

**CSIJ 共通評価フレームワーク  
(セキュリティ体制版)  
調査結果レポート 速報版**



**サイバーセキュリティイニシアティブジャパン (CSIJ)  
2024年12月13日**

## 目次

1.	本調査の概要 .....	3
2.	調査結果 .....	6
2.1.	カテゴリ別遵守率.....	6
2.1.1.	従業員規模ごとのカテゴリ別遵守率 .....	6
2.1.2.	業界ごとのカテゴリ別遵守率.....	8
2.1.3.	売上高ごとのカテゴリ別遵守率 .....	9
2.1.4.	セキュリティ対策に関する外部レビュー・サービスの利用状況とカテゴリ別遵守率 .....	11
2.2.	遵守率が低い項目 .....	13
2.3.	回答データの注目点.....	14

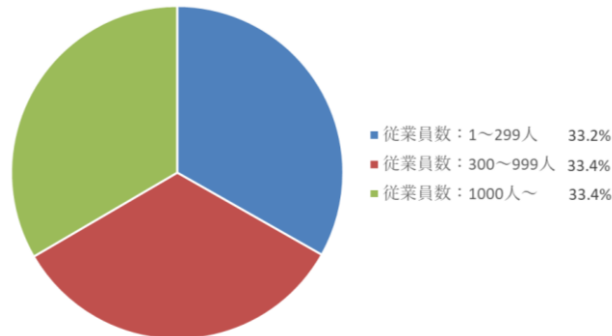
## 1. 本調査の概要

調査目的	企業のセキュリティ体制の現状を把握・分析することを通じて、実施すべきサイバーセキュリティの対策状況を可視化し、日本の組織のセキュリティレベルの底上げを実現すること。
調査手法	インターネット調査
調査対象	過去 3 年以内に、情報システム部門や情報セキュリティ推進部門、リスク管理部門などに在籍した経験があり、情報セキュリティに関するインシデント対応やインシデント対応体制の構築、その他情報セキュリティに関する施策推進に従事した経験がある担当者や意思決定者
調査内容	<p>回答者の属性を調査する設問(13問)と、企業のセキュリティ体制の状況を問う4カテゴリ(※1)の設問(20問)を用いた調査。</p> <p>(※1) &lt;評価カテゴリ&gt;</p> <p>① ガバナンス…自組織のセキュリティを推進する体制の有無やセキュリティの規程について確認するカテゴリ</p> <p>② インシデントレスポンス…インシデント対応の体制や初動から復旧までの対応状況を確認するカテゴリ</p> <p>③ 教育…自組織の従業員に対するセキュリティ教育の実施状況を確認するカテゴリ</p> <p>④ 資産管理…自組織の IT 資産の管理状況を確認するカテゴリ</p>
分析方法	<p>設問に対する自組織の状況を 3 段階 (◎、×、△) で評価した結果を収集する。それぞれの段階に点数を割り当て(※2)、各評価の点数を合計し、その総計を基に全体の合計との割合を算出する(※3)。この割合を「セキュリティ対策遵守率」として表す。(以下、「遵守率」と表記)</p> <p>(※2) &lt;回答と点数の換算&gt;</p> <p>◎…設問内容を実施している。(2点換算)</p> <p>×…設問内容を実施していない。(0点換算)</p> <p>△…◎とも×とも断定できない実施状況である。(1点換算)</p> <p>(※3) &lt;遵守率の算出方法&gt;</p> <p>遵守率…評価による点数の合計/総得点数(単位: %)</p>

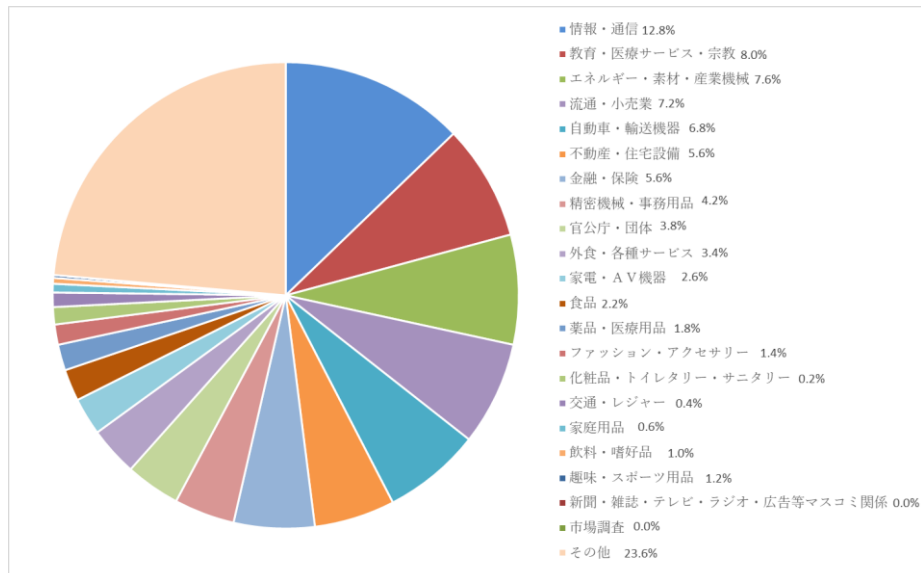
サンプル  
情報

サンプル数：総計 500 サンプル

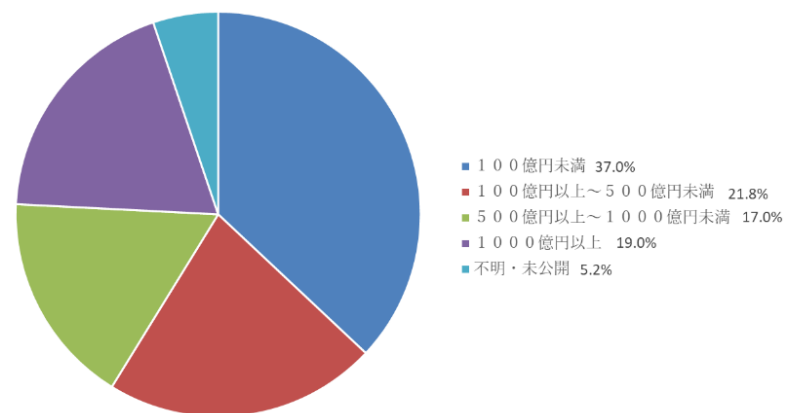
<従業員規模割合>



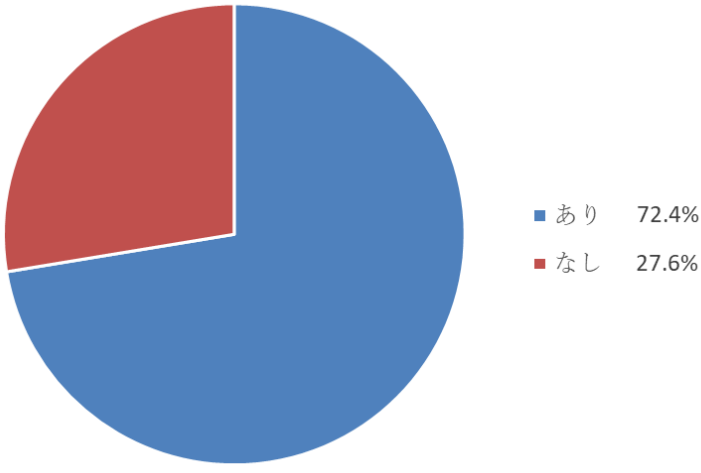
<業界割合>



<売上高割合>



<過去三年以内のセキュリティ対策に関する外部レビュー・サービス利用有無割合>

	 <p>■ あり 72.4% ■ なし 27.6%</p>
調査時期	2024年10月実施
調査主体	サイバーセキュリティイニシアティブジャパン

## 2. 調査結果

### 2.1. カテゴリ別遵守率

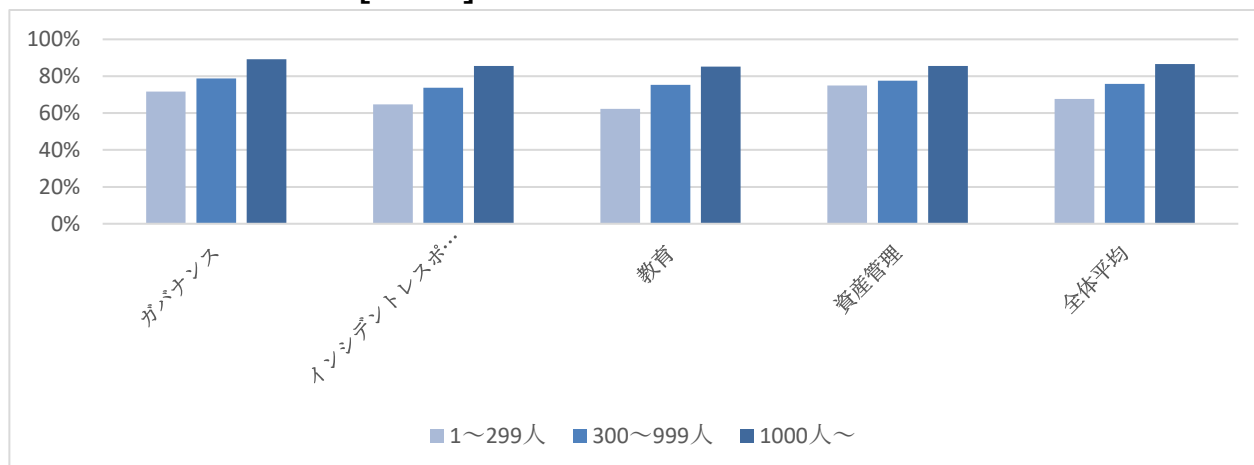
#### 2.1.1. 従業員規模ごとのカテゴリ別遵守率

従業員規模ごとの、カテゴリ別の遵守率を以下に記す。

[表 2.1] 従業員規模ごとのカテゴリ別遵守率

従業員規模	ガバナンス	インシデントレスポンス	教育	資産管理	全体平均
1～299人	71.6%	64.8%	62.3%	75.0%	67.6%
300～999人	78.7%	73.7%	75.3%	77.5%	75.8%
1000人～	89.2%	85.6%	85.2%	85.6%	86.6%
総計	79.9%	74.7%	74.3%	79.4%	76.7%

[図 2.1] カテゴリごとの従業員規模別遵守率グラフ



いずれのカテゴリでも、従業員規模が大きいほど遵守率が高いことが確認できる。特に「インシデントレスポンス」と「教育」のカテゴリにおいて、「1～299人」の企業では遵守率が60%台となっており、他の従業員規模との遵守率の差が見られる。「1000人～」の企業は全てのカテゴリで高い遵守率を示しており、人的リソースの充実が影響していると考えられる。加えて、「資産管理」のカテゴリに関しては、「1～299人」の企業と「300～999人」の企業では遵守率があまり変わらないことから、調査対象の企業は「資産管理」のセキュリティ体制を優先的に整えていることが考えられる。

「ガバナンス」カテゴリの遵守率は全体的に高く、特に「1000人～」の企業で顕著である。一方で、「1～299人」の企業では、他の従業員規模の企業に比べ相対的に遵守率が低い傾向が見られた。

また、「インシデントレスポンス」カテゴリに関しては、従業員規模が大きいほど遵守率が高いことがわかる。「1000人～」の企業ではインシデントレスポンスの体制が整えられているが、「1～299人」の企業では、インシデントレスポンスの体制整備が比較的遅れている可能性がある。

一方、「教育」カテゴリに関しては、他のカテゴリに比べて全体的に低い遵守率を示している。特に「1～299 人」の企業においては、同じ「1～299 人」の「ガバナンス」カテゴリの遵守率である71.6%と比べても、遵守率が62.3%となっており、教育を行う体制が比較的整えられていないと考えられる。

### 2.1.2. 業界ごとのカテゴリ別遵守率

業界ごとの、カテゴリ別の遵守率を以下に記す。

**[表 2.2] 業界ごとのカテゴリ別遵守率**

業界	回答数	ガバナンス	インシデントレス ポンス	教育	資産管理	全体平均
情報・通信	64	83.6%	77.2%	80.1%	88.7%	80.5%
教育・医療サービス・宗教	40	74.4%	62.0%	61.3%	59.4%	65.4%
エネルギー・素材・ 産業機械	38	79.2%	74.1%	78.3%	85.5%	77.2%
流通・小売業	36	82.9%	77.4%	80.6%	79.2%	79.5%
自動車・輸送機器	34	90.4%	83.8%	78.7%	83.1%	85.2%
金融・保険	28	89.0%	88.4%	89.3%	87.5%	88.6%
不動産・住宅設備	28	60.1%	53.4%	53.6%	66.1%	56.7%
精密機械・事務用品	21	89.7%	83.8%	77.4%	86.9%	85.2%
官公庁・団体	19	87.3%	82.6%	77.6%	81.6%	83.4%
外食・各種サービス	17	72.1%	66.5%	63.2%	70.6%	68.2%
家電・AV機器	13	84.6%	82.3%	71.2%	98.1%	83.5%
食品	11	92.4%	80.9%	75.0%	81.8%	83.9%
薬品・医療用品	9	76.9%	80.0%	72.2%	86.1%	78.9%
ファッション・ アクセサリー	7	72.6%	73.6%	82.1%	71.4%	73.9%
化粧品・トイレタリー・サニ タリー	6	68.1%	59.2%	54.2%	70.8%	62.5%
交通・レジャー	5	78.3%	92.0%	70.0%	70.0%	83.5%
家庭用品	3	83.3%	68.3%	83.3%	83.3%	75.8%
飲料・嗜好品	2	54.2%	72.5%	75.0%	75.0%	67.5%
趣味・スポーツ用品	1	100.0%	100.0%	100.0%	100.0%	100.0%
その他	118	76.5%	72.8%	73.7%	77.3%	74.4%
総計	500	79.9%	74.7%	74.3%	79.4%	76.7%

「インシデントレスポンス」カテゴリについては、「不動産・住宅設備」業界や「化粧品・トイレタリー・サニタリー」業界の遵守率が 50%台となっている一方、「交通・レジャー」業界では 90%以上となっている。このように、特に「インシデントレスポンス」と「教育」のカテゴリでは、業界ごとに大きな差が見られる。



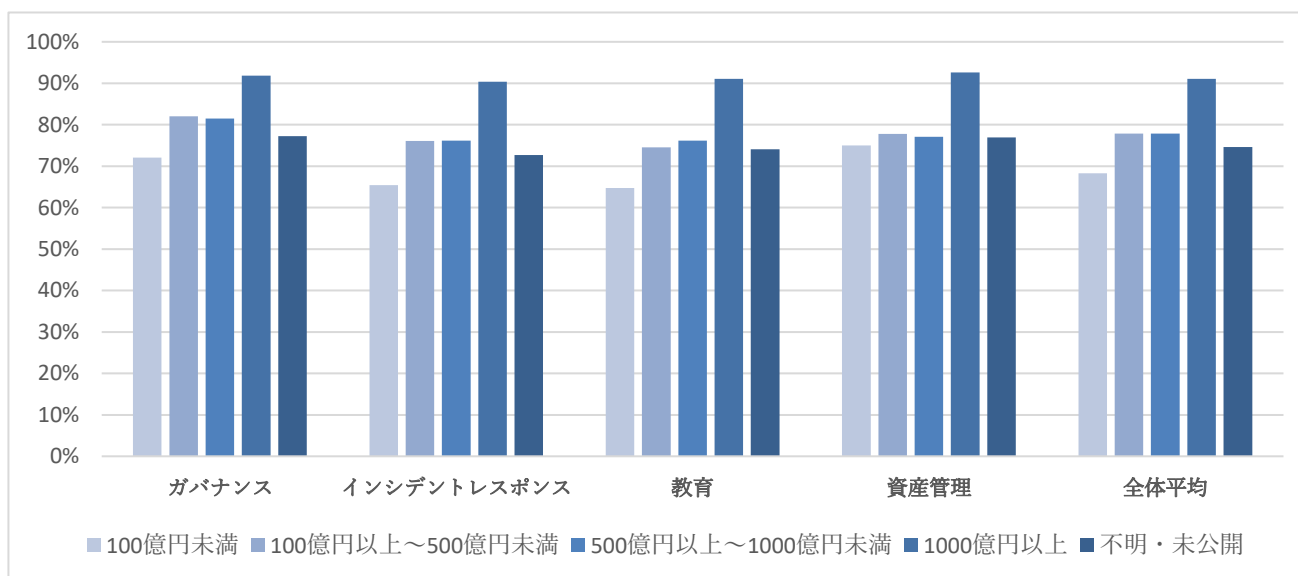
### 2.1.3. 売上高ごとのカテゴリ別遵守率

売上高ごとの、カテゴリ別の遵守率を以下に記す。

**[表 2.3] 売上高ごとのカテゴリ別遵守率**

売上高	ガバナンス	インシデントレスポンス	教育	資産管理	全体平均
100 億円未満	72.1%	65.4%	64.7%	75.0%	68.3%
100 億円以上～500 億円未満	82.0%	76.1%	74.5%	77.8%	77.9%
500 億円以上～1000 億円未満	81.5%	76.2%	76.2%	77.1%	77.9%
1000 億円以上	91.8%	90.4%	91.1%	92.6%	91.1%
不明・未公開	77.2%	72.7%	74.0%	76.9%	74.6%
総計	79.9%	74.7%	74.3%	79.4%	76.7%

**[図 2.2] カテゴリごとの売上高別遵守率グラフ**



「全体平均」を見ると、売上高が大きいほど遵守率が高いことが確認できる。特に、「1000 億円以上」の企業は全カテゴリにおいて 90%を超える高い遵守率を示しているが、「100 億円未満」の企業は 60%台の遵守率となっているカテゴリもある。また、「100 億円以上～500 億円未満」の企業と「500 億円以上～1000 億円未満の企業」では全体的に遵守率がほとんど変わらないことも特徴的である。

一方、「資産管理」カテゴリに関しては異なる特徴がある。「1000 億円以上」の企業では遵守率が 92.6%と非常に高いが、それ以外の売上高の企業では 75.0%から 78.1%と、比較的均

一な遵守率が見られる。このことから、資産管理については「1000 億円以上」の企業が突出して高い遵守率を示している一方で、その他の企業はほぼ同様の遵守率を維持していることがわかる。

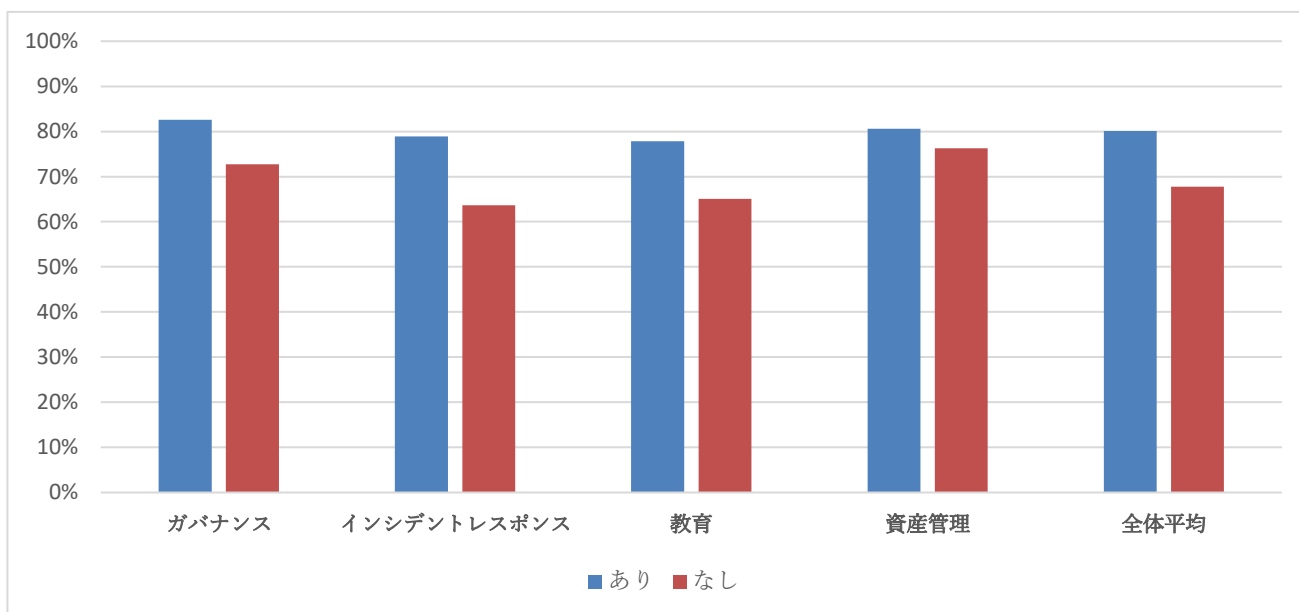
#### 2.1.4. セキュリティ対策に関する外部レビュー・サービスの利用状況とカテゴリ別遵守率

インシデント対応体制の整備にあたり、外部の専門家によるセキュリティ対策に関するレビューやサービス（例えばコンサルティングサービス等）を過去3年以内に利用したか否かの、カテゴリ別の遵守率を以下に記す。

**[表 2.4] セキュリティ対策に関する外部レビュー・サービスの過去3年以内の利用状況とカテゴリ別遵守率**

レビュー・サービスの利用有無	ガバナンス	インシデントレスポンス	教育	資産管理	全体平均
「あり」と回答した企業の平均遵守率	82.6%	78.9%	77.8%	80.6%	80.1%
「なし」と回答した企業の平均遵守率	72.8%	63.6%	65.0%	76.3%	67.8%
総計	79.9%	74.7%	74.3%	79.4%	76.7%

**[図 2.3] カテゴリごとの外部レビュー・サービスの利用状況別遵守率**



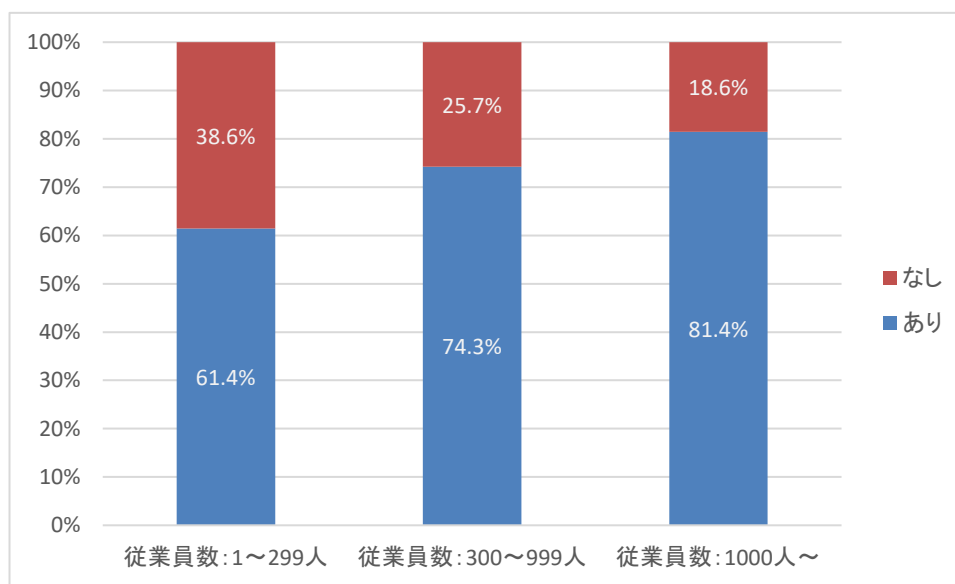
「全体平均」を見ると、「外部レビュー・サービスを利用している」企業は 80.1%と高い遵守率を示しているのに対し、「利用していない」企業は 67.8%と低い遵守率を示している。特に、「インシデントレスポンス」と「教育」のカテゴリでは、遵守率に顕著な差が見られる。

さらに、企業規模別で同様に比較した結果を以下に記す。

**【表 2.5】 従業員規模とセキュリティ対策に関する  
外部レビュー・サービスの過去3年以内の利用状況**

従業員規模	あり	なし
1～299人	61.4%	38.6%
300～999人	74.3%	25.7%
1000人～	81.4%	18.6%
総計	72.4%	27.6%

**【図 2.4】 従業員規模とセキュリティ対策に関する  
外部レビュー・サービスの過去3年以内の利用状況割合**



従業員規模が大きくなるほど、外部レビュー・サービスの利用率が高くなる傾向が見られる。前述のとおり、従業員規模が大きいほど遵守率が高い傾向が見られるほか、外部レビュー・サービスの利用状況とカテゴリ別遵守率にも相関があるとみられるため、外部レビュー・サービスの利用が遵守率の向上に寄与していると推測される。

## 2.2. 遵守率が低い項目

各セキュリティ対策の遵守率について順位を付けた。以下にワースト 1 位から 10 位までを記す。

**[表 2.6] 遵守率が低いセキュリティ対策項目**

ワースト	カテゴリ	設問 No.	設問	遵守率
1	インシデントレスポンス	設問 15	サイバー攻撃被害／セキュリティ事故対応の訓練を定期的実施していますか。具体的には、最低年一回、机上訓練・手順書の読み合わせ等を通して、サイバー攻撃被害／セキュリティ事故対応手順の検証および改善を行っていますか。	69.6%
2	インシデントレスポンス	設問 13	サイバー攻撃被害／セキュリティ事故発生時に、行政機関や関連団体、マスコミ等への対外連絡を行う手順、フローなどを定めていますか。	70.0%
3	インシデントレスポンス	設問 11	複数箇所ですべてサイバー攻撃被害が同時に発生した場合に、どのサーバ・システムから優先して復旧対応する等、判断するための基準が定められていますか。	72.3%
4	教育	設問 18	セキュリティ管理者に対して、外部組織の教育サービス等でセキュリティ教育を実施していますか。	72.8%
5	ガバナンス	設問 6	B C P（事業継続計画）を定めていますか。	72.9%
6	インシデントレスポンス	設問 9	サイバー攻撃被害／セキュリティ事故対応について、内部で対応できる体制がありますか。（人・モノ）	74.9%
7	インシデントレスポンス	設問 10	サイバー攻撃被害／セキュリティ事故が発生した際に、報告を受け付ける窓口等の連絡先はありますか。	75.4%
8	教育	設問 17	従業員のセキュリティ意識の向上のために、セキュリティに関する教育や社内のセキュリティ関連ルールを周知し、習熟度を確認していますか。	75.8%
9	インシデントレスポンス	設問 16	サイバー攻撃で被害を受けたシステムを復旧するための事前対策が取られていますか。対策としては例えば以下のようなものがあげられます。・復旧手順（復旧優先順位等）・バックアップの取得	76.1%
10	インシデントレスポンス	設問 7	インシデント（サイバー攻撃被害／セキュリティ事故）管理・連携する人がいますか。	76.4%

まず、「インシデントレスポンス」カテゴリに属する設問が多く含まれており、全体的に遵守率が低い傾向が見られる。例えば、設問 15（「サイバー攻撃被害／セキュリティ事故対応の訓練を定期的実施していますか。」）は 69.6%、設問 13（「サイバー攻撃被害／セキュリティ事故発生時に、行政機関や関連団体、マスコミ等への対外連絡を行う手順、フローなどを定めていますか。」）は 70.0%と低い遵守率を示している。

また、「教育」カテゴリに関しては、2 つの設問の両方が遵守率の低いセキュリティ項目に含まれている。設問 18（「セキュリティ管理者に対して、外部組織の教育サービス等でセキュリティ教育を実施していますか。」）が 72.8%、設問 17（「従業員のセキュリティ意識の向上のために、セキュリティに関する教育や社内のセキュリティ関連ルールを周知し、習熟度を確認していますか。」）が 75.8%の遵守率を示している。これらの項目から、従業員のセキュリティ意識向上に対する体制の整備が比較的高いことがわかるが、セキュリティに関しては人による対応が重要であるため、100%を目指してさらなる取り組みが必要だと考えられる。

### 2.3. 回答データの注目点

その他、得られた回答データから注目した点を以下に記載する。

- ・ 過去3年以内にインシデント対応体制の整備にあたり、セキュリティ対策に関する外部の専門家によるレビューやサービスを利用したことがある企業が72.4%と過半数を超えている。
- ・ サイバー攻撃被害／セキュリティ事故発生時に、行政機関や関連団体、マスコミ等への対外連絡を行う手順、フローなどを定める設問と、サイバー攻撃被害／セキュリティ事故対応の訓練を定期的実施する設問の2つが、今回の調査項目の中で最も「◎」（実施している）と回答した企業の割合が少ない設問だった。しかしその割合は61.6%であり、過半数を超えている。

今後は、これらの調査結果を更に詳細に分析し、随時結果を報告する。

■ **本調査結果レポート作成者（敬称略、五十音順）**

作成者	所属企業
足立 道拓 上田 直哉 山口 雅史	NRI セキュアテクノロジーズ株式会社
小関 直樹 刀川 郁也	エムオーテックス株式会社
西野 哲生	グローバルセキュリティエキスパート株式会社
小淵 慈英 仲上 竜太 安田 良明	ニューリジエンセキュリティ株式会社
持田 啓司（CSIJ 事務局長） 奥野 康城（評価分科会代表） 秋山 真菜 岡本 大輝 田中 伶佳 谷口 諒之介 藤原 青空	株式会社ラック

■ **CSIJ 入会案内**

本調査等への参加は、CSIJ 入会により可能となります。

入会のご検討をいただけますと幸いです。

<https://www.csi-japan.org/join>

■ **本調査結果レポートに関するお問合せ先（制作・著作）**

サイバーセキュリティイニシアティブジャパン（CSIJ）

東京都千代田区平河町 2 丁目 16 番 1 号 平河町森タワー

E-Mail : [sec@csi-japan.org](mailto:sec@csi-japan.org)

URL : <https://www.csi-japan.org/>

