

サイバー犯罪被害・対策アンケート結果

【有効回答：県内企業112社】

※本頁は、アンケート結果の一部抜粋となります。
基礎情報及び結果の詳細は別紙をご覧ください。

Q.自社がサイバー攻撃を受けたことがある

はい **20.5%**

業種別「はい」の内訳

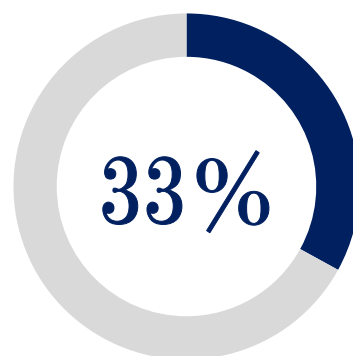
70.0% 製造業

33.3% 第一次産業(農業等)

25.0% サービス業

21.4% 卸売・小売・飲食業

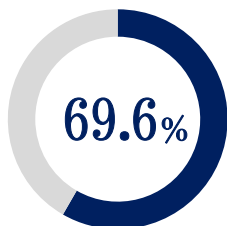
Q.サイバー攻撃・被害のニュース等を見ても他人事(自社は大丈夫)と感じた経験



ある

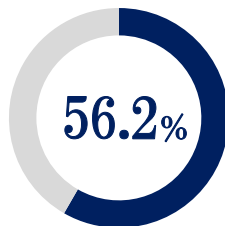
(+どちらかと言えばある)

Q.自社が被害を受けたサイバー攻撃の手口



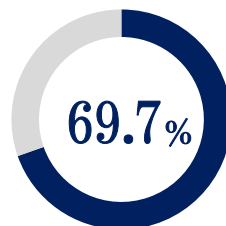
サプライチェーン攻撃 (最多)

Q.自社のサイバーセキュリティ対策は万全か



万全だと思う
(+まあ万全だと思う)

Q.インシデント発生時の社内マニュアルの有無



ない
(+分からない)

Q.サイバーセキュリティ対策への投資額(過去3期)

22.3% 投資していない

41.1% 100万円未満

6.3% 100万円～500万円未満

1.8% 500万円～1,000万円未満

0.0% 1,000万円～1億円未満

0.9% 1億円以上

※ 分からない：27.7%

Q.社員へのサイバーセキュリティ教育頻度(年)

68.9% 実施していない

6.7% 1回

5.6% 2回

8.9% 3回～4回

10% 5回以上

Q.サイバー攻撃被害時に警察への通報をためらう理由

60% 社会的反響が気になる

15% 大きさにしたくない

10% 自社で解決したい

10% 外部の委託会社に任せる

5% 警察に通報すべきか分からない

目 次 ①

○ 基 礎 情 報	・・・1
-----------	------

社内セキュリティ

Q1. 社内のサイバーセキュリティ対策は万全ですか？	・・・2
▶ Q1.の「万全だと思う・まあ万全だと思う」の各種別割合	・・・2
Q2. 社内の情報資産管理で最も脅威と覚えることは何ですか？	・・・2
Q3. 社内に導入されているセキュリティ対策は何ですか？	・・・3
▶ Q3.の「導入しているものはない」の各種別上位	・・・3
Q4. 今後さらに必要(重要)だと思われるサイバーセキュリティ対策は何ですか？	・・・3
Q5. サイバーセキュリティ対策を実施する上での課題は何ですか？	・・・4
Q6. 社内のサイバーセキュリティ対策はどこで管理していますか？	・・・4
Q7. サイバーセキュリティ対策の体制について教えてください。	・・・4
▶ Q7.の「担当者はいない」の各種別割合	・・・5
Q8. サイバーセキュリティへの投資額（直近過去3期）を教えてください。	・・・5
▶ Q8.の「投資をしていない」の理由は何ですか？	・・・5
▶ Q8.の「投資をしていない」の各種別割合	・・・6
Q9. サイバーセキュリティ関連製品やソフトウェアの導入状況を教えてください。	・・・6
Q10. サイバーセキュリティ対策が取引要件に入っていた（対策が取引に繋がった）ことがありますか？	・・・7
▶ Q10.の「ある」の各種別割合	・・・7
Q11. サイバーセキュリティ対策で警察に期待することは何ですか？	・・・7

目 次 ②

サイバー犯罪・攻撃被害

Q12. 過去にサイバー犯罪・攻撃の被害を受けたことがありますか？	・・・8
▶ Q12.の「はい」の各種別割合	・・・8
▶ Q12.の被害を受けたサイバー犯罪・攻撃の手口は何ですか？	・・・8
▶ Q12.の具体的な被害は何ですか？	・・・9
▶ Q12.の被害により生じた影響は何ですか？	・・・9
▶ Q12.の被害により生じた取引先（サプライチェーン）への影響は何がありますか？	・・・9

サイバーインシデント対応

Q13. 社内にサイバーインシデント発生時のマニュアルはありますか？	・・・10
▶ Q13.の「ない」の各種別割合	・・・10
Q14. サイバーインシデント発生時の相談先として、どこを想定していますか？	・・・10
Q15. サイバーセキュリティに関する被害のニュース等を見て、「当社は大丈夫だ」（他人事）と感じたことはありますか？	・・・11
▶ Q15.の「ある」・「どちらかといえばある」の各種別割合	・・・11
Q16. 自社がサイバー攻撃等を受けて情報流出等があった場合、警察への通報をためらう可能性はありますか？	・・・11
▶ Q16.の警察に通報したくない理由は何ですか？	・・・12

目 次 ③

サイバーセキュリティ教育

Q17. 従業員に対するサイバーセキュリティ教育の年間実施頻度を教えてください。	…12
▶ Q17.の従業員への教育を年3回以上実施している各種別割合	…12
▶ Q17.の教育で得られている効果は何ですか？	…13
▶ Q17.の教育を実施する上での課題は何ですか？	…13

サイバー保険

Q18. 企業向けサイバー保険に加入していますか？	…13
▶ Q18.の「はい」の各種別割合	…14
▶ Q18.の保険に加入したきっかけは何ですか？	…14
▶ Q18.の保険に加入していない理由は何ですか？	…14
▶ Q18.の保険に加入していない理由の「その他」の理由	…15
▶ Q18.の保険に今後加入する予定はありますか？	…15
▶ Q18.の今後加入する予定「ある・検討したい」の各種別割合	…15

基 礎 情 報

調査期間 : 2025.5.19～2025.8.30
調査対象 : 県内企業（無作為）
調査方法 : Googleフォーム
有効回答 : 112社

有効回答の内訳

地域別

国 中 : 83

峡東 : 22
峡北 : 15
峡南 : 06
峡西 : 06
峡中 : 34

郡 内 : 28

東部 : 11
富士五湖 : 17

未回答 : 01

※管轄署別に集計したため、峡中の甲斐市（甲斐署）は峡北にカウント

管轄別

甲 府 警 察 署 : 22
南 甲 府 警 察 署 : 12
南アルプス警察署 : 06
甲 斐 警 察 署 : 13
北 杜 警 察 署 : 02
鰍 沢 警 察 署 : 03
南 部 警 察 署 : 03
笛 吹 警 察 署 : 10
日 下 部 警 察 署 : 12
吉 田 警 察 署 : 17
大 月 警 察 署 : 10
上 野 原 警 察 署 : 01
未 回 答 : 01

業種別

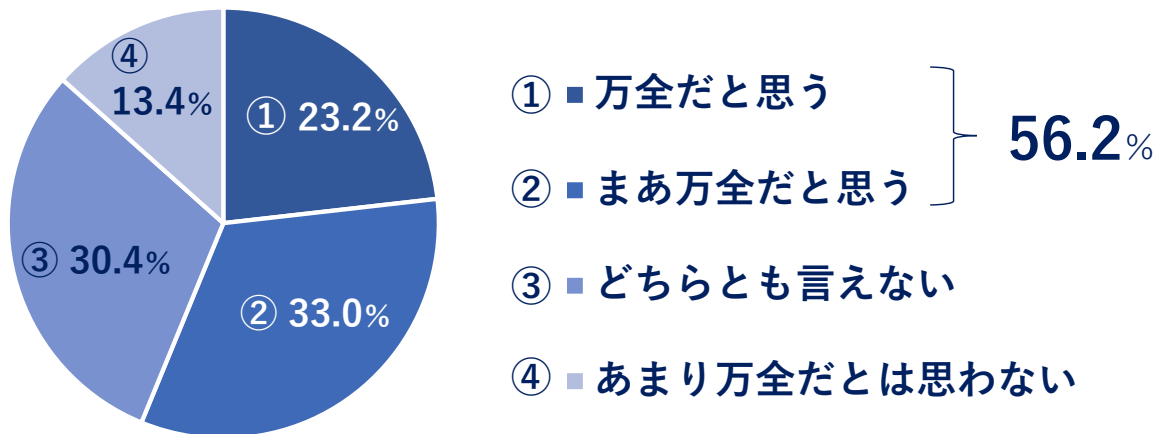
金 融 ・ 保 険 業 : 34
建 設 業 : 31
卸売・小売・飲食業 : 14
サ ー ビ ス 業 : 12
製 造 業 : 10
運 輸 ・ 通 信 業 : 04
第一次産業（農業等） : 03
不 動 産 業 : 02
そ の 他 : 02

従業員数別

9 名 以 下 : 48
10 名 ～ 29 名 : 34
30 名 ～ 49 名 : 12
50 名 ～ 99 名 : 08
100 名 ～ 499 名 : 08
500 名 ～ 999 名 : 00
1,000 名 以 上 : 02

Q1. 社内のサイバーセキュリティ対策は万全ですか？

※小数点第1位以下四捨五入のため合計100%とならない場合あり。以下共通。



Q1.の「万全だと思う・まあ万全だと思う」の各種別割合

業種別

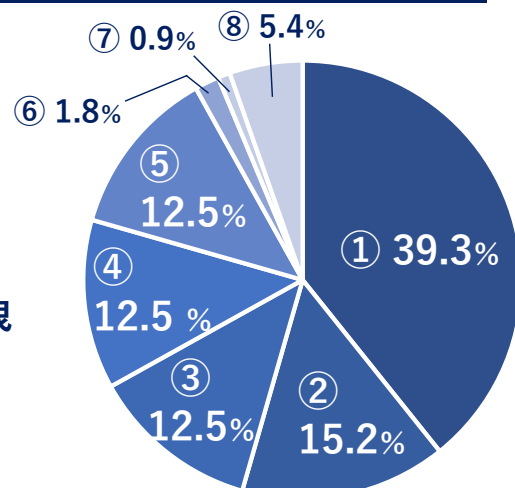
	(%)
金融・保険業	88.2
建設業	25.8
卸売・小売・飲食業	42.9
サービス業	50.0
製造業	80.0
運輸・通信業	25.0
第一次産業（農業等）	33.3
不動産業	100
その他	50.0

従業員数別

	(%)
9名以下	54.2
10名～29名	50.0
30名～49名	83.3
50名～99名	37.5
100名～499名	62.5
500名～999名	—
1,000名以上	100

Q2. 社内の情報資産管理で最も脅威と覚えることは何ですか？

- ① 標的型攻撃による情報流出
- ② ランサムウェアによる詐欺・恐喝
- ③ 妨害攻撃によるサービスの停止
- ④ 内部不正による情報漏洩
- ⑤ 災害等不測の事態に伴う情報漏洩
- ⑥ ウェブサイトの改ざん
- ⑦ 脅威と覚えるものはない
- ⑧ わからない



Q3. 社内に導入されているセキュリティ対策は何ですか？

(複数回答可)

(回答数)

- 89 ウイルス対策ソフトのインストール・ウイルス定義ファイルの更新
- 47 社内ネットワークへの不正侵入検知・フィルタリング
- 42 ファイルデータのバックアップ
- 39 社員への情報セキュリティ研修
- 34 USBメモリ等での情報持出規制・社外送信メールへのファイル添付規制
- 32 ファイルデータのバックアップ（クラウドとの連携）
- 30 お客様情報等、機密情報へのアクセス制限
- 19 セキュリティ機器の遠隔監視
- 03 ファイルデータの世代管理
- 03 導入しているものはない

Q3.の「導入しているものはない」の各種別上位

業種別

- ① 卸売・小売・飲食業 ……02件
- ② サービス業 ……01件

従業員数別

- ① 9人以下 ……03件

Q4. 今後さらに必要(重要)だと思われるサイバーセキュリティ対策は何ですか？

(複数回答可)

(回答数)

- 43 社内ネットワークへの不正侵入検知・フィルタリング
- 40 従業員へのサイバーセキュリティ研修
- 33 ウイルス対策ソフトのインストール・ウイルス定義ファイルの更新
- 29 お客様情報等の機密情報へのアクセス制限
- 22 USBメモリ等での情報持出規制・社外送信メールへのファイル添付規制
- 20 ファイルデータのバックアップ（クラウドとの連携）
- 18 セキュリティ機器の遠隔監視
- 15 ファイルデータの世代管理
- 13 ファイルデータのバックアップ

Q5. サイバーセキュリティ対策を実施する上での課題は何ですか？

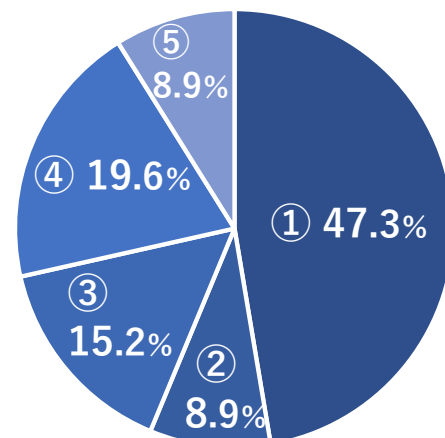
(複数回答可)

(回答数)

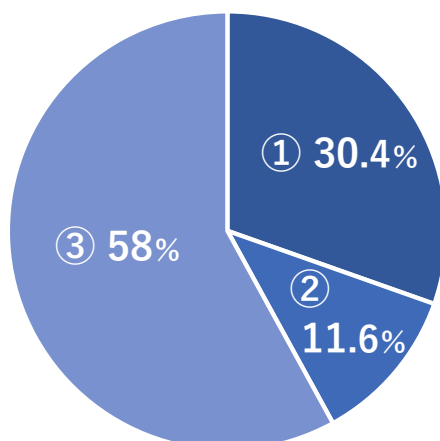
69	コスト面の不安がある
46	社内に対策スキルを持つ人材がいない
38	社員教育が不十分で対策が徹底されていない
26	社内に専任の担当（部署）がない
19	対策の優先順位が不明瞭
12	最新の情報を得る手段がない
04	統一的なポリシーがなく部署により対応にばらつきがある

Q6. 社内のサイバーセキュリティ対策はどこで管理していますか？

- ① ■ 社内管理している
- ② ■ 外部委託している
- ③ ■ 一部外部委託している
- ④ ■ セキュリティ対策をしていない
- ⑤ ■ わからない



Q7. サイバーセキュリティ対策の体制について教えてください。



- ① ■ 専門部署（担当者）がある
- ② ■ 兼務で担当者がある
- ③ ■ 担当者はいない

Q7.の「担当者はいない」の各種別割合

業種別

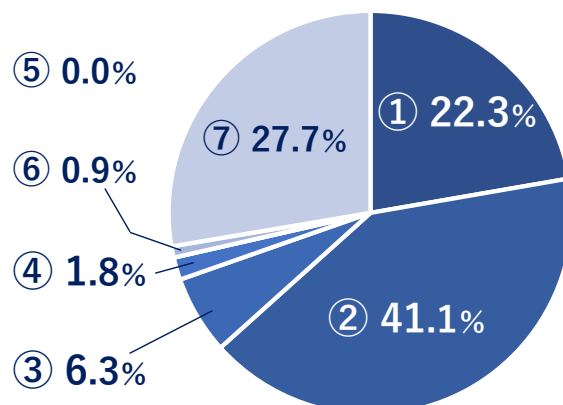
	(%)
金融・保険業	8.8
建設業	83.9
卸売・小売・飲食業	85.7
サービス業	66.7
製造業	70.0
運輸・通信業	100
第一次産業（農業等）	66.7
不動産業	50.0
その他	100

従業員数別

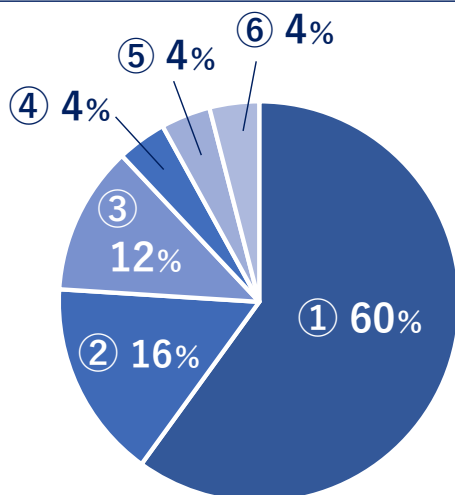
	(%)
9名以下	62.5
10名～29名	70.6
30名～49名	66.7
50名～99名	25.0
100名～499名	12.5
500名～999名	—
1,000名以上	0.0

Q8. サイバーセキュリティへの投資額（直近過去3期）を教えてください。

- ① ■ 投資していない
- ② ■ 100万円未満
- ③ ■ 100～500万円未満
- ④ ■ 500～1,000万円未満
- ⑤ ■ 1,000～1億円未満
- ⑥ ■ 1億円以上
- ⑦ ■ わからない



Q8.の「投資をしていない」の理由は何ですか？



- ① ■ どこから始めたらよいか分からない
- ② ■ 費用対効果が見えない
- ③ ■ コストがかかりすぎる
- ④ ■ 必要性を感じない
- ⑤ ■ 親会社に任せている
- ⑥ ■ 以前に投資している(3期より前)

Q8.の「投資をしていない」の各種別割合

業種別	(%)	従業員数別	(%)
金融・保険業	2.9	9名以下	37.5
建設業	25.8	10名～29名	14.7
卸売・小売・飲食業	14.3	30名～49名	16.7
サービス業	50.0	50名～99名	0.0
製造業	30.0	100名～499名	0.0
運輸・通信業	50.0	500名～999名	—
第一次産業（農業等）	33.3	1,000名以上	0.0
不動産業	50.0		
その他	50.0		

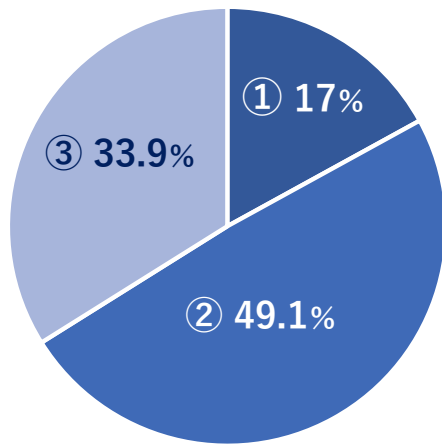
Q9. サイバーセキュリティ関連製品やソフトウェアの導入状況を教えてください。

（複数回答可）

（回答数）

80	ウイルス対策ソフト
30	ファイアーウォール
24	ウェブ閲覧のフィルタリングソフト
24	ワンタイムパスワード、ICカード、USBキー、生体認証等
18	VPN
15	暗号化製品（ディスク、ファイル、メール等）
14	セキュリティ情報管理システム製品（ログ情報の統合分析等）
12	ソフトウェアライセンス管理・IT資産管理製品
11	アイデンティティ管理・ログオン管理・アクセス許可製品
10	クライアントPCの設定・動作等を管理する製品
04	フィルタリングソフトウェア
12	特に導入しているものはない

Q10. サイバーセキュリティ対策が取引要件に入っていた (対策が取引に繋がった) ことがありますか？



- ① ■ ある
- ② ■ ない
- ③ ■ わからない

Q10.の「ある」の各種別割合

業種別

	(%)
金融・保険業	14.7
建設業	6.5
卸売・小売・飲食業	14.3
サービス業	25.0
製造業	60.0
運輸・通信業	0.0
第一次産業（農業等）	0.0
不動産業	50.0
その他	0.0

従業員数別

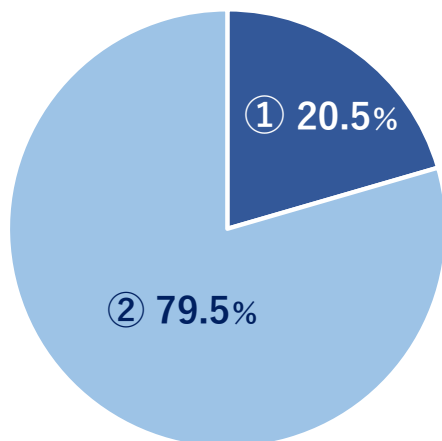
	(%)
9名以下	10.4
10名～29名	11.8
30名～49名	58.3
50名～99名	12.5
100名～499名	25.0
500名～999名	—
1,000名以上	0.0

Q11. サイバーセキュリティ対策で警察に期待することは 何ですか？

(回答数)

60	犯人の逮捕・検挙
50	サイバーセキュリティに関する情報提供
40	サイバーセキュリティ対策講演等の実施
32	インシデント発生時の相談
04	期待することはない

Q12. 過去にサイバー犯罪・攻撃の被害を受けたことがありますか？



① ■ はい

② ■ いいえ

Q12.の「はい」の各種別割合

業種別

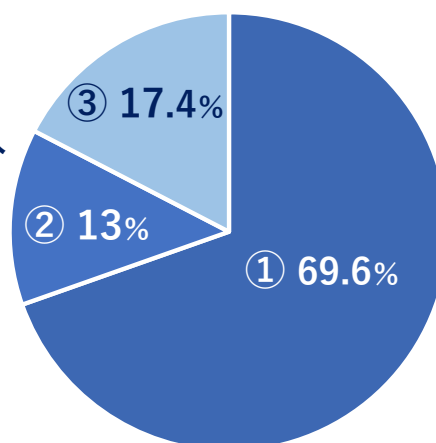
	(%)
金融・保険業	8.8
建設業	19.4
卸売・小売・飲食業	21.4
サービス業	25.0
製造業	70.0
運輸・通信業	0.0
第一次産業（農業等）	33.3
不動産業	0.0
その他	0.0

従業員数別

	(%)
9名以下	8.3
10名～29名	20.6
30名～49名	58.3
50名～99名	25.0
100名～499名	25.0
500名～999名	—
1,000名以上	50.0

Q12.の被害を受けたサイバー犯罪・攻撃の手口は何ですか？

- ① ■ 取引先やグループ会社等を経由して侵入
(サプライチェーン攻撃)
- ② ■ 脆弱性を突かれた不正アクセス
- ③ ■ 手口不明



Q12.の具体的な被害は何ですか？（複数回答可）

（回答数 ※本頁以下同じ）

- 04 業務サーバのサービス停止（又は機能低下）
- 03 個人情報の漏洩
- 03 取引先（企業・個人）への被害拡大
- 03 ランサムウェアによる身代金の要求
- 02 標的型攻撃による不正アクセス
- 02 自社ウェブサイトのサービス停止（又は機能低下）
- 01 自社ウェブサイトの改ざん
- 01 業務サーバの内容の改ざん
- 01 提供するネットワークサービスの不正利用
- 07 被害なし

Q12.の被害により生じた影響は何ですか？（複数回答可）

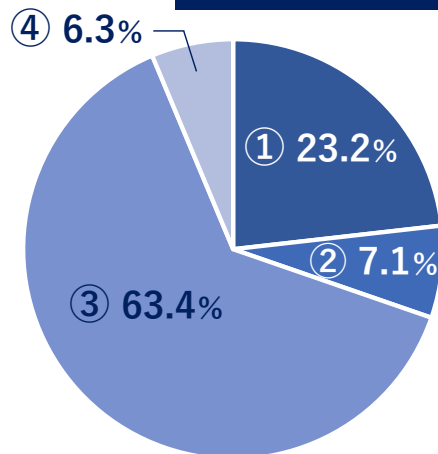
- 08 システム停止・性能低下
- 06 パソコン単体の停止
- 05 ウイルスメール等の発信
- 04 データの破壊
- 02 個人情報の漏洩
- 02 ネットワークの遅延
- 02 取引先への感染拡大
- 01 個人の業務停滞
- 02 特になし

（複数回答可）

Q12.で取引先（サプライチェーン）への影響は何がありますか？

- 11 サービスの障害、遅延、停止等による逸失利益
- 06 原因調査、復旧等にかかわる人件費等の経費負担
- 03 個人顧客や法人取引先に対する信頼の失墜
- 02 個人顧客への賠償や法人取引先への補償負担
- 01 裁判、調停等にかかわる人件費等の経費負担
- 06 特になし

Q13. 社内にサイバーインシデント発生時のマニュアルはありますか？



- ① ■ ある
② ■ あるが内容は知らない
③ ■ ない
④ ■ わからない
- 69.7%

Q13.の「ない」の各種別割合

業種別

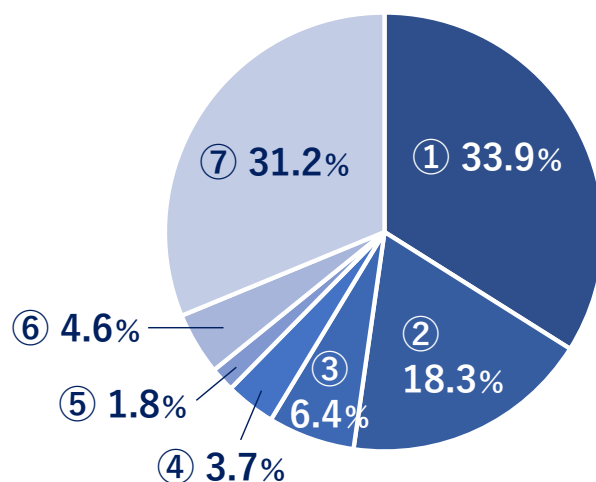
	(%)
金融・保険業	2.9
建設業	100
卸売・小売・飲食業	71.4
サービス業	75.0
製造業	100
運輸・通信業	100
第一次産業（農業等）	100
不動産業	50.0
その他	100

従業員数別

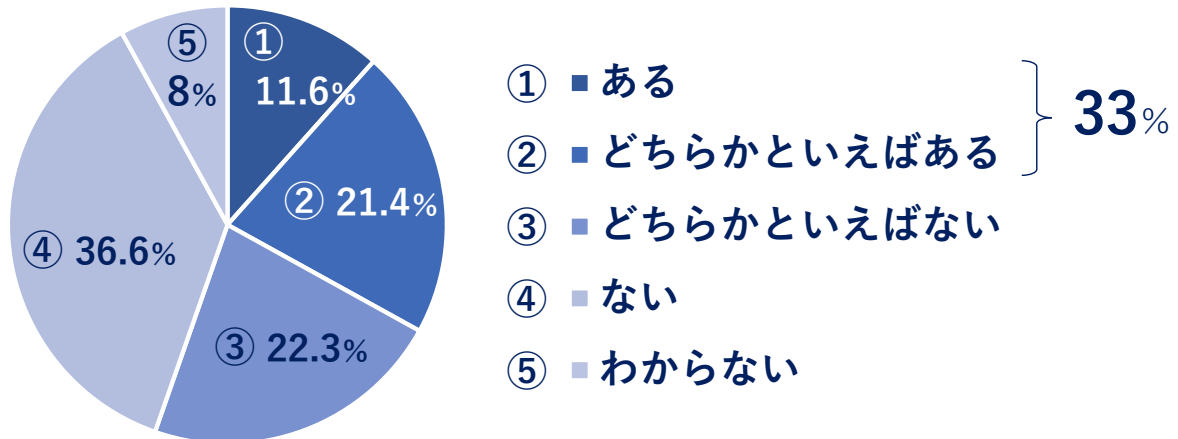
	(%)
9名以下	64.6
10名～29名	73.5
30名～49名	83.3
50名～99名	50.0
100名～499名	12.5
500名～999名	—
1,000名以上	0.0

Q14. サイバーインシデント発生時の相談先としてどこを想定していますか？

- ① ■ 警察
② ■ パートナー企業
③ ■ 親会社・本社・社内担当部署
④ ■ 情報処理推進機構（IPA）
⑤ ■ JPCERT/CC
⑥ ■ その他
⑦ ■ 想定していない・分からない



Q15. サイバーセキュリティに関する被害のニュース等を見て、「当社は大丈夫だ」（他人事）と感じたことはありますか？

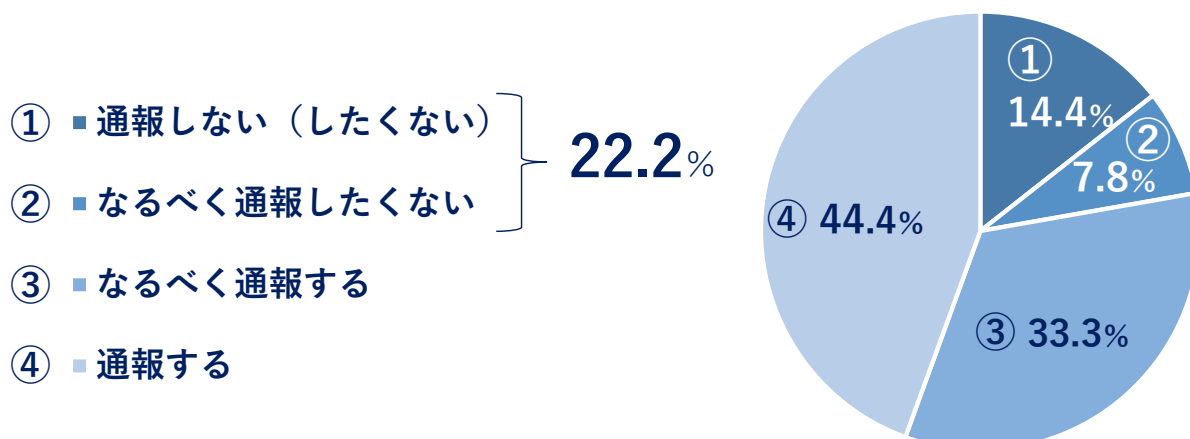


Q15.の「ある」・「どちらかといえばある」の各種別割合

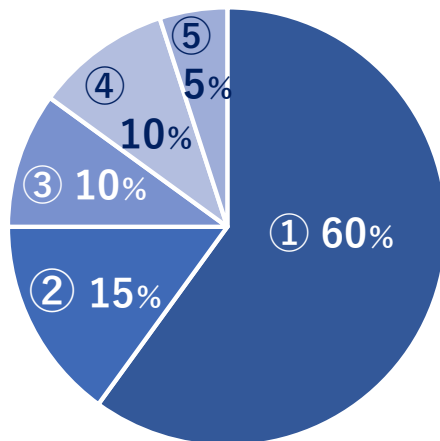
業種別		(%)
金融・保険業	55.9	
建設業	6.5	
卸売・小売・飲食業	21.4	
サービス業	41.7	
製造業	70.0	
運輸・通信業	25.0	
第一次産業（農業等）	0.0	
不動産業	0.0	
その他	0.0	

従業員数別		(%)
9名以下	29.2	
10名～29名	29.4	
30名～49名	50.0	
50名～99名	37.5	
100名～499名	50.0	
500名～999名	－	
1,000名以上	0.0	

Q16. 自社がサイバー攻撃等を受けて情報流出等があった場合、警察への通報をためらう可能性はありますか？



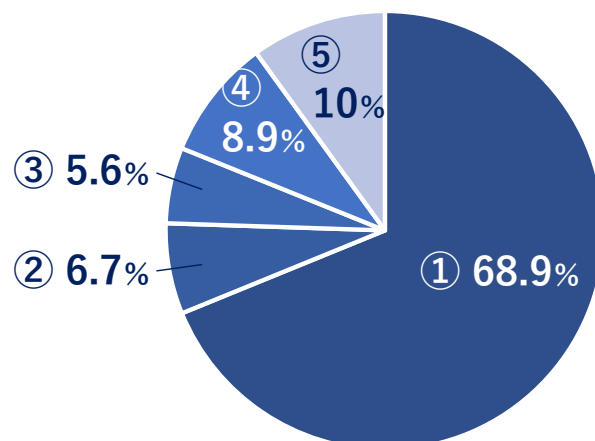
Q16.の警察に通報したくない理由は何ですか？



- ① ■ 社会的反響が気になる
- ② ■ 大げさにしたくない
- ③ ■ 自社で解決したい
- ④ ■ 外部の委託会社に任せる
- ⑤ ■ 通報すべきか分からない

Q17. 従業員に対するサイバーセキュリティ教育の年間実施頻度を教えてください。

- ① ■ 実施していない
- ② ■ 1 回
- ③ ■ 2 回
- ④ ■ 3～4 回
- ⑤ ■ 5 回以上



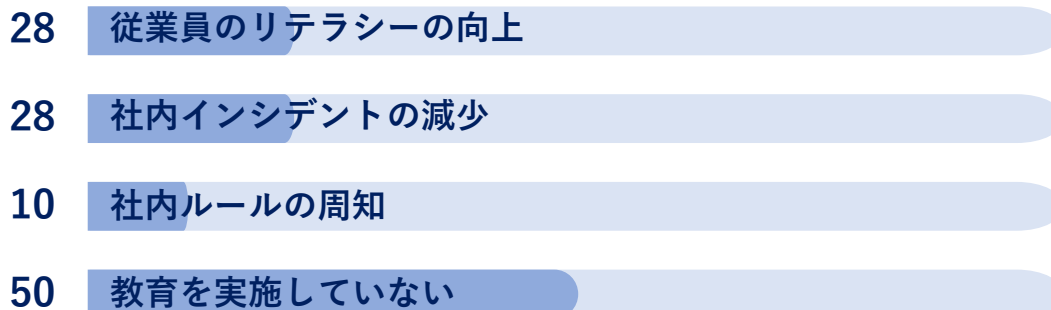
Q17.の従業員への教育を年 3 回以上実施している各種別割合

業種別	(%)
金融・保険業	68.2
建設業	0.0
卸売・小売・飲食業	0.0
サービス業	16.7
製造業	0.0
運輸・通信業	0.0
第一次産業（農業等）	0.0
不動産業	0.0
その他	0.0

従業員数別	(%)
9 名 以下	20.9
10 名～29 名	7.7
30 名～49 名	0.0
50 名～99 名	50.0
100 名～499 名	40.0
500 名～999 名	—
1,000 名 以上	100

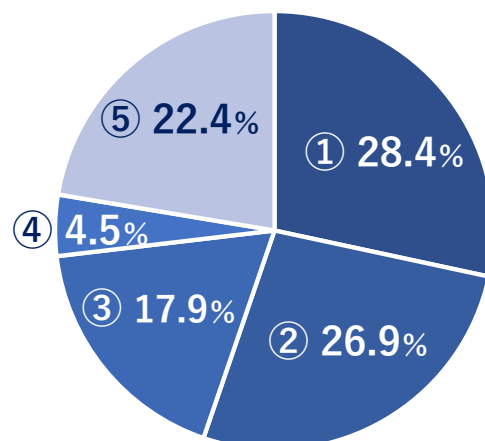
Q17.の教育で得られている効果は何ですか？（複数回答可）

（回答数）



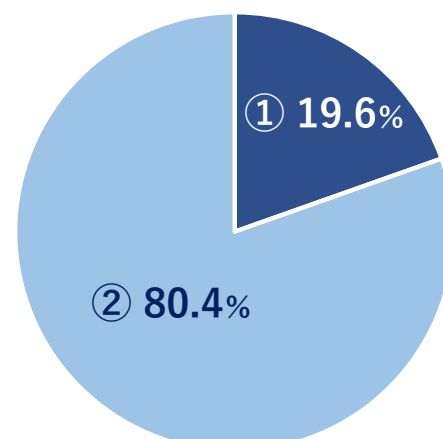
Q17.の教育を実施する上での課題は何ですか？

- ① ■ コンテンツの作成
- ② ■ 教育体制の構築にかかる手間
- ③ ■ 教育の頻度
- ④ ■ その他
- ⑤ ■ 課題は特にない



Q18. 企業向けサイバー保険に加入していますか？

- ① ■ はい
- ② ■ いいえ



Q18.の「はい」の各種別割合

業種別	(%)	従業員数別	(%)
金融・保険業	35.3	9名以下	10.4
建設業	22.0	10名～29名	23.5
卸売・小売・飲食業	14.3	30名～49名	25.0
サービス業	0.0	50名～99名	25.0
製造業	0.0	100名～499名	37.5
運輸・通信業	0.0	500名～999名	—
第一次産業（農業等）	0.0	1,000名以上	50.0
不動産業	50.0		
その他	0.0		

Q18.の保険に加入したきっかけは何ですか？

(%)

- 30 保険会社・保険代理店からの提案
- 20 ニュース等で様々な事件が取り上げられているため
- 20 年々リスクが複雑化しているため
- 15 自社の規模が大きくなり必要性が生じたため
- 05 ヒヤリハットを感じた経験があったため
- 05 周囲の企業が保険に加入していたため
- 05 取引先に対しての信用力を高めるため

Q18.の保険に加入していない理由は何ですか？

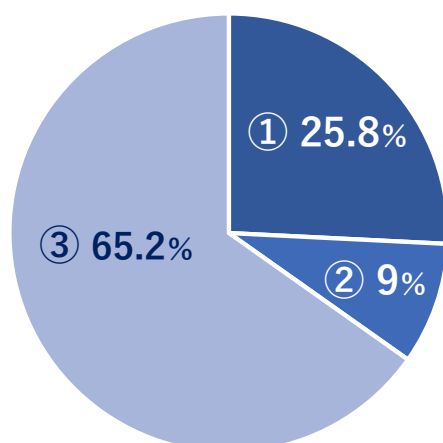
(%)

- 20.2 費用の問題（費用に余裕がない・他事業に比べ優先順位が低い）
- 16.9 サイバー保険の存在を知らなかったため
- 14.6 リスクが発生する可能性が低いと考えているため
- 4.5 リスクによって生じる影響・損失が不明なため
- 4.5 具体的な相談先が分からないため
- 4.5 社内に検討できる担当（専門）の人材がいないため
- 28.1 分からない／特に理由はない
- 6.7 その他

Q18.の保険に加入していない理由の「その他」の理由

- ・ 周囲の企業も加入していないため
- ・ 本社で一括して加入していると思われるため
- ・ 上部機関が決めるため
- ・ 顧客被害に対する保険に加入しているため
- ・ 検討に充てる時間に余裕がないため

Q18.の保険に今後加入する予定はありますか？



- ① ■ 有る
- ② ■ 検討したい
- ③ ■ ない

Q18.の保険に今後加入する予定「有る・検討したい」の各種別割合

業種別

	(%)
金融・保険業	9.5
建設業	29.2
卸売・小売・飲食業	50.0
サービス業	33.3
製造業	70.0
運輸・通信業	50.0
第一次産業（農業等）	33.3
不動産業	0.0
その他	100

従業員数別

	(%)
9名以下	23.3
10名～29名	46.2
30名～49名	55.6
50名～99名	60.0
100名～499名	20.0
500名～999名	—
1,000名以上	0.0