たんと繁盛

記者発表資料

令和元年（２０１９年）５月１０日

大阪経済記者クラブ会員各位

「サプライチェーンにおける取引先のサイバーセキュリティ対策等に関する調査」結果について

【お問合先】大阪商工会議所　経営情報センター（野田・中川）
ＴＥＬ：０６－６９４４－６３５３

調査概要

◆背　　景：オリパラ、万博など国際的に注目を集めるイベントを控え、サイバー攻撃の増加と巧妙化が予想される。サイバーセキュリティが手薄になりがちな中小企業に先ず侵入し、そこを“踏み台”にしてサプライチェーンを辿って大企業・中堅企業に至り、秘密情報・個人情報等を窃取する手口などが懸念されており、個社レベルで防御できる次元を超える場合もあるため、サプライチェーン全体で対策を講じていく必要性が高まっている。

◆調査目的：商取引の結節点に位置する大企業・中堅企業が、サプライチェーン上の取引先のサイバーセキュリティにつき、どの程度把握・関与しているか、取引先に由来してどの程度サイバー攻撃被害に遭っているか、今後、取引先に対しどのような要求事項を有しているか等を調査・公表することを通じて、サプライチェーン全体でのサイバーセキュリティに対する意識向上を図ること。

◆調査期間：平成３１年（２０１９年）２月～３月

◆調査方法：郵送、ＦＡＸ、メール、Ｗｅｂ、対面による依頼・回答

◆調査対象：全国の従業員１００人以上の企業

◆回 答 数：１１８社

【調査結果のポイント】

●**大企業・中堅企業の約７割（68%）**は、「仕入・外注・委託先（買い先）」「販売・受注・受託先（売り先）」におけるサイバーセキュリティやサイバー攻撃被害について**「あまり把握していない」**。また**56%**は、取引先のサイバーセキュリティへの**「関与・管理等」**につき**「何も（殆ど）せず」**と回答。

●「取引先に**今後求めていきたいこと**」は**「口頭や文書での注意喚起」（42%）、「契約締結の依頼／要件化」（34%）。「何も（殆ど）せず」の企業も約２割（19%）存在。**

●**「取引先がサイバー攻撃被害を受け、それが自社に及んだ経験」がある企業は４社に１社（25%）。**内容は、標的型メール(15 社)、詐欺的誘導メール(13 社)など。その結果、**「情報漏洩」(5 社)、システムダウン（3 社）、データ損壊（3 社）など実害も**出ている。

●「取引先がもしサイバー攻撃を受け、その**被害が自社にも及んだ場合、採り得る対処**」としては、**「口頭や文書での注意喚起」(51%)、「損害賠償請求」(47%)、「セキュリティソフト・ハード導入の依頼／要件化」(37%)、「取引停止」(29%)**など。

●**「中小企業は今後どうしていくべきか」**については、「**中小企業自身が自衛すべき」(60%)、「国や自治体が支援すべき」(45%)、「IT 企業や損保会社が安価・簡便なセキュリティサービスを提供すべき」(30%)、「商工会議所などが支援すべき」(27%)**など。

たんと繁盛

設問ごとのポイント

業種：

別紙のとおり、あらゆる業種を対象とした。
本調査の回答企業は、サービス業がやや少ないほかは、概ねわが国の業種別構成に近い。

従業員：

今回の調査対象は、中小企業基本法の定義する中小企業者および小規模企業者以外によって構成される一般的な意味での大企業ではなく、従業員 100 人以上の全国の法人企業（あらゆる業種）を便宜上、大企業・中堅企業と位置づけ、これらに該当する 118 社の回答企業を分析対象とした。

問１：直接的・間接的に継続取引のある系列企業･サプライチェーンの規模を教えて下さい

●「買い先」「売り先」ともに、1001 社以上で構成されるサプライチェーンがそれぞれ 30%以上を占め、調査対象の大企業・中堅企業が非常に大規模なサプライチェーンに属していることを示している。

問２：取引先のサイバーセキュリティ／攻撃の状況につき 「貴社の把握の現状」とその理由を教えて下さい

●回答のあった大企業・中堅企業の約７割（68%）は、取引先（「仕入・外注・委託先（買い先)」「販売・受注・受託先（売り先)」）におけるサイバーセキュリティやサイバー攻撃被害について「(担当者も）あまり把握していない」ことが分かった。

●その理由として一番多かったのは「把握手段や把握すべき事項が社内規定や第三者認証等により明確化されていない（分からない）ため」であった。

●「買い先」より「売り先」、「特注品・直接材の取引先」より「汎用品・間接材の取引先」の方が、若干、把握率が悪いが、有意差は見られなかった。

●システムや重要データの連携先については 54%が「概ね把握」しているものの、こうした重要取引先ですら 38%は「あまり把握していない」実態が明らかとなった。

問３：取引先が「Windows7/Windows Server2008」サポート終了の対応が出来ているかどうか把握していますか

●サイバーセキュリティの分野では重要度が高い「Windows7/Windows Server2008」のサポート終了（2020 年１月）については、63%が取引先での対応状況につき「把握自体できていない」ことが判明。一方「(取引先が）対応済みと（自社が）把握」は 4%にすぎなかった。

問４：取引先のサイバーセキュリティにつき 「貴社の関与・管理等の現状」 を教えて下さい

●回答のあった大企業・中堅企業の半数強（56%）は、取引先のサイバーセキュリティへの「関与・管理等」につき「何も（殆ど）していない」ことが分かった。
次いで「口頭や文書での注意喚起」(25%)、「契約締結の依頼／要件化」(20%)」と続き、「自社のセキュリティ基準や共通システムの採用・準拠の依頼／要件化」(13%)など具体的セキュリティ対策への「関与・管理」は比較的少数に留まっている。

●「その他」の自由記述の中には、「セキュリティという名目で安易に他社へ確認を求めることに疑問」という意見もみられた。

問５:取引先のサイバーセキュリティにつき「貴社が今後求めていきたいこと（取引要件等）」を教えて下さい

●「口頭や文書での注意喚起」(42%)、「契約締結の依頼／要件化」(34%)、「何も（殆ど）せず」(19%)などが上位を占めた傍らで、「セキュリティソフト・ハード導入の依頼／要件化」(15%)、「認証（ISMS 等）取得の依頼／要件化」(13%)、「損保付保の依頼／要件化」(4%）のような具体的セキュリティ対策を求める意向は少数に留まっている。

問６：取引先のサイバーセキュリティーにつき「貴社が今後求めていきたいが足かせとなる点」を教えて下さい

●自社に関係することとしては、「取引先に求めていく立場にない」(38%）や「取引先に求めていくことを控えるべき立場にある」(18%）など。

●相手先に関係することとしては、「取引先の IT 力が低い」(37%)、「取引先の意識が低い」(31%）など。

問７：取引先がサイバー攻撃被害を受け、それが貴社に及んだ経験がある場合（のみ） 「内容・被害」を教えて下さい

●回答のあった大企業・中堅企業の 25%（30 社）は「取引先がサイバー攻撃被害を受け、それが貴社に及んだ経験」があり、その内容として「標的型メールが届く」「詐欺的誘導メールが届く」「不正アクセスがある」など。

●その結果の被害の有無としては、上記「及んだ経験がある」企業のうち 80%（24 社）は「被害は（殆ど）及ばなかった」と回答。

●その傍らで、「情報漏洩」(5 社)、システムダウン（3 社)、データ損壊（3 社）などの被害を（取引先経由で）被っている企業もあった。

問８：取引先がもしサイバー攻撃被害を受け、その被害が貴社にも及んだ場合「貴社が採りうる対処」を教えて下さい

●51%の大企業・中堅企業が「口頭や文書での注意喚起」といった最低限の対処に留まった。

●一方で「損害賠償請求」（47%）、「セキュリティソフト・ハード導入の依頼／要件化」（37%）、「取引停止」（29%）などが上位に続くなど、比較的厳しめの対処を採る可能性も示されている。

問９：貴社の最重要サプライチェーンにおいてサイバーセキュリティーの協定・マニュアル等はありますか

●「サイバーセキュリティ専用のものがある」が 11%、「一般的な情報管理・危機管理に係るものなら有り、その中にサイバーセキュリティに関する記述が有る」が 25%であり、なんらかの形で規約化されている割合は 36%であった。

●協定・マニュアルの作成者は、54%がサプライチェーンの中の主導的企業、8%が業種・産業別団体であった。

問 10：中小企業のサイバーセキュリティーは今後どうしていくべきだと思いますか

●60%が「中小企業自身が自衛すべき」と回答。次いで「国や自治体が支援すべき」（45%）、「IT 企業や損保会社が安価・簡便なセキュリティサービスを提供すべき」（30%）、「商工会議所など支援機関が支援すべき」（27%）と続いている。

以上

令和元年（2019年）5月10日

サプライチェーンにおける取引先のサイバーセキュリティー対策等に関する調査　結果

大阪商工会議所　経営情報センター

◆実施者
大阪商工会議所

◆背　景
オリパラ、万博など国際的に注目を集めるイベントを控え、サイバー攻撃の増加と巧妙化が予想される。サイバーセキュリティが手薄になりがちな中小企業に先ず侵入し、そこを“踏み台”にしてサプライチェーンを辿って大企業・中堅企業に至り、秘密情報・個人情報等を窃取する手口などが懸念されており、個社レベルで防御できる次元を超える場合もあるため、サプライチェーン全体で対策を講じていく必要性が高まっている。

◆調査目的
商取引の結節点に位置する大企業・中堅企業が、サプライチェーン上の取引先のサイバーセキュリティにつき、どの程度把握・関与しているか、取引先に由来してどの程度サイバー攻撃被害に遭っているか、今後、取引先に対しどのような要求事項を有しているか等を調査・公表することを通じて、サプライチェーン全体でのサイバーセキュリティに対する意識向上を図ること。

◆調査期間
平成31年（2019年）2月～3月

◆調査方法
郵送、FAX、メール、Web、対面による依頼・回答

◆調査対象
全国の従業員100人以上の企業

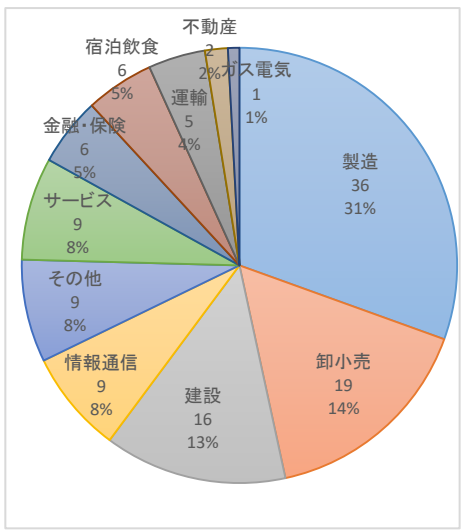
◆回 答 数
118社

※協力：一般財団法人関西情報センター

総回答社数（従業員数100人以上の中堅企業・大企業）	118

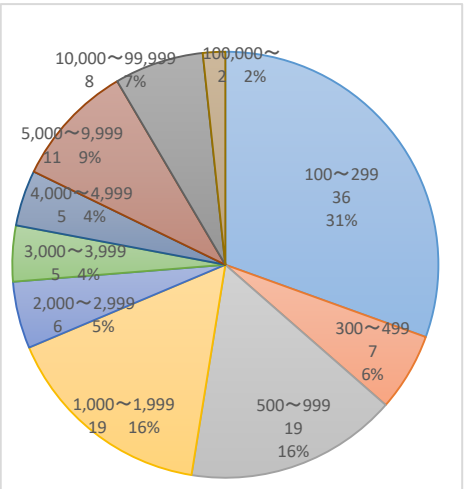
＜業種＞

製造	36	31%
卸小売	19	16%
建設	16	14%
情報通信	9	8%
その他	9	8%
サービス	9	8%
金融・保険	6	5%
宿泊飲食	6	5%
運輸	5	4%
不動産	2	2%
ガス電気	1	1%
	118	100%



＜従業員数＞

100～299	36	31%
300～499	7	6%
500～999	19	16%
1,000～1,999	19	16%
2,000～2,999	6	5%
3,000～3,999	5	4%
4,000～4,999	5	4%
5,000～9,999	11	9%
10,000～99,999	8	7%
100,000～	2	2%
	118	100%

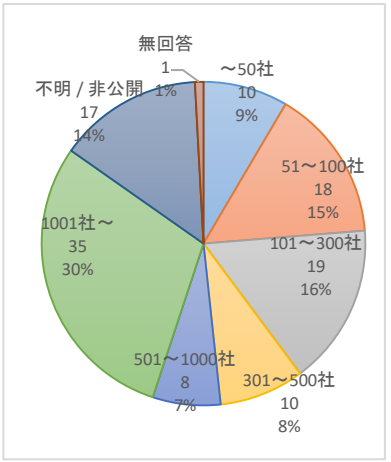


中小企業基本法で定義される中小企業者・小規模企業者以外（卸、サービスは100人超、小売は50人超、それ以外300人超）は、一般的に「大企業」と呼称されるが、本調査では、従業員数100人以上の法人を便宜上、大企業・中堅企業と分類し、調査・分析対象とした。

＜問1＞直接的・間接的に継続取引のある系列企業・サプライチェエーンの規模 【単数回答】

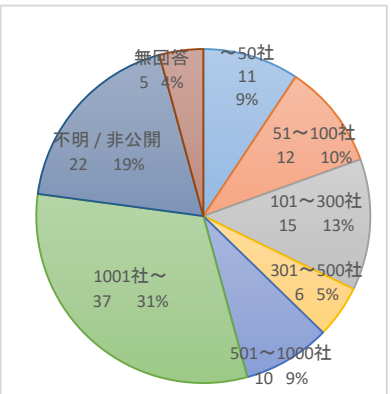
1-1：仕入・外注・委託先(買い先)

～50社	10	8%
51～100社	18	15%
101～300社	19	16%
301～500社	10	8%
501～1000社	8	7%
1001社～	35	30%
不明 / 非公開	17	14%
無回答	1	1%
	118	100%



1-2：販売・受注・受託先(売り先)

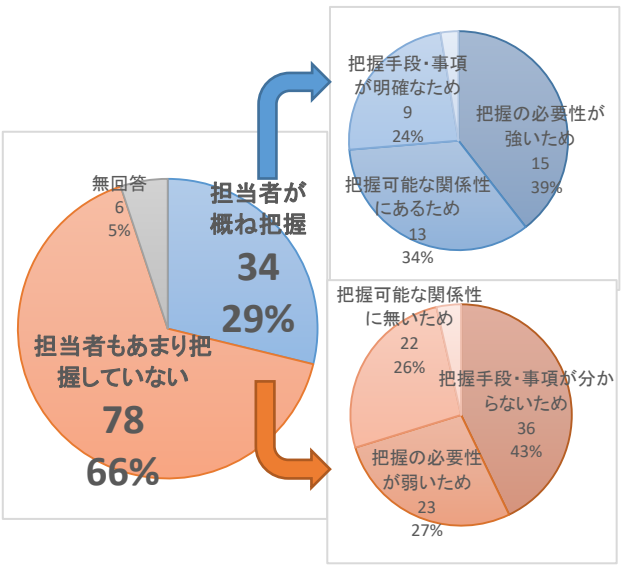
～50社	11	9%
51～100社	12	10%
101～300社	15	13%
301～500社	6	5%
501～1000社	10	8%
1001社～	37	31%
不明 / 非公開	22	19%
無回答	5	4%
	118	100%



＜問2＞取引先のサイバーセキュリティー／攻撃の状況につき「貴社の把握の現状」【単数回答】とその理由【複数回答】を教えて下さい

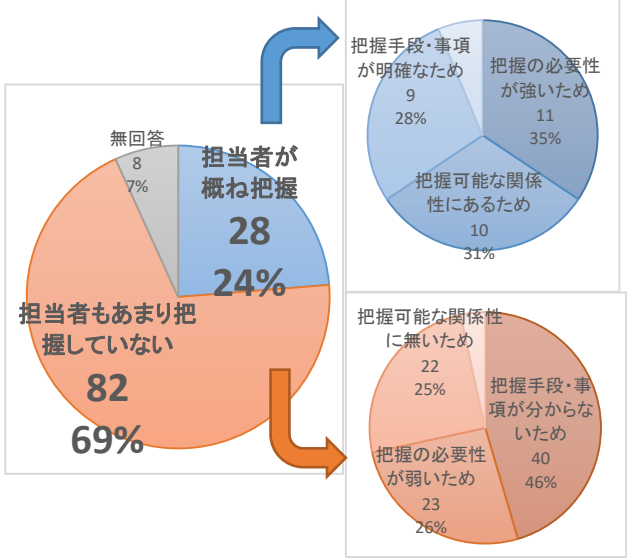
①-A：仕入・外注・委託先（買い先）

現状	**担当者が概ね把握**	**34**	**29%**
理由	把握するべき必要性が有る（強い）ため	15	39%
理由	把握可能な（教えてもらえる）関係性に有るため（信頼関係・上下関係等）	13	34%
理由	把握手段や把握すべき事項が社内規定や第三者認証等により明確化されているため	9	24%
理由	その他 （ ・把握が必要な場合は個別対応）	1	3%
現状	**担当者もあまり把握していない**	**78**	**66%**
理由	把握手段や把握すべき事項が社内規定や第三者認証等により 明確化されていない（分からない）ため	36	43%
理由	把握するべき必要性が 無い（弱い）ため	23	27%
理由	把握可能な（教えてもらえる）関係性に無いため（信頼関係・上下関係等）	22	26%
理由	その他（ ・対象数が多いため ・取引先数が多く全体の把握が困難なため ）	3	4%
現状	**無回答**	**6**	**5%**
		118	100%



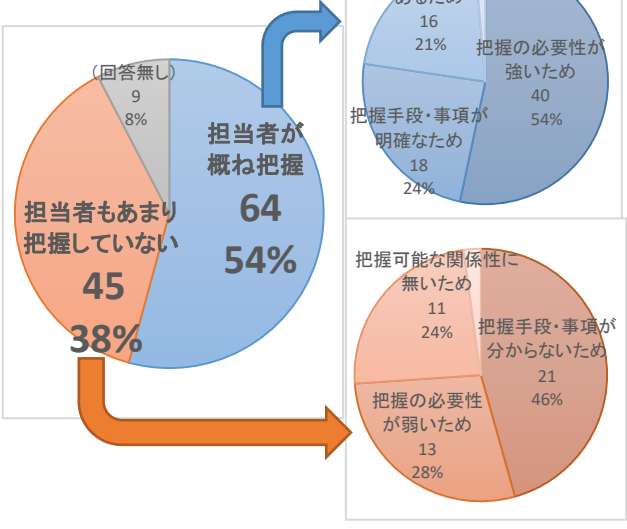
①-B：販売・受注・受託先（売り先）

現状	**担当者が概ね把握**	**28**	**24%**
理由	把握するべき必要性が有る（強い）ため	11	34%
理由	把握可能な（教えてもらえる）関係性に有るため（信頼関係・上下関係等）	10	31%
理由	把握手段や把握すべき事項が社内規定や第三者認証等により明確化されているため	9	28%
理由	その他 （ ・把握が必要な場合は個別対応）	2	6%
現状	**担当者もあまり把握していない**	**82**	**69%**
理由	把握手段や把握すべき事項が社内規定や第三者認証等により 明確化されていない（分からない）ため	40	45%
理由	把握するべき必要性が 無い（弱い）ため	23	26%
理由	把握可能な（教えてもらえる）関係性に無いため（信頼関係・上下関係等）	22	25%
理由	その他（ ・対象数が多いため ）	3	3%
現状	**無回答**	**8**	**7%**
		118	100%



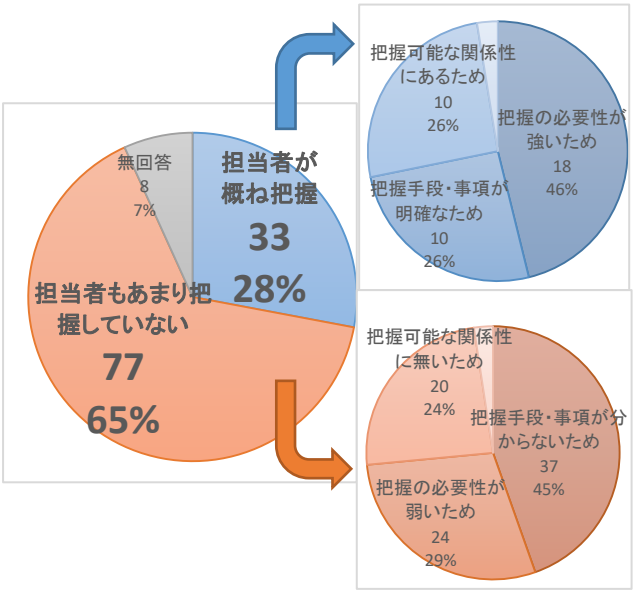
②-A：システムや重要データの連携先

現状	**担当者が概ね把握**	**64**	**54%**
理由	把握するべき必要性が有る（強い）ため	40	53%
理由	把握手段や把握すべき事項が社内規定や第三者認証等により明確化されているため	18	24%
理由	把握可能な（教えてもらえる）関係性に有るため（信頼関係・上下関係等）	16	21%
理由	その他 （ ・把握が必要な場合は個別対応）	1	1%
現状	**担当者もあまり把握していない**	**45**	**38%**
理由	把握手段や把握すべき事項が社内規定や第三者認証等により 明確化されていない（分からない）ため	21	46%
理由	把握するべき必要性が 無い（弱い）ため	13	28%
理由	把握可能な（教えてもらえる）関係性に無いため（信頼関係・上下関係等）	11	24%
理由	その他	1	2%
現状	**（回答無し）**	**9**	**8%**
※（回答無し）含む		**118**	**100%**



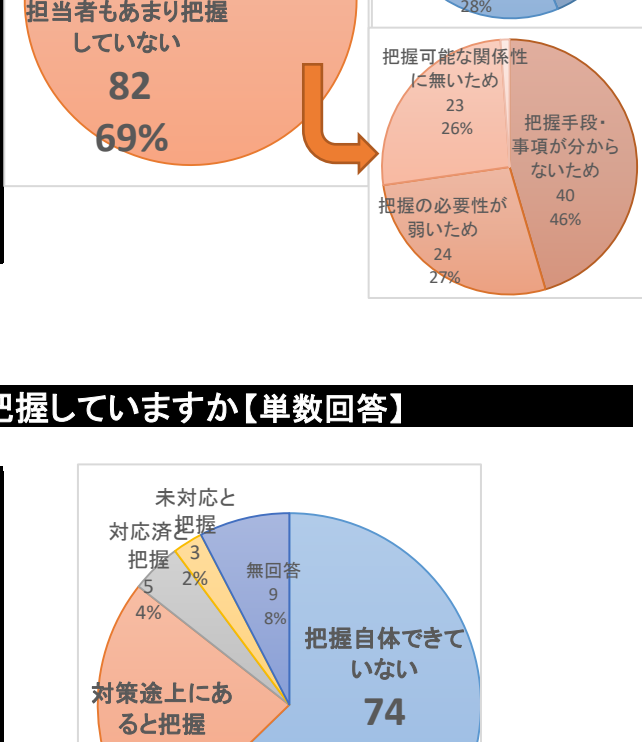
②-B：システムや重要データの非連携先

現状	担当者が概ね把握	33	28%
理由	把握するべき必要性が有る（強い）ため	18	46%
	把握手段や把握すべき事項が社内規定や第三者認証等により明確化されているため	10	26%
	把握可能な（教えてもらえる）関係性に有るため（信頼関係・上下関係等）	10	26%
	その他 （ ・把握が必要な場合は個別対応）	1	3%
現状	担当者もあまり把握していない	77	65%
理由	把握手段や把握すべき事項が社内規定や第三者認証等により 明確化されていない（分からない）ため	37	45%
	把握するべき必要性が 無い（弱い）ため	24	29%
	把握可能な（教えてもらえる）関係性に無いため（信頼関係・上下関係等）	20	24%
	その他	2	2%
現状	無回答	8	7%
		118	100%



③-A：汎用品・間接材等の取引先

現状	担当者が概ね把握	22	19%
理由	把握するべき必要性が有る（強い）ため	10	40%
	把握手段や把握すべき事項が社内規定や第三者認証等により明確化されているため	7	28%
	把握可能な（教えてもらえる）関係性に有るため（信頼関係・上下関係等）	7	28%
	その他 （ ・把握が必要な場合は個別対応）	1	4%
現状	担当者もあまり把握していない	88	75%
理由	把握手段や把握すべき事項が社内規定や第三者認証等により 明確化されていない（分からない）ため	40	43%
	把握するべき必要性が 無い（弱い）ため	27	29%
	把握可能な（教えてもらえる）関係性に無いため（信頼関係・上下関係等）	25	27%
	その他	1	1%
現状	無回答	8	7%
		118	100%

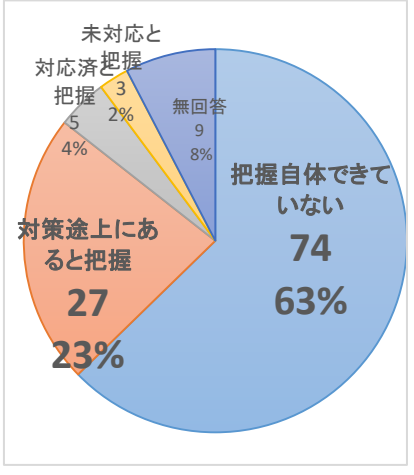


③-B：特注品・直接材等の取引先

現状	担当者が概ね把握	28	24%
理由	把握するべき必要性が有る（強い）ため	14	44%
	把握手段や把握すべき事項が社内規定や第三者認証等により明確化されているため	9	28%
	把握可能な（教えてもらえる）関係性に有るため（信頼関係・上下関係等）	8	25%
	その他 （ ・把握が必要な場合は個別対応）	1	3%
現状	担当者もあまり把握していない	82	69%
理由	把握手段や把握すべき事項が社内規定や第三者認証等により 明確化されていない（分からない）ため	40	45%
	把握するべき必要性が 無い（弱い）ため	24	27%
	把握可能な（教えてもらえる）関係性に無いため（信頼関係・上下関係等）	23	26%
	その他	1	1%
現状	無回答	8	7%
		118	100%

＜問3＞取引先が「Windows7/Windows Server2008」サポート終了の対応が出来ているかどうか把握していますか【単数回答】

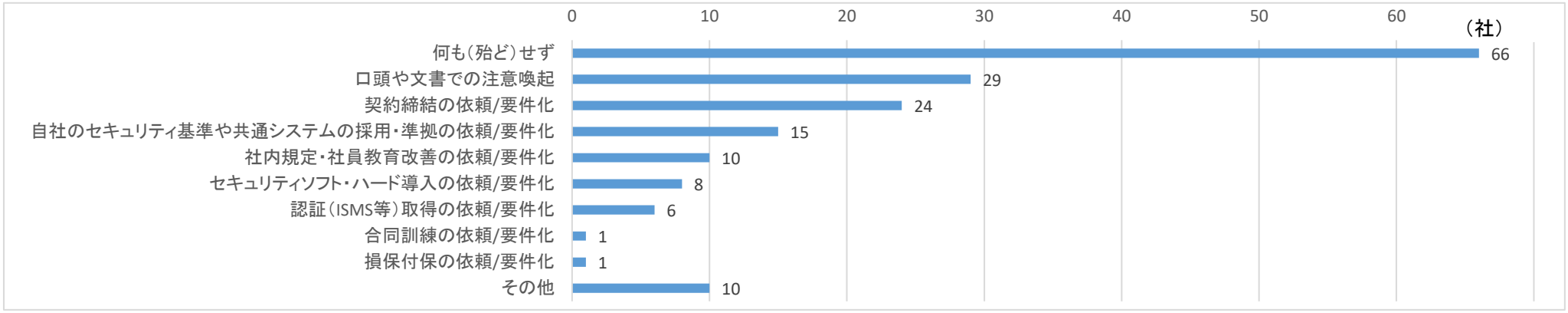
把握自体できていない	74	63%
対策途上にあると把握	27	23%
対応済と把握	5	4%
未対応と把握	3	3%
無回答	9	8%
	118	100%



＜問4＞取引先のサイバーセキュリティーにつき「貴社の関与・管理等の現状」を教えて下さい【複数回答】

何も（殆ど）せず	66	56%
口頭や文書での注意喚起	29	25%
契約締結の依頼/要件化	24	20%
自社のセキュリティ基準や共通システムの採用・準拠の依頼/要件化	15	13%
社内規定・社員教育改善の依頼/要件化	10	8%
セキュリティソフト・ハード導入の依頼/要件化	8	7%
認証（ISMS等）取得の依頼/要件化	6	5%
合同訓練の依頼/要件化	1	1%
損保付保の依頼/要件化	1	1%
その他	10	8%
回答社数	118	—

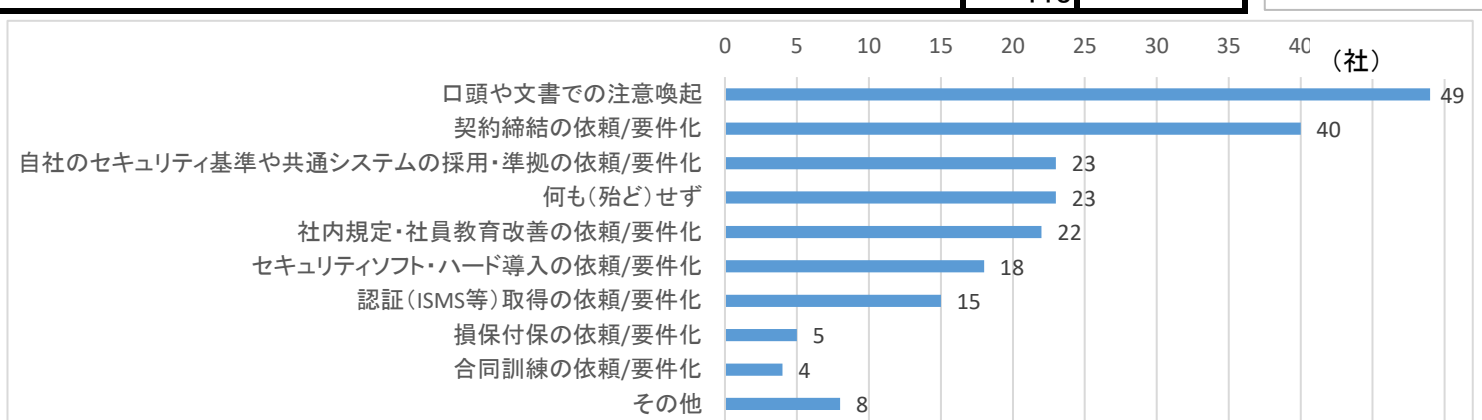
その他
・必要な場合は契約締結
・セキュリティという名目で安易に他社へ確認を求めること疑問
・取引の内容や取引先との関係により異なる
・外部委託先管理の一環として定期的にサイバーセキュリティへの取組状況を確認
・IT関連パートナーにはセキュリティ要件を求めている
・セキュリティテスト実施
・セキュリティ現状確認アンケートを一部の取引先に対し実施
・情報漏えい防止誓約書の提出
・情報セキュリティ対策に関する定期的な自己診断の依頼
・重要な情報やシステムの連携先は自社セキュリティ基準や共通システムの採用・準拠を依頼



＜問5＞取引先のサイバーセキュリティーにつき「貴社が今後求めていきたいこと（取引要件等）」を教えて下さい【複数回答】

口頭や文書での注意喚起	49	42%
契約締結の依頼/要件化	40	34%
自社のセキュリティ基準や共通システムの採用・準拠の依頼/要件化	23	19%
何も（殆ど）せず	23	19%
社内規定・社員教育改善の依頼/要件化	22	19%
セキュリティソフト・ハード導入の依頼/要件化	18	15%
認証（ISMS等）取得の依頼/要件化	15	13%
損保付保の依頼/要件化	5	4%
合同訓練の依頼/要件化	4	3%
その他	8	7%
回答社数	118	—

その他
・必要な場合は契約締結可能か
・セキュリティという名目で安易に他社へ確認 を求めることに疑問
・販売先がアナログであり今は必要性を感じない
・取引契約へのサイバー攻撃被害に関する保証規定の追記等
・取引の内容や取引先との関係により異なる
・サイバーセキュリティ管理体制や取組状況に関する十分な情報開示
・情報漏えい防止誓約書の提出
・弊社に関する情報セキュリティインシデント 発生時の迅速な報告体制の整備

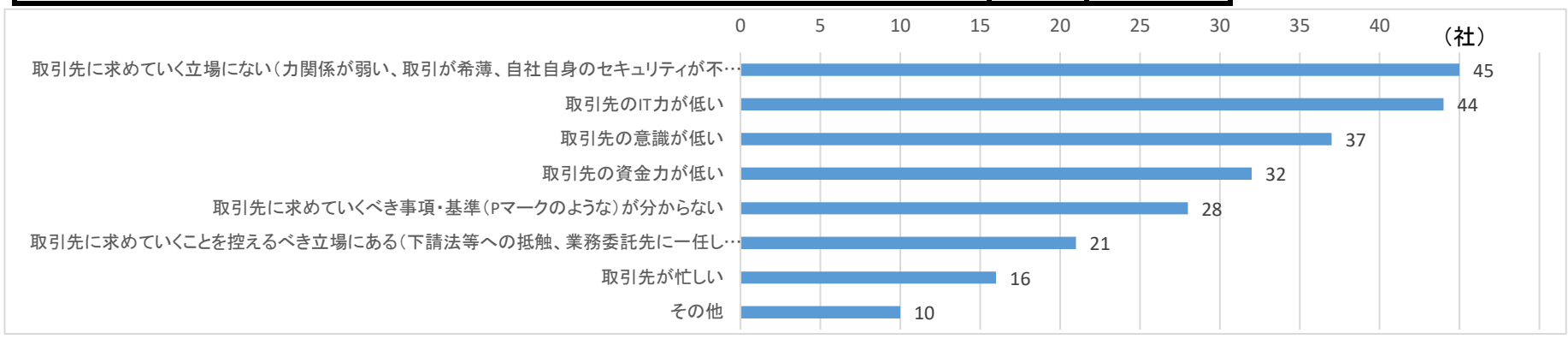


＜問6＞取引先のサイバーセキュリティーにつき「貴社が今後求めていきたいが足かせとなる点」を教えて下さい【複数回答】

取引先に求めていく立場にない（力関係が弱い、取引が希薄、自社自身のセキュリティが不十分等）	45	38%
取引先のIT力が低い	44	37%
取引先の意識が低い	37	31%
取引先の資金力が低い	32	27%
取引先に求めていくべき事項・基準（Pマークのような）が分からない	28	24%
取引先に求めていくことを控えるべき立場にある（下請法等への抵触、業務委託先に一任している等）	21	18%
取引先が忙しい	16	14%
その他	10	8%
回答社数	118	—

その他

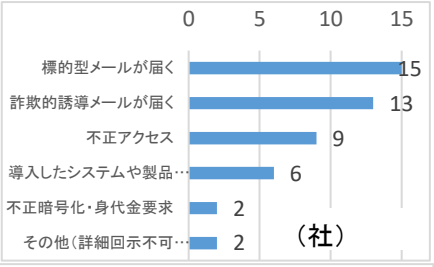
・各社各様確認しないとわからない
・取引先数が多いため、作業が煩雑になる
・取引内容や関係により異なる
・再委託先や再々委託先以降の把握
・取引先のIT環境が不明
・取引先が多すぎて、現実的ではない



＜問7＞取引先がサイバー攻撃被害を受け、それが貴社に及んだ経験がある場合（のみ）「内容・被害」を教えて下さい【複数回答】

内容（「及んだ経験がある」と回答した30社）

		経験ある30社の中で（内訳の比率）	経験ないを含む全118社の中で
標的型メールが届く	15	50%	13%
詐欺的誘導メールが届く	13	43%	11%
不正アクセス	9	30%	8%
導入したシステムや製品にウィルス等が混入	6	20%	5%
不正暗号化・身代金要求	2	7%	2%
その他（詳細回示不可　など）	2	7%	2%
	30	—	—



被害（「及んだ経験がある」と回答した30社）

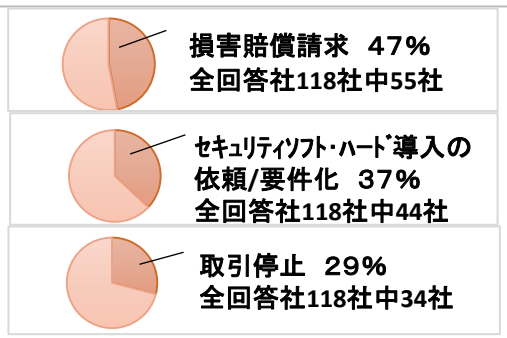
		経験ある30社の中で（内訳の比率）	経験ないを含む全118社の中で
被害は（殆ど）及ばなかった	24	80%	
情報漏洩	5	17%	4%
システムのダウン	3	10%	3%
データの損壊	3	10%	3%
流通途絶	0	0%	0%
信用低下	0	0%	0%
	30	—	—

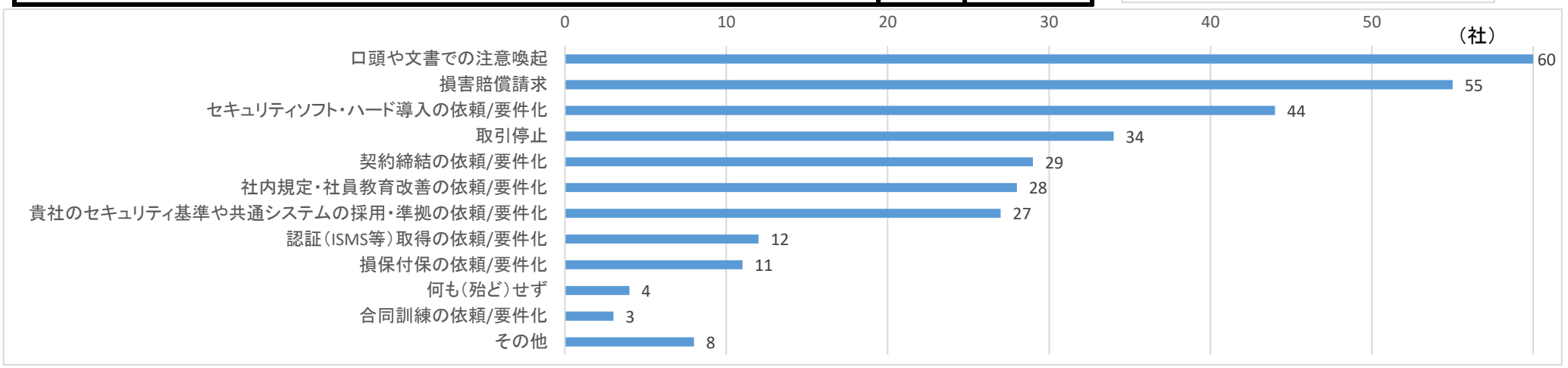
※被害が及んだ頭数：8社（全体の約7%）
※「被害は（殆ど）及ばなかった」とともに
　複数回答している会社あり

＜問8＞取引先がもしサイバー攻撃被害を受け、その被害が貴社にも及んだ場合「貴社が採り得る対処」を教えて下さい【複数回答】

口頭や文書での注意喚起	60	51%
損害賠償請求	55	47%
セキュリティソフト・ハード導入の依頼/要件化	44	37%
取引停止	34	29%
契約締結の依頼/要件化	29	25%
社内規定・社員教育改善の依頼/要件化	28	24%
貴社のセキュリティ基準や共通システムの採用・準拠の依頼/要件化	27	23%
認証（ISMS等）取得の依頼/要件化	12	10%
損保付保の依頼/要件化	11	9%
何も（殆ど）せず	4	3%
合同訓練の依頼/要件化	3	3%
その他	8	7%
	118	—

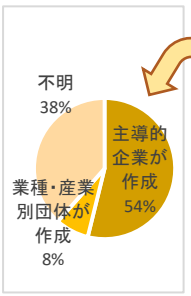
その他
・ケースバイケースでの判断となる
・再発防止策の提出を求める
・取引先との力関係による
・わからない
・フォレンジック調査
・公的機関（IPA等）への報告要請
・お客さま本位の観点からその他何らかの要請は有り得る
・改善提案

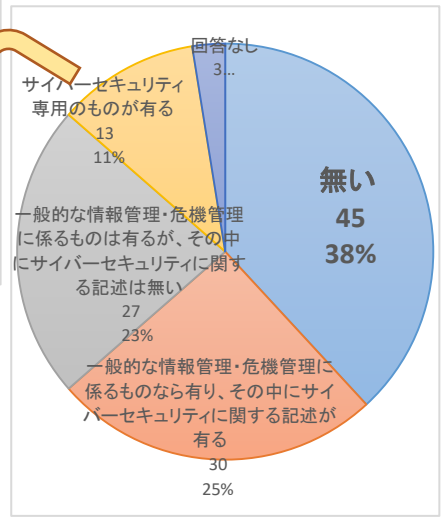




＜問9＞貴社の最重要サプライチェーンにおいてサイバーセキュリティーの協定・マニュアル等はありますか【単数回答】

サイバーセキュリティ専用のものが有る		**13**	**11%**
作成者	主導的企業が作成	7	54%
	業種・産業別団体が作成	1	8%
	不明	5	38%
一般的な情報管理・危機管理に係るものなら有り、その中にサイバーセキュリティに関する記述が有る		**30**	**25%**
一般的な情報管理・危機管理に係るものは有るが、その中にサイバーセキュリティに関する記述は無い		**27**	**23%**
無い		**45**	**38%**
理由	対象企業の線引きが困難	15	33%
	主導的企業が無い	9	20%
	業種・産業別団体が無い	4	9%
	その他（・対象の線引きが困難だが、サイバーセキュリティに関する記述等は有ると思われる　）	17	38%
無回答		**3**	**3%**
		118	100%

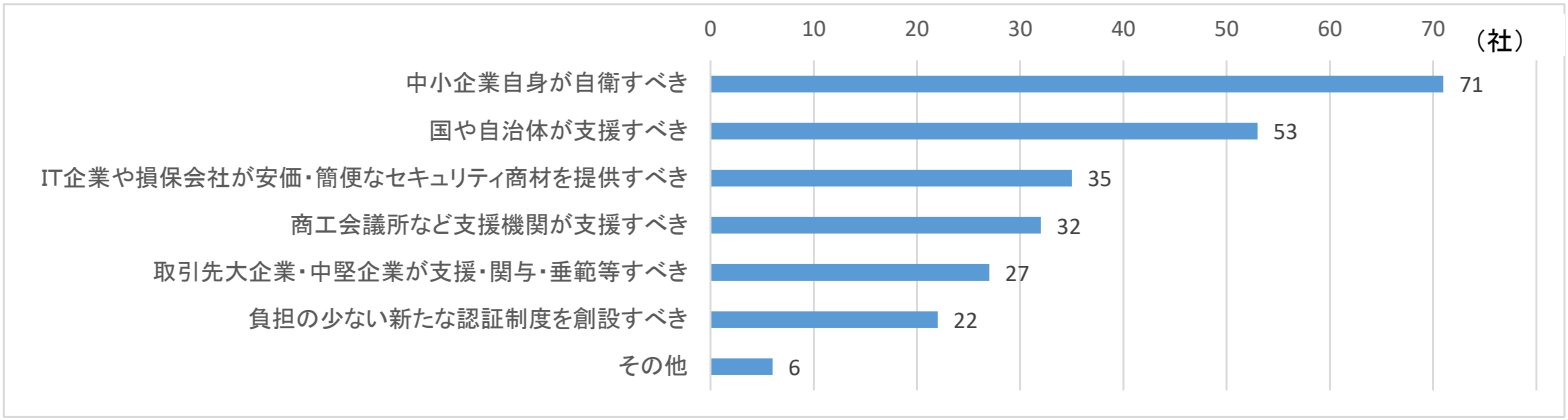


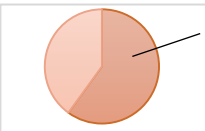


＜問10＞中小企業のサイバーセキュリティーは今後どうしていくべきだと思いますか【複数回答】

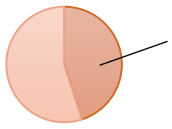
中小企業自身が自衛すべき	71	60%
国や自治体が支援すべき	53	45%
IT企業や損保会社が安価・簡便なセキュリティ商材を提供すべき	35	30%
商工会議所など支援機関が支援すべき	32	27%
取引先大企業・中堅企業が支援・関与・垂範等すべき	27	23%
負担の少ない新たな認証制度を創設すべき	22	19%
その他	6	5%
	118	—

その他
・セキュリティソフトの導入を促す政策を整備する必要がある。
・契約上、セキュリティ義務を果たしても、実際にテストや監査までは手が回らない。
・単独での対応はコスト面で困難。
・中国の様に国として国外からの攻撃を防ぐことが効果的と考え、末端での施策に対し、費用や技術指導等の助成が必要。
・自己防衛が基本。

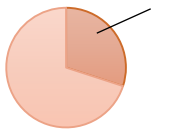




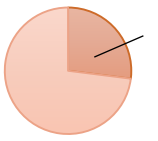
中小企業自身が自衛すべき　60%
全回答社118社中71社



国や自治体が支援すべき　45%
全回答社118社中53社



IT企業や損保会社が安価・簡便なセキュリティ商材を提供すべき
30%
全回答社118社中35社



商工会議所など支援機関が支援すべき
27%
全回答社118社中32社