

**CSIJ 共通評価フレームワーク
(サプライチェーンリスク版)
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）
2025 年 12 月 19 日**

目次

1.	本調査の概要	3
2.	調査結果	5
2.1.	カテゴリ別遵守率	5
2.1.1.	従業員規模ごとのカテゴリ別遵守率	5
2.1.2.	業界ごとのカテゴリ別遵守率	6
2.1.3.	売上高ごとのカテゴリ別遵守率	7
2.1.4.	サプライチェーン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 ...	8
2.2.	遵守率が低い項目	10
2.3.	回答データの注目点	11

1. 本調査の概要

調査目的	企業のサプライチェーンリスクに対するセキュリティ体制の現状を把握・分析することで、サイバーセキュリティの対策状況を可視化し、国内組織のセキュリティレベルを底上げすること。
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（またはそれに該当する部門）に在籍した経験があり、委託先の選定/評価/管理や、委託先のセキュリティ要件定義/評価/監査/運用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(11 問)と、企業のセキュリティ体制の状況を問う 3 カテゴリー(※1)の設問(30 問)を用いた調査。</p> <p>(※1)＜評価カテゴリ＞</p> <ul style="list-style-type: none"> ・ガバナンス ・インシデントレスポンス ・サプライチェーンマネジメント
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)＜回答と点数の換算＞</p> <ul style="list-style-type: none"> ◎…設問内容を実施している。(2 点換算) ×…設問内容を実施していない。(0 点換算) △…◎とも×とも断定できない実施状況である。(1 点換算) <p>(※3)＜遵守率の算出方法＞</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 1200 サンプル

<従業員規模割合>

従業員規模	回答数	%
1~299 人	400	33.3
300~999 人	400	33.3
1000 人~	400	33.3

<業界割合>

業界	回答数	%
製造業	303	25.3
サービス	205	17.1
情報処理	177	14.8
小売・流通	134	11.2
建設不動産	89	7.4
金融	78	6.5
インフラ	61	5.1
その他	153	12.8

<売上高割合>

売上高	回答数	%
100 億円未満	457	38.1
100 億円以上~500 億円未満	315	26.3
500 億円以上~1000 億円未満	157	13.1
1000 億円以上	221	18.4
わからない	50	4.2

調査時期 2025 年 6 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

本調査は、以下の3カテゴリに基づいて分析する。

<評価カテゴリ>

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

インシデントレスポンス…インシデント対応体制や、初動から復旧までの対応状況について

サプライチェーンマネジメント…委託先企業に対するセキュリティ対策の実施状況について

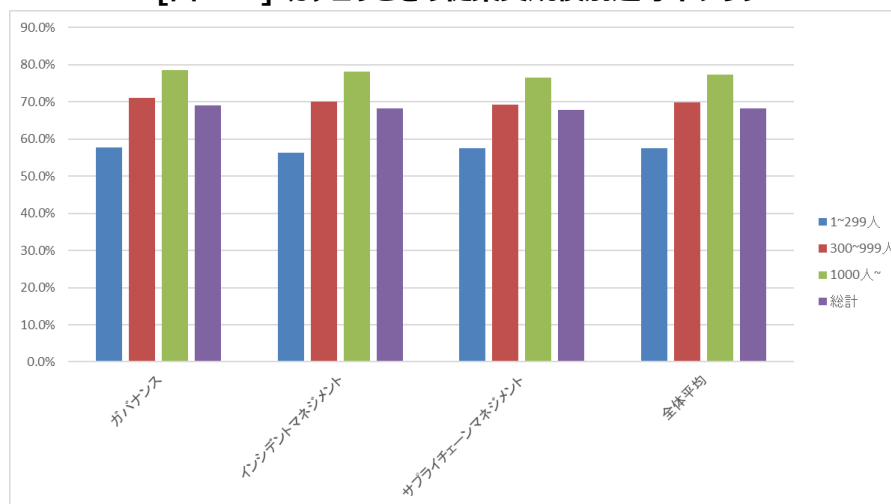
2.1.1. 従業員規模ごとのカテゴリ別遵守率

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 マネジメント	サプライチェーン マネジメント	全体平均
1～299 人	57.7%	56.3%	57.6%	57.5%
300～999 人	71.0%	70.1%	69.3%	69.8%
1000 人～	78.5%	78.1%	76.6%	77.2%
総計	69.1%	68.2%	67.8%	68.2%

[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、従業員数が大きくなるほど遵守率が高まる傾向が見られる。特に「1～299 人」と「1000 人～」を比較すると、全てのカテゴリで遵守率に 20%前後の差があり、「1000 人以上」の企業ではすべてのカテゴリで 75%以上の遵守率を示している。大企業がセキュリティ対策をより充実させられる背景には、人的リソースの豊富さに加え、情報セキュリティを専任で対応する部門や責任者の配置、運用体制が確立されていることが大きな要因として挙げられる。

また、従業員規模が「1～299 人」と「300～999 人」の間では、遵守率が大きく伸びる傾向が見られた。一般的には企業規模が拡大するにつれて、より体系的かつ形式的な情報セキュリティ管理体制が求められるとされており、これが理由で遵守率の差が開いていると推察される。

サプライチェーンリスクに関するガバナンスが確立できている企業では、それに則ってインシデントレスポンスやサプライチェーンマネジメントもほぼ確立できている。一方で、「インシデントレスポンス」や「サプライチェーンマネジメント」は、「ガバナンス」と比べ専門チームの設置や検知・対応手順の演習、外部ベンダー評価・監査、契約管理やモニタリング体制の構築といった多くの工数が求められるため、全社展開されにくく、遵守率が若干低く留まっていると考えられる。

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	サプライチェーンマネジメント	全体平均
金融	78	78.1%	76.7%	77.4%	77.5%
情報処理	177	69.8%	69.4%	71.4%	70.8%
サービス	205	68.5%	66.3%	68.0%	67.9%
小売、流通	134	69.6%	69.5%	66.1%	67.4%
製造業	303	68.9%	68.3%	66.3%	67.2%
建設不動産	89	65.3%	65.5%	65.5%	65.5%
インフラ	61	66.6%	64.5%	64.4%	65.0%
その他	153	67.5%	66.8%	65.7%	66.3%
総計	1200	69.1%	68.2%	67.8%	68.2%

金融業界は「ガバナンス」の遵守率が 78.1%と、全体平均（68.2%）を約 10 ポイント上回り、業界間で最も高い結果となっている。一方で、「インシデントレスポンス」は 76.7%、「サプライチェーンマネジメント」は 77.4%と、いずれも全体平均を 10 ポイント以上上回っているものの、「ガバナンス」比では約 1～2 ポイント低く、比較して若干の対策漏れがうかがえる。この傾向は金融業界にとどまらず他分野でも見られるが、情報処理業界および建設・不動産業界においては異なり、業界内カテゴリ別で「サプライチェーンマネジメント」の遵守率が最も高く、「ガバナンス」や「インシデントレスポンス」を上回っている。これは、情報処理業界ではクラウドサービスやアウトソーシング、パッケージソフトの導入など外部事業者との連携を前提としたビジネスモデルが主流であり、建設・不動産業界では多段階の下請け構造を通じた資材調達や作業者管理といったサプライチェーンが極めて複雑であることから、特にサプライチェーンマネジメントが重要視されているからと考えられる。

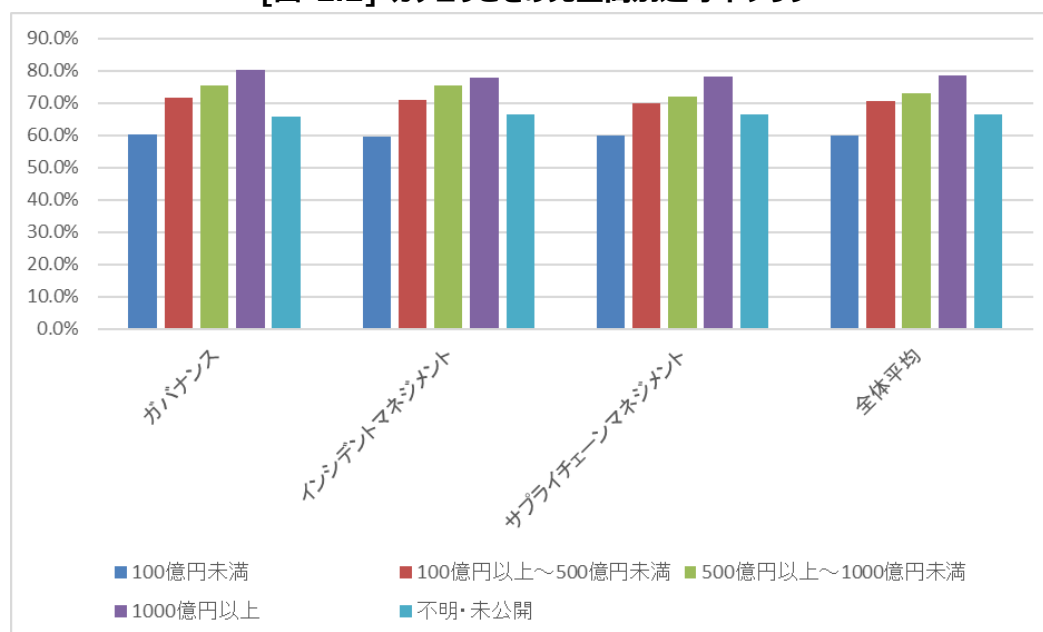
2.1.3. 売上高ごとのカテゴリ別遵守率

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	サプライチェーンマネジメント	全体平均
100 億円未満	60.2%	59.5%	60.0%	60.0%
100 億円以上～500 億円未満	71.5%	70.8%	69.9%	70.4%
500 億円以上～1000 億円未満	75.3%	75.4%	71.9%	73.2%
1000 億円以上	80.1%	77.8%	78.3%	78.7%
不明・未公開	65.9%	66.3%	66.5%	66.3%
総計	69.1%	68.2%	67.8%	68.2%

【図 2.2】 カテゴリごとの売上高別遵守率グラフ



従業員数と同様に、売上規模が大きくなるほど各カテゴリの遵守率は上昇傾向にあり、「ガバナンス」の遵守率はおおよそ 1～2 ポイント高い遵守率を示している。「ガバナンス」と「インシデントマネジメント」の両カテゴリでは、「100 億円未満」と「100 億円以上～500 億円未満」の間に最も大きな増加が見られる。

また、「サプライチェーンマネジメント」では、「100 億円未満」・「100 億円以上～500 億円未満」間に大きな伸びが確認できるが、「500 億円以上～1000 億円未満」と「1000 億円以

上」の間にも再び顕著な増加が観測され、さらなる規模拡大後の体制整備が加速をみせていることがうかがえる。全体として、ガバナンスがわずかに他領域を上回るものの、「インシデントマネジメント」と「サプライチェーンマネジメント」も売上規模に応じて着実に遵守率を高めており、特に中小規模から中堅規模からの各カテゴリに対する体制強化が大きく進んでいることが示唆できる。

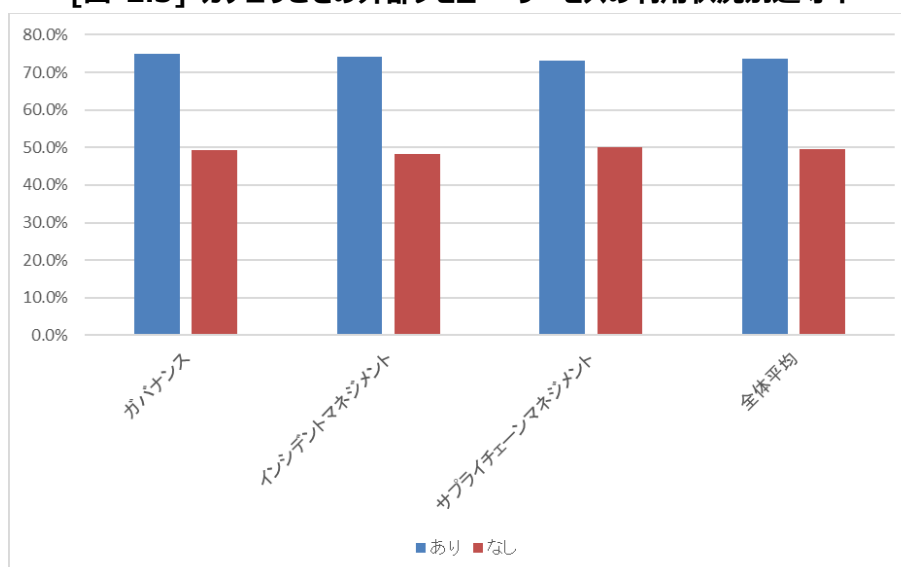
2.1.4. サプライチェーンリスクの評価や対策に関する外部レビュー・サービスの利用状況とカテゴリ別遵守率

サプライチェーンリスクの評価や対策にあたり、外部の専門家によ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	サプライチェーン マネジメント	全体平均
「あり」と回答した 企業の平均遵守率	74.1%	73.0%	73.6%	74.1%
「なし」と回答した 企業の平均遵守率	48.2%	50.1%	49.6%	48.2%
総計	68.2%	67.8%	68.2%	68.2%

[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



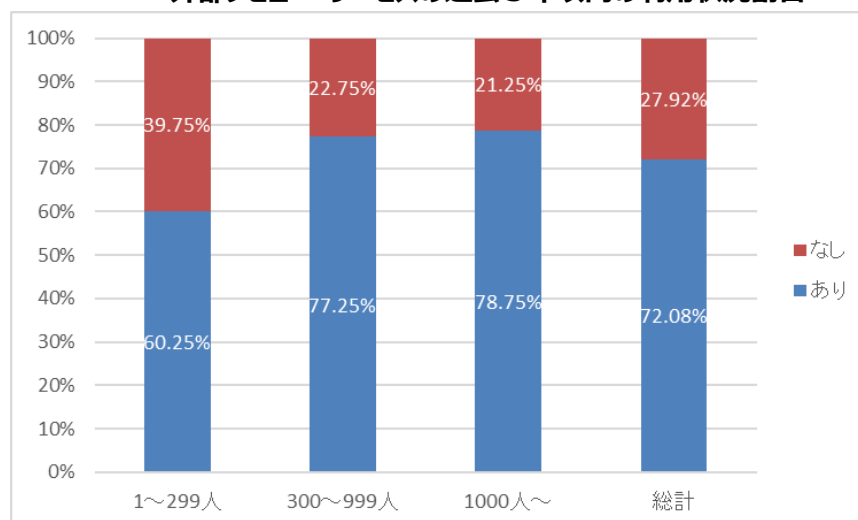
外部レビュー・サービスを過去3年以内に利用した企業は、「ガバナンス」で74.1%、「インシデントレスポンス」で73.0%、「サプライチェーンマネジメント」で73.6%と、いずれの領域でも約73～74%の高い遵守率を示している。一方、利用していない企業は「ガバナンス」48.2%、「インシデントレスポンス」50.1%、「サプライチェーンマネジメント」49.6%にとどまり、両者の差はいずれのカテゴリでも約24～26ポイントに達している。全体平均で見ると、「利用あり」の企業が74.1%、「利用なし」の企業が48.2%で、その差は25.9ポイントとなっており、外部レビュー・サービスの活用がセキュリティ対策の制度・運用面において一貫して大きな効果をもたらしていることがうかがえる。

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	60.25%	39.75%
300～999 人	77.25%	22.75%
1000 人～	78.75%	21.25%
総計	72.08%	27.92%

**【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考えられる。

2.2. 遵守率が低い項目

各セキュリティ対策の遵守率が特に遵守率が低い項目は以下の通りである。

[表 2.6] 遵守率が低いセキュリティ対策項目

順位	カテゴリ	設問 No.	設問	遵守率
1	サプライチェーン マネジメント	設問 27	委託先企業に対し、必要に応じてサイバー保険への加入を推奨していますか。	58.4%
2	サプライチェーン マネジメント	設問 16	委託先企業の選定にあたり、委託先企業が ISMS 等のセキュリティマネジメント認証を取得していることを確認していますか。	63.0%
3	サプライチェーン マネジメント	設問 17	委託先企業の選定にあたり、コストや体制、技術力のみでなく、環境リスク、地政学リスク及び経済リスクの影響を考慮していますか。	64.2%
4	サプライチェーン マネジメント	設問 26	業務委託終了時には、委託先企業に対し、自社（委託元企業）から提供した情報等を確実に返却又は廃棄を促していますか。	66.3%
5	インシデントレス ポンス	設問 13	グループ企業や委託先企業でのインシデントに対し、再発防止策の策定及び必要に応じて対策計画の策定を実施していることを確認していますか。	66.4%
6	ガバナンス	設問 5	サプライチェーンリスクについて、自社の対応方針および対応計画を定めていますか。	66.9%
7	ガバナンス	設問 9	自社の従業員に対して、業務委託に関するルールを周知し、教育していますか。	67.3%
8	サプライチェーン マネジメント	設問 25	業務委託契約において合意した情報セキュリティ対策について、委託先企業が遵守し実施していることを、定期的なセキュリティチェックや立入り監査等によって確認していますか。また、問題があった場合には是正を促していますか。	67.6%
9	サプライチェーン マネジメント	設問 20	業務委託契約を更新する際には、委託先評価やリスク評価を再度実施し、その結果に基づいて委託先企業に求めるセキュリティ対策を見直していますか。	67.8%
10	サプライチェーン マネジメント	設問 18	業務委託契約の締結にあたり、委託先企業に求める情報セキュリティ対策を明文化し、その実施について双方で合意していますか。	68.3%

遵守率の最も低い 10 項目のうち、「サプライチェーンマネジメント」に関する設問が半数以上を占めている。特に、委託先企業への保険加入推奨（設問 27：58.4%）、ISMS 等認証取得状況の確認（設問 16：63.0%）、委託先選定時の多面的リスク評価（設問 17：64.2%）など、外部委託先との関係構築・契約管理における取り組み不足が浮き彫りとなっている。また、業務委託終了時の情報返却・廃棄（設問 26：66.3%）、委託先のセキュリティ対策運用状況チェック（設問 25：67.6%）、契約更新時の再評価と要件見直し（設問

20：67.8%）など、ビジネスサイクル全体を通じた管理プロセス強化が求められている。

「ガバナンス」の全体的な遵守率は比較すると平均より高いものの、設問 5「サプライチェーンリスクに関する対応方針および対応計画の策定」（66.9%）と設問 9「従業員への業務委託ルール周知・教育」（67.3%）が上位に入っている。これはガバナンス体制自体は整いつつあるが、外部連携や現場教育の具体的な運用・定着に課題が残されていることを示している。

2.3. 回答データの注目点

今回の調査で、従業員数・売上規模が最も小さい企業を底上げすることが、サプライチェーン全体の遵守率を最も効果的に向上させることが分かった。また、外部レビューの有無を示すグラフと、従業員数・売上規模別のグラフの形状が類似していることに加え、外部レビューの有無が平均で 25 ポイントもの差を生じさせている点から、外部レビューの影響は極めて大きいと考えられる。

本レポートの次のステップとして、外部レビューの有無でデータをセグメント化し、改めて精緻に分析することで、外部レビュー以外の要因が遵守率に与える影響やトレンドも明らかになる可能性がある。より詳細に分析を行ったレポートを今後掲載する予定である。

■ **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 道拡 上田 直哉 鈴木 伸 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
出本 圭介 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
持田 啓司（CSIJ 事務局長） 谷口 諒之介（評価分科会リーダー） 岡本 勝仁 岡本 大輝 秋山 真菜 奥野 康城 田中 伶佳 杉村 駿 中野 華穂 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

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

