	(193)	54.9%	52.8%	42.0%	32.1%	25.4%	18.7%	9.3%	4.7%	2.6%	1.6%	1.6%	2.1%	1.6%	3.1%
	02_51～100人	(97)	57.7%	51.5%	49.5%	28.9%	29.9%	16.5%	8.2%	5.2%	2.1%	3.1%	4.1%	4.1%	1.0%	2.1%
	03_101～300人	(95)	62.1%	49.5%	46.3%	26.3%	25.3%	21.1%	10.5%	4.2%	5.3%	4.2%	1.1%	3.2%	1.1%	5.3%
	04_301～1,000人	(23)	69.6%	60.9%	34.8%	34.8%	8.7%	13.0%	8.7%	0.0%	0.0%	4.3%	4.3%	0.0%	0.0%	0.0%
	05_1,000人超	(9)	33.3%	33.3%	44.4%	44.4%	33.3%	22.2%	11.1%	0.0%	11.1%	22.2%	0.0%	0.0%	0.0%	11.1%
サーバーリスク保険加入有無	加入している	(119)	50.4%	51.3%	36.1%	37.0%	46.2%	26.1%	15.1%	4.2%	4.2%	7.6%	3.4%	3.4%	2.5%	0.0%
	今後加入予定	(298)	60.4%	52.0%	47.7%	27.9%	17.4%	15.4%	7.0%	4.4%	2.7%	1.3%	1.7%	2.3%	0.7%	4.7%

※複数回答の為、構成比の合計は100%にならない場合がございます。

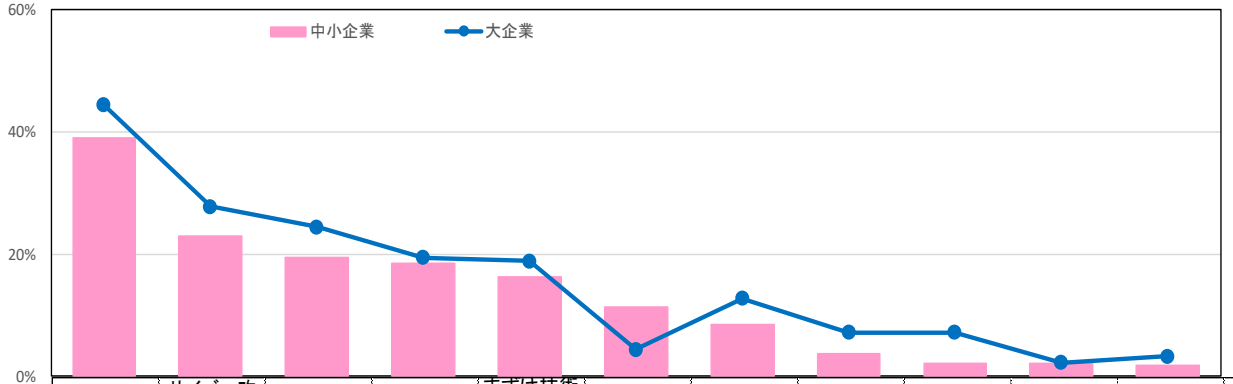
Ⅲ．集計結果（３）サイバーリスク保険への加入状況について

【問13.で『現在も今後も加入予定なし』を選択された企業のみ対象】

問15．サイバーリスク保険に加入しない理由について、当てはまるものをすべてお選びください。(MA)

■サイバーリスク保険に加入しない理由について、「保険の補償内容や保険料についてよく知らないため」（40.7%）が最も多く、次に「サイバー攻撃に伴う損害額(必要な補償額)がわからないため」（24.5%）、「サイバーセキュリティ対策の優先度が低いため」（21.0%）が多かった。

■2割（18.8%）が「サイバー被害を受ける可能性が低いため」としており、危機意識の低さもうかがえる。

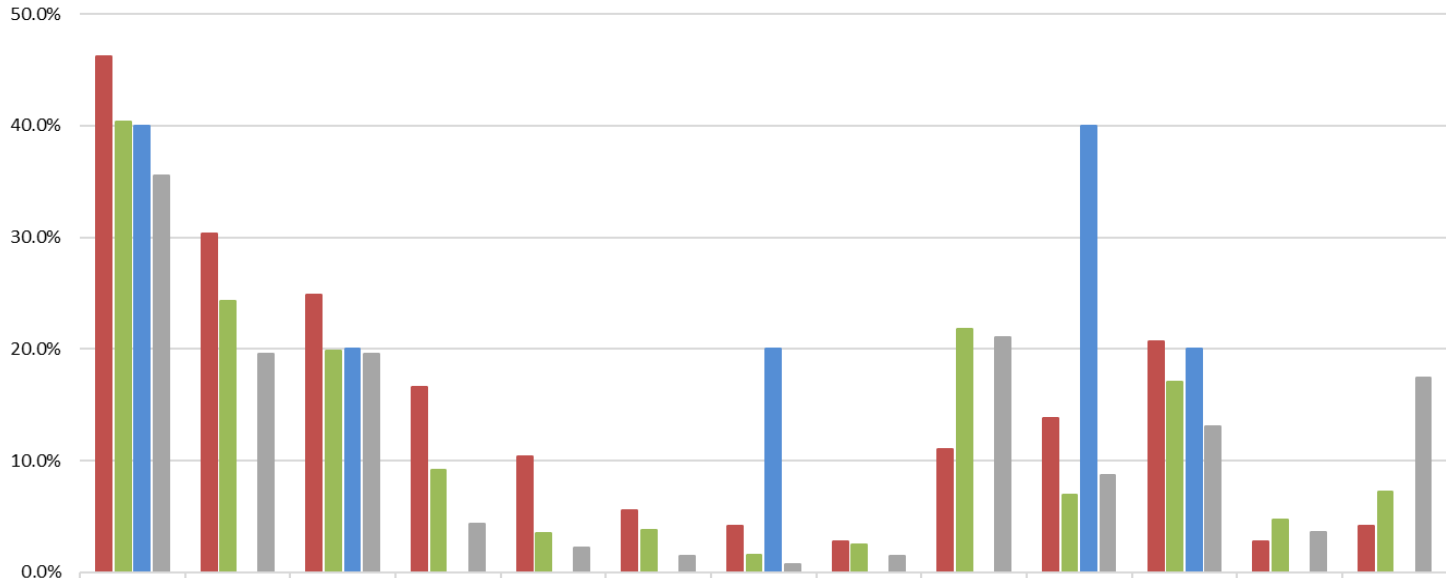


		n=	保険の補償内容や保険料についてよく知らないため	サイバー攻撃に伴う損害額(必要な補償額)がわからないため	サイバーセキュリティ対策の優先度が低いため	サイバー被害を受ける可能性が低いため	まずは技術的な対策を行ってから保険加入を検討したいため	資金に余裕がないため	保険料が高いため	実際に補償を受けられるか心配なため	補償額が十分でないため	加入にかかる手間が多いため	サイバー被害を受けても自己資金で対応できるため	その他	わからない
全体		(605)	40.7%	24.5%	21.0%	18.8%	17.0%	9.3%	9.8%	4.8%	3.6%	2.1%	2.3%	4.0%	8.8%
業種別	01_製造業	(167)	37.1%	29.3%	22.2%	19.2%	13.8%	10.8%	9.0%	4.8%	3.0%	3.6%	3.6%	3.0%	12.0%
	02_非製造業	(438)	42.0%	22.6%	20.5%	18.7%	18.3%	8.7%	10.0%	4.8%	3.9%	1.6%	1.8%	4.3%	7.5%
企業規模別	01大企業	(180)	44.4%	27.8%	24.4%	19.4%	18.9%	4.4%	12.8%	7.2%	7.2%	2.2%	3.3%	3.9%	4.4%
	02中小企業	(425)	39.1%	23.1%	19.5%	18.6%	16.2%	11.3%	8.5%	3.8%	2.1%	2.1%	1.9%	4.0%	10.6%
所在地別	01_都市部	(303)	39.3%	23.4%	20.1%	21.1%	17.2%	9.2%	11.9%	5.0%	4.3%	1.7%	2.6%	4.0%	7.3%
	02_地方部	(302)	42.1%	25.5%	21.9%	16.6%	16.9%	9.3%	7.6%	4.6%	3.0%	2.6%	2.0%	4.0%	10.3%
従業員数別	01_50人以下	(311)	39.5%	22.2%	20.3%	19.3%	16.4%	10.9%	7.1%	3.2%	2.9%	1.9%	2.3%	3.2%	9.6%
	02_51～100人	(150)	48.0%	26.0%	21.3%	17.3%	16.0%	10.0%	9.3%	6.0%	4.0%	1.3%	0.7%	5.3%	8.0%
	03_101～300人	(111)	32.4%	28.8%	21.6%	19.8%	19.8%	4.5%	13.5%	8.1%	4.5%	2.7%	4.5%	4.5%	9.9%
	04_301～1,000人	(30)	46.7%	26.7%	26.7%	16.7%	20.0%	6.7%	20.0%	3.3%	0.0%	6.7%	3.3%	3.3%	0.0%
	05_1,000人超	(3)	33.3%	0.0%	0.0%	33.3%	0.0%	0.0%	66.7%	0.0%	66.7%	0.0%	0.0%	0.0%	0.0%

※複数回答の為、構成比の合計は100%にならない場合がございます。

Ⅲ．集計結果（３）サイバーリスク保険への加入状況について
参考：サイバー攻撃を受ける可能性の認識（問5）×サイバーリスク保険に加入しない理由（問15）

■新型コロナウイルスの感染拡大以前よりサイバー攻撃を受ける可能性が「高まった」と認識しているが、サイバーリスク保険に現在も今後も加入する予定がない企業において、加入しない理由としては「保険の補償内容や保険料についてよく知らないため」（46.2%）が最も多く、次に「サイバー攻撃に伴う損害額（必要な補償額）がわからないため」（30.3%）が多かった。



	保険の補償内容や保険料についてよく知らないため	サイバー攻撃に伴う損害額(必要な補償額)がわからないため	サイバーセキュリティ対策の優先度が低いため	保険料が高いため	実際に補償を受けられるか心配なため	補償額が十分でないため	加入にかかる手間が多いため	サイバー被害を受けても自己資金で対応できるため	サイバー被害を受ける可能性が低いため	資金に余裕がないため	まずは技術的な対策を行ってから保険加入を検討したいため	その他	わからない
高まった（n=145）	46.2%	30.3%	24.8%	16.6%	10.3%	5.5%	4.1%	2.8%	11.0%	13.8%	20.7%	2.8%	4.1%
変わらない（n=317）	40.4%	24.3%	19.9%	9.1%	3.5%	3.8%	1.6%	2.5%	21.8%	6.9%	17.0%	4.7%	7.3%
低くなった（n=5）	40.0%	0.0%	20.0%	0.0%	0.0%	0.0%	20.0%	0.0%	0.0%	40.0%	20.0%	0.0%	0.0%
その他+わからない（n=138）	35.5%	19.6%	19.6%	4.3%	2.2%	1.4%	0.7%	1.4%	21.0%	8.7%	13.0%	3.6%	17.4%

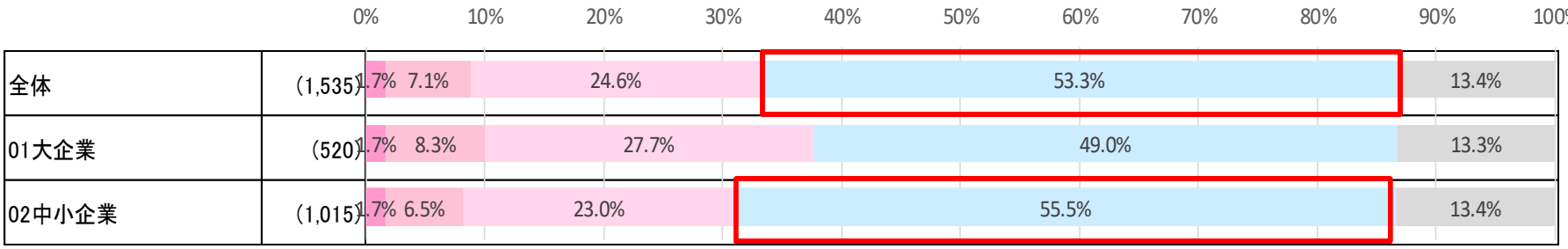
Ⅲ．集計結果（３）サイバーリスク保険への加入状況について

問16．サイバーリスク保険では、サイバー被害を受けた場合の補償だけでなく、保険会社に各種の相談ができる（付帯サービスがある※）ことを知っていますか。(SA)

※「情報セキュリティ診断サービス」、「専門事業者の紹介サービス」等。（保険会社によって異なります。）

■サイバーリスク保険の付帯サービスについて、半数（53.3%）が「知らなかった」としている。

■企業規模別に見ると、大企業と比べて、中小企業の方が認知度が低い（大企業49.0%、中小企業55.5%）。



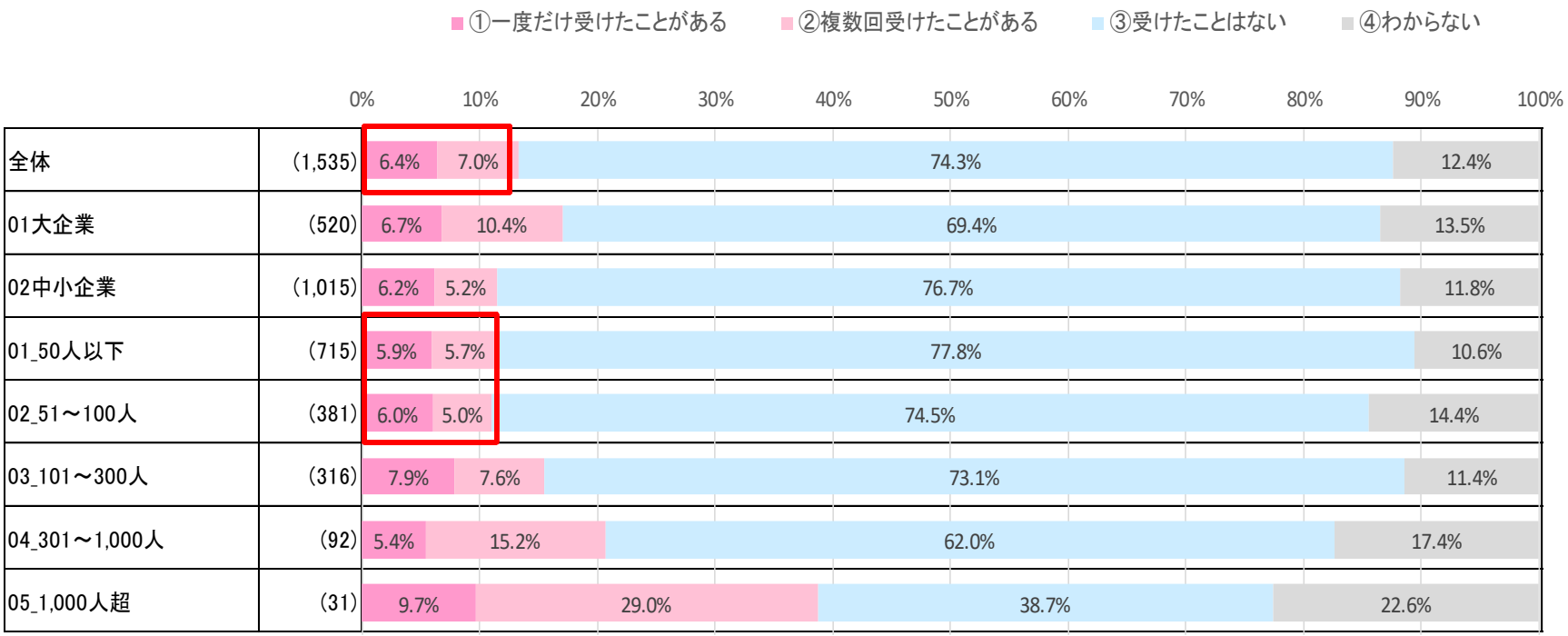
		①サービスを利用したことがあり、よく知っている	②サービスを利用したことはないが、よく知っている	③よく知らないが、聞いたことはある	④知らなかった	⑤わからない
全体	(1,535)	1.7%	7.1%	24.6%	53.3%	13.4%
01大企業	(520)	1.7%	8.3%	27.7%	49.0%	13.3%
02中小企業	(1,015)	1.7%	6.5%	23.0%	55.5%	13.4%

Ⅲ．集計結果（４）サイバーリスクによる被害状況について

問17．サイバー被害状況についてお伺いします。貴社ではこれまでにサイバー被害を受けたことはありますか。(SA)

■13.4%（205社）がこれまでにサイバー被害を受けたことがあるとしている。

■従業員数が多い企業ほどサイバー被害の経験があるが、規模が小さい企業でも、1割超がサイバー被害を経験している。



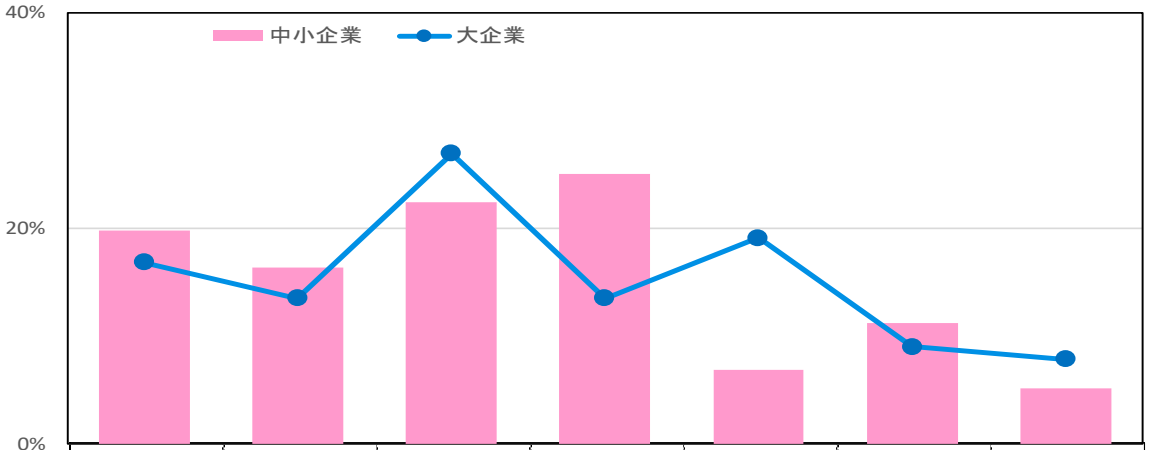
		①一度だけ受けたことがある	②複数回受けたことがある	③受けたことはない	④わからない
全体	(1,535)	6.4%	7.0%	74.3%	12.4%
01大企業	(520)	6.7%	10.4%	69.4%	13.5%
02中小企業	(1,015)	6.2%	5.2%	76.7%	11.8%
01_50人以下	(715)	5.9%	5.7%	77.8%	10.6%
02_51～100人	(381)	6.0%	5.0%	74.5%	14.4%
03_101～300人	(316)	7.9%	7.6%	73.1%	11.4%
04_301～1,000人	(92)	5.4%	15.2%	62.0%	17.4%
05_1,000人超	(31)	9.7%	29.0%	38.7%	22.6%

Ⅲ．集計結果（４）サイバーリスクによる被害状況について

【問17.で『一度だけ受けたことがある』『複数回受けたことがある』を選択された企業のみ対象】

問18-1．サイバー被害を受けた時期について、当てはまるものをすべてお選びください。(MA)

■サイバー被害を受けたことがある企業のうち、18.5%が「直近半年以内」に被害を受けたとしている。



		n=	直近半年以内	1年以内	3年以内	5年以内	10年以内	10年以上前	わからない
全体		(205)	18.5%	15.1%	24.4%	20.0%	12.2%	10.2%	6.3%
業種別	01_製造業	(66)	18.2%	12.1%	18.2%	21.2%	7.6%	13.6%	15.2%
	02_非製造業	(139)	18.7%	16.5%	27.3%	19.4%	14.4%	8.6%	2.2%
企業規模別	01大企業	(89)	16.9%	13.5%	27.0%	13.5%	19.1%	9.0%	7.9%
	02中小企業	(116)	19.8%	16.4%	22.4%	25.0%	6.9%	11.2%	5.2%
所在地別	01_都市部	(124)	18.5%	18.5%	25.0%	17.7%	13.7%	7.3%	6.5%
	02_地方部	(81)	18.5%	9.9%	23.5%	23.5%	9.9%	14.8%	6.2%
従業員数別	01_50人以下	(83)	15.7%	18.1%	26.5%	21.7%	10.8%	9.6%	2.4%
	02_51～100人	(42)	21.4%	7.1%	23.8%	21.4%	7.1%	16.7%	7.1%
	03_101～300人	(49)	18.4%	14.3%	22.4%	18.4%	16.3%	8.2%	10.2%
	04_301～1,000人	(19)	26.3%	15.8%	31.6%	21.1%	10.5%	5.3%	5.3%
	05_1,000人超	(12)	16.7%	25.0%	8.3%	8.3%	25.0%	8.3%	16.7%

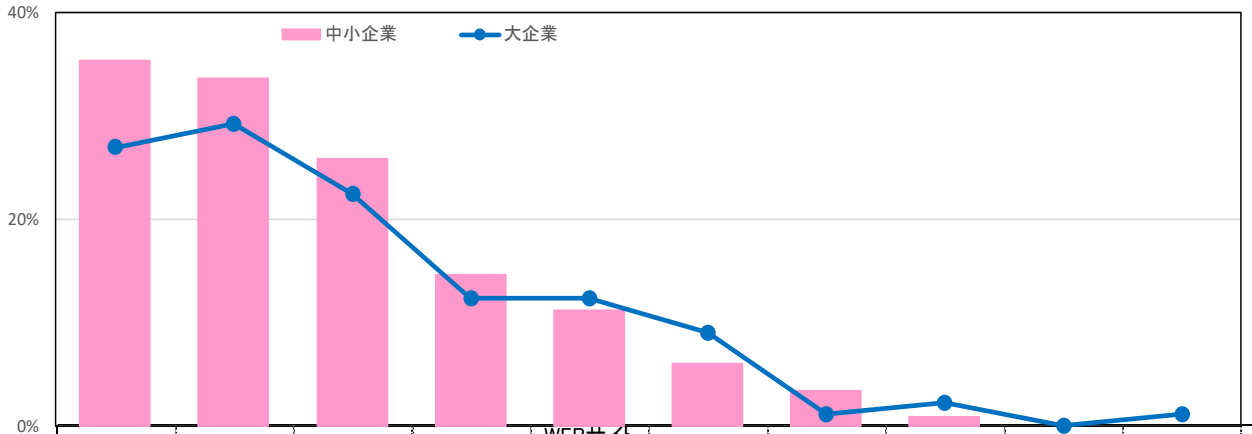
※複数回答の為、構成比の合計は100%にならない場合がございます。

Ⅲ．集計結果（４）サイバーリスクによる被害状況について

【問17.で『一度だけ受けたことがある』『複数回受けたことがある』を選択された企業のみ対象】

問18-2．サイバー被害を受けた際の攻撃の種類について、当てはまるものをすべてお選びください。(MA)

■サイバー被害を受けた際の攻撃の種類としては、「マルウェア」や「ランサムウェア」（いずれも31.7%）が最も多く、次に「不正送金を促すビジネスメール詐欺やフィッシングサイト」（24.4%）が多かった。



		n=	マルウェア	ランサムウェア	不正送金を促すビジネスメール詐欺やフィッシングサイト	標的型攻撃	WEBサイトへの不正ログイン・情報窃取およびWEBサイトの改ざん	DDoS(サービス妨害)攻撃	制御システムに対する攻撃	PWリスト攻撃	IoTデバイスに対する攻撃	ゼロデイ攻撃	その他	わからない
全体		(205)	31.7%	31.7%	24.4%	13.7%	11.7%	7.3%	2.4%	1.5%	0.0%	0.5%	4.9%	10.7%
業種別	01_製造業	(66)	28.8%	34.8%	33.3%	15.2%	15.2%	4.5%	3.0%	1.5%	0.0%	0.0%	3.0%	10.6%
	02_非製造業	(139)	33.1%	30.2%	20.1%	12.9%	10.1%	8.6%	2.2%	1.4%	0.0%	0.7%	5.8%	10.8%
企業規模別	01大企業	(89)	27.0%	29.2%	22.5%	12.4%	12.4%	9.0%	1.1%	2.2%	0.0%	1.1%	2.2%	14.6%
	02中小企業	(116)	35.3%	33.6%	25.9%	14.7%	11.2%	6.0%	3.4%	0.9%	0.0%	0.0%	6.9%	7.8%
所在地別	01_都市部	(124)	37.1%	30.6%	21.8%	15.3%	11.3%	8.1%	3.2%	1.6%	0.0%	0.8%	4.0%	11.3%
	02_地方部	(81)	23.5%	33.3%	28.4%	11.1%	12.3%	6.2%	1.2%	1.2%	0.0%	0.0%	6.2%	9.9%
従業員数別	01_50人以下	(83)	38.6%	25.3%	26.5%	9.6%	10.8%	8.4%	2.4%	2.4%	0.0%	0.0%	8.4%	10.8%
	02_51～100人	(42)	31.0%	42.9%	11.9%	16.7%	9.5%	7.1%	4.8%	0.0%	0.0%	0.0%	4.8%	11.9%
	03_101～300人	(49)	24.5%	30.6%	26.5%	14.3%	18.4%	6.1%	2.0%	0.0%	0.0%	2.0%	2.0%	10.2%
	04_301～1,000人	(19)	15.8%	57.9%	21.1%	21.1%	10.5%	5.3%	0.0%	0.0%	0.0%	0.0%	0.0%	10.5%
	05_1,000人超	(12)	41.7%	0.0%	50.0%	16.7%	0.0%	8.3%	0.0%	8.3%	0.0%	0.0%	0.0%	8.3%

※複数回答の為、構成比の合計は100%にならない場合がございます。

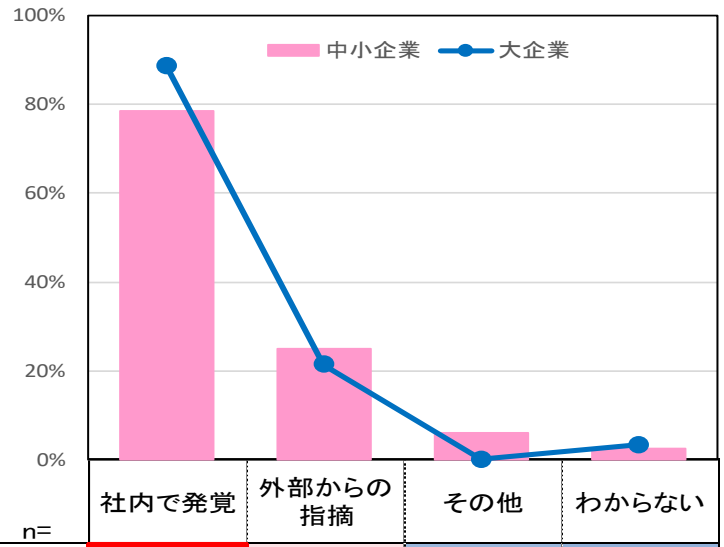
Ⅲ．集計結果（４）サイバーリスクによる被害状況について

【問17.で『一度だけ受けたことがある』『複数回受けたことがある』を選択された企業のみ対象】

問18-3．貴社においてサイバー被害を発見した要因について、当てはまるものをすべてお選びください。(MA)

■サイバー被害の発見要因としては、「社内で発覚」が8割を超えている（82.9%）。

■企業規模別に見ると、「社内で発覚」は大企業の比率が高いが、「外部からの指摘」は中小企業の比率が高くなっている。



		n=	社内で発覚	外部からの指摘	その他	わからない
全体		（205）	82.9%	23.4%	3.4%	2.9%
業種別	01_製造業	（66）	89.4%	19.7%	1.5%	3.0%
	02_非製造業	（139）	79.9%	25.2%	4.3%	2.9%
企業規模別	01大企業	（89）	88.8%	21.3%	0.0%	3.4%
	02中小企業	（116）	78.4%	25.0%	6.0%	2.6%
所在地別	01_都市部	（124）	82.3%	25.8%	2.4%	2.4%
	02_地方部	（81）	84.0%	19.8%	4.9%	3.7%
従業員数別	01_50人以下	（83）	73.5%	28.9%	8.4%	3.6%
	02_51～100人	（42）	92.9%	19.0%	0.0%	2.4%
	03_101～300人	（49）	89.8%	20.4%	0.0%	2.0%
	04_301～1,000人	（19）	78.9%	26.3%	0.0%	5.3%
	05_1,000人超	（12）	91.7%	8.3%	0.0%	0.0%

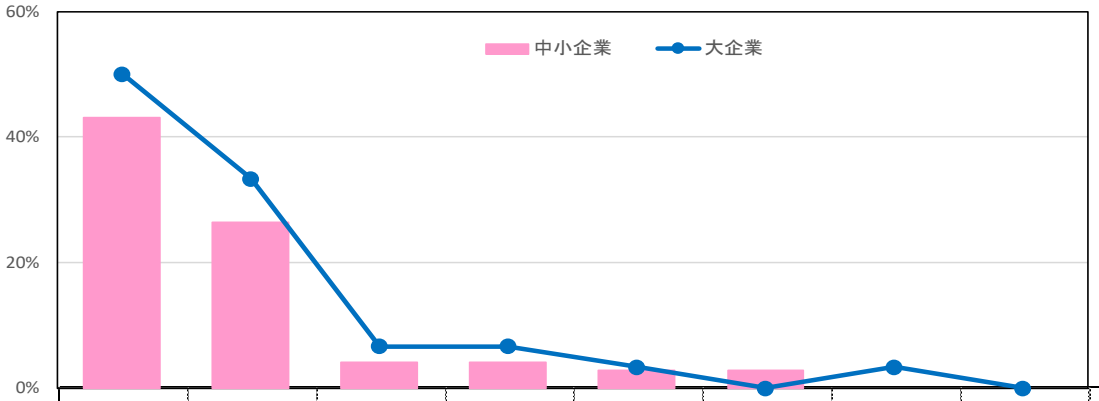
※複数回答の為、構成比の合計は100%にならない場合がございます。

Ⅲ．集計結果（４）サイバーリスクによる被害状況について

【問17.で『一度だけ受けたことがある』『複数回受けたことがある』を選択された企業のみ対象】

問18-4．サイバー被害によって生じた不利益について、当てはまるものをすべてお選びください。(MA)

■サイバー被害によって生じた不利益として、46.2%が「原因・影響調査や関係者対応等にかかる事故対応費用」としており、次に「業務関連システムやメールの停止による納期遅れ・営業機会損失」（29.5%）が多かった。



		n=	原因・影響調査や関係者対応等にかかる事故対応費用	業務関連システムやメールの停止による納期遅れ・営業機会損失	取引先・顧客からの損害賠償請求	顧客の流出	生産停止による売上減	（社内のモラル・士気低下が遠因となる）人材流出	得意先からの受注停止	従業員からの訴訟	その他
全体		（132）	46.2%	29.5%	5.3%	5.3%	3.0%	1.5%	1.5%	0.0%	31.8%
業種別	01_製造業	（41）	51.2%	29.3%	2.4%	4.9%	0.0%	0.0%	0.0%	0.0%	26.8%
	02_非製造業	（91）	44.0%	29.7%	6.6%	5.5%	4.4%	2.2%	2.2%	0.0%	34.1%
企業規模別	01大企業	（60）	50.0%	33.3%	6.7%	6.7%	3.3%	0.0%	3.3%	0.0%	25.0%
	02中小企業	（72）	43.1%	26.4%	4.2%	4.2%	2.8%	2.8%	0.0%	0.0%	37.5%
所在地別	01_都市部	（82）	50.0%	28.0%	7.3%	7.3%	3.7%	1.2%	2.4%	0.0%	30.5%
	02_地方部	（50）	40.0%	32.0%	2.0%	2.0%	2.0%	2.0%	0.0%	0.0%	34.0%
従業員数別	01_50人以下	（47）	34.0%	29.8%	6.4%	2.1%	2.1%	4.3%	2.1%	0.0%	42.6%
	02_51～100人	（29）	51.7%	37.9%	3.4%	6.9%	6.9%	0.0%	0.0%	0.0%	20.7%
	03_101～300人	（31）	51.6%	22.6%	6.5%	6.5%	0.0%	0.0%	3.2%	0.0%	35.5%
	04_301～1,000人	（17）	52.9%	17.6%	0.0%	11.8%	5.9%	0.0%	0.0%	0.0%	29.4%
	05_1,000人超	（8）	62.5%	50.0%	12.5%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%

※複数回答の為、構成比の合計は100%にならない場合がございます。

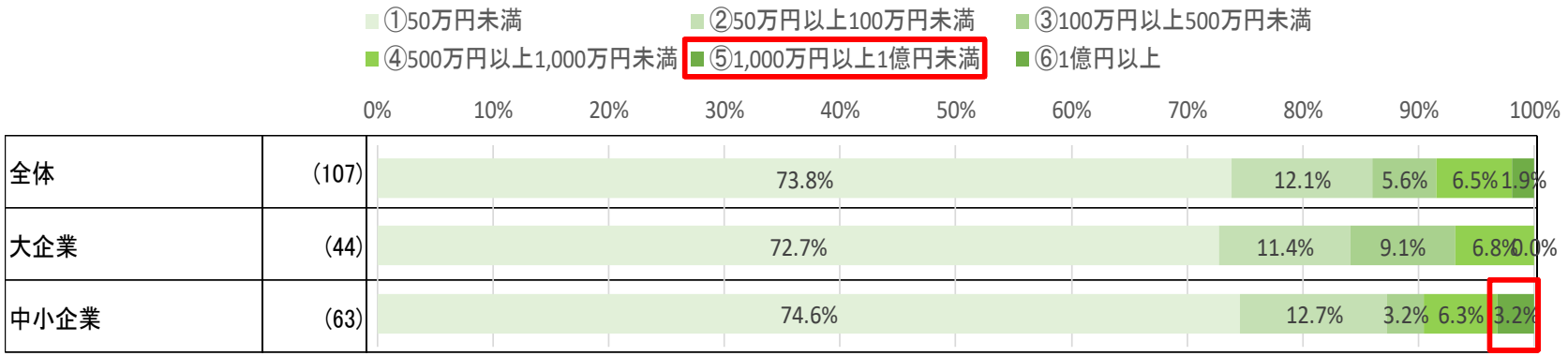
Ⅲ．集計結果（４）サイバーリスクによる被害状況について

【問17.で『一度だけ受けたことがある』『複数回受けたことがある』を選択された企業のみ対象】

問18-5．サイバー被害を受けた際の被害総額（複数回被害を受けたことがある場合は、もっとも被害が大きかったもの）について教えてください。(SA)

■サイバー被害を受けた際の被害総額は、大企業と中小企業でほとんど差はなかった。

■中小企業でも数千万円の高額被害が発生している（「1,000万円以上1億円未満」との回答あり）。



		①50万円未満	②50万円以上100万円未満	③100万円以上500万円未満	④500万円以上1,000万円未満	⑤1,000万円以上1億円未満	⑥1億円以上
全体	(107)	73.8%	12.1%	5.6%	6.5%	1.9%	
大企業	(44)	72.7%	11.4%	9.1%	6.8%	0.0%	
中小企業	(63)	74.6%	12.7%	3.2%	6.3%	3.2%	

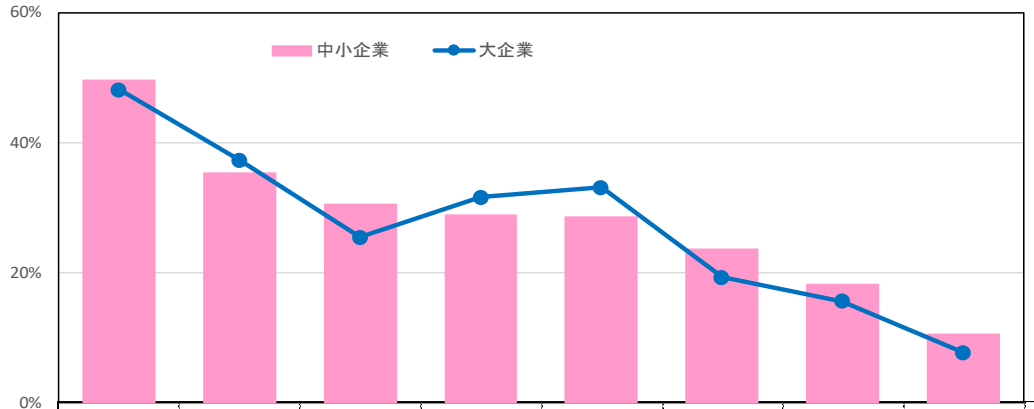
※「⑥1億円以上」は回答企業なし

Ⅲ．集計結果（４）サイバーリスクによる被害状況について

問19．サイバー被害を受けた直後の対応で苦労したこと(受けたことがない場合は、懸念すること)について、当てはまるものをすべてお選びください。(MA)

■サイバー被害を受けた直後の対応で苦労したこと（受けたことがない場合は、懸念すること）としては、「復旧対応」（49.1%）が最も多く、被害を受けたことがある企業では62.9%となっている。

■従業員別に見ると、1,000人超の企業では、「復旧対応」、「原因・影響範囲の特定」に次いで、「二次被害の防止」、「社内・社外への周知」の比率が高くなっている。



		n=	復旧対応	原因・影響範囲の特定	会社の信用力の回復	二次被害の防止	社内・社外への周知	謝罪対応	第三者からの損害賠償請求対応	対応資金の確保	その他	わからない
全体		(1535)	49.1%	36.0%	28.7%	29.7%	30.0%	22.1%	17.3%	9.6%	2.1%	36.6%
業種別	01_製造業	(428)	51.4%	38.8%	30.1%	29.7%	29.4%	22.9%	17.3%	9.3%	1.9%	35.5%
	02_非製造業	(1107)	48.1%	34.9%	28.2%	29.7%	30.3%	21.8%	17.3%	9.7%	2.3%	37.0%
企業規模別	01大企業	(520)	48.1%	37.3%	25.4%	31.5%	33.1%	19.2%	15.6%	7.7%	2.3%	36.0%
	02中小企業	(1015)	49.6%	35.3%	30.4%	28.8%	28.5%	23.5%	18.1%	10.5%	2.1%	36.9%
所在地別	01_都市部	(774)	51.4%	38.4%	29.2%	29.7%	31.8%	21.6%	16.3%	9.7%	1.4%	34.6%
	02_地方部	(761)	46.6%	33.5%	28.3%	29.7%	28.3%	22.6%	18.3%	9.5%	2.9%	38.6%
従業員数別	01_50人以下	(715)	46.7%	33.0%	28.8%	27.7%	28.0%	22.4%	17.2%	11.2%	2.0%	39.2%
	02_51～100人	(381)	52.0%	37.0%	28.1%	32.0%	27.8%	22.3%	17.8%	8.4%	2.4%	34.1%
	03_101～300人	(316)	52.5%	40.2%	30.4%	30.4%	35.1%	22.8%	18.7%	8.9%	1.9%	34.2%
	04_301～1,000人	(92)	41.3%	35.9%	27.2%	28.3%	32.6%	18.5%	12.0%	3.3%	4.3%	38.0%
	05_1,000人超	(31)	54.8%	48.4%	22.6%	45.2%	45.2%	16.1%	12.9%	12.9%	0.0%	29.0%
サイバー被害状況	受けたことがある	(205)	62.9%	58.5%	5.9%	20.0%	39.0%	7.8%	1.5%	3.4%	2.4%	10.7%
	受けたことはない	(1140)	49.9%	34.2%	34.8%	33.3%	30.8%	26.1%	21.2%	11.6%	2.5%	36.5%

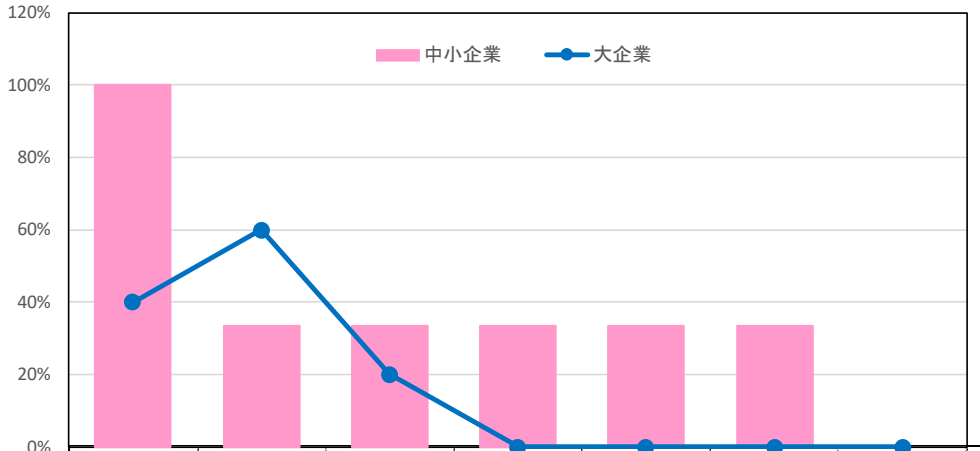
※複数回答の為、構成比の合計は100%にならない場合がございます。

Ⅲ．集計結果（４）サイバーリスクによる被害状況について

【問17.で『一度だけ受けたことがある』『複数回受けたことがある』を選択し、且つ、問13.で『加入している』を選択した企業のみ対象】

問20．サイバーリスク保険が活用できた場面について、当てはまるものをすべてお選びください。(MA)

■サイバー被害を受けたことがあり、且つ、サイバー保険に加入している企業では、主に「復旧作業」、「原因・影響調査」、「被害者への対応」の場面でサイバー保険を活用できたとの回答があった。



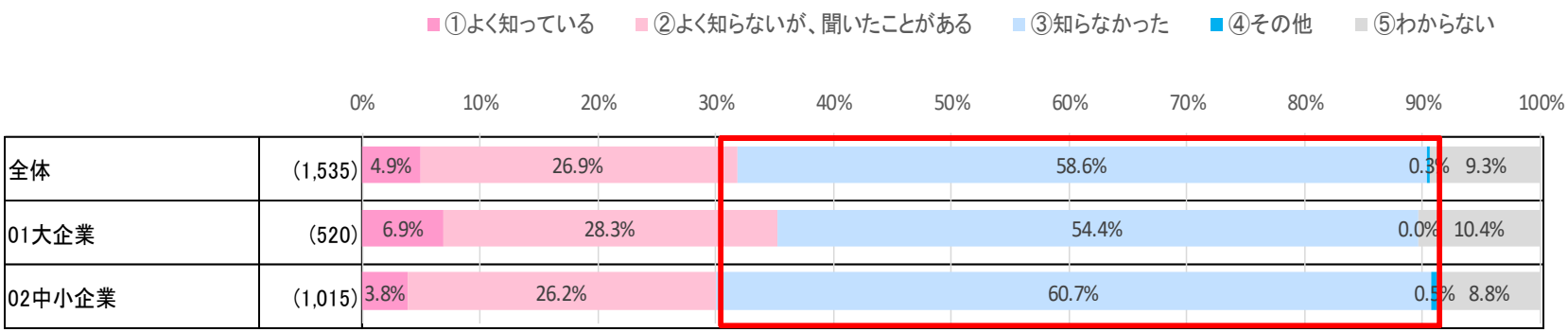
		n=	復旧作業	原因・影響調査	被害者への対応	専門家への委託・相談	損害賠償請求・争訟対応	再発防止策の策定	IT機器等の機能停止	その他
全体		(8)	62.5%	50.0%	25.0%	12.5%	12.5%	12.5%	0.0%	12.5%
業種別	01_製造業	(1)	0.0%	100.0%	100.0%	0.0%	0.0%	0.0%	0.0%	0.0%
	02_非製造業	(7)	71.4%	42.9%	14.3%	14.3%	14.3%	14.3%	0.0%	14.3%
企業規模別	01大企業	(5)	40.0%	60.0%	20.0%	0.0%	0.0%	0.0%	0.0%	20.0%
	02中小企業	(3)	100.0%	33.3%	33.3%	33.3%	33.3%	33.3%	0.0%	0.0%
所在地別	01_都市部	(8)	62.5%	50.0%	25.0%	12.5%	12.5%	12.5%	0.0%	12.5%
	02_地方部	(0)	－	－	－	－	－	－	－	－
従業員数別	01_50人以下	(3)	66.7%	0.0%	0.0%	33.3%	0.0%	0.0%	0.0%	33.3%
	02_51～100人	(1)	100.0%	100.0%	100.0%	0.0%	100.0%	100.0%	0.0%	0.0%
	03_101～300人	(2)	50.0%	100.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
	04_301～1,000人	(2)	50.0%	50.0%	50.0%	0.0%	0.0%	0.0%	0.0%	0.0%
	05_1,000人超	(0)	－	－	－	－	－	－	－	－

※複数回答の為、構成比の合計は100%にならない場合がございます。

Ⅲ．集計結果（５）その他

問21．2022年内にも、政府はサイバー攻撃(不正アクセス等)で個人情報が漏えいした企業に対し、被害が発生した全員への通知を義務付ける方針を知っていますか。(SA)

■2022年以降の個人情報漏えい時の被害者への通知義務について、半数以上（58.6%）が「知らなかった」としており、企業規模を問わず、多くの企業に認知されていない。



		①よく知っている	②よく知らないが、聞いたことがある	③知らなかった	④その他	⑤わからない
全体	(1,535)	4.9%	26.9%	58.6%	0.3%	9.3%
01大企業	(520)	6.9%	28.3%	54.4%	0.0%	10.4%
02中小企業	(1,015)	3.8%	26.2%	60.7%	0.5%	8.8%

＜補足＞

＊令和2年改正個人情報保護法について

令和2年6月12日に「個人情報の保護に関する法律等の一部を改正する法律」が公布されました。改正法の施行は、一部を除き公布後2年以内とされており、施行後、企業において個人情報の漏えい等が発生し個人の権利利益を害するおそれがある場合には、個人情報保護委員会への報告及び本人への通知が義務化されます。

今般の調査によると、上記の方針を知っている企業は31.8%にとどまっています。悪質な場合は社名も公表されるなど、企業に対する規制が強まることから、サイバー事故が発生した企業を包括的にサポートする「サイバー保険」の必要性がますます高まっていくと考えられます。

参考リンク：https://www.ppc.go.jp/files/pdf/200612_gaiyou.pdf

（「個人情報保護委員会HP「個人情報の保護に関する法律等の一部を改正する法律（概要）」）

Ⅲ．集計結果（５）その他
参考：個人情報漏えい時の通知義務に関する認知状況（問21）×サイバーリスク保険加入状況（問13）

■個人情報漏えい時の被害者への通知義務について、「よく知っている」と回答した企業では、サイバー保険に「加入している」、「今後加入予定」は合わせて48.0%となり、サイバー保険に対する意識の高さがうかがえる。

■一方、通知義務の方針について「知らなかった」と回答した企業では、サイバー保険に「加入予定なし」、「わからない」は合わせて77.7%となっている。