CSIJ 共通評価フレームワーク
（OT 版）
アンケート調査結果レポート
「2025 年度　一般公開版」

※本レポートは一般公開用として
調査のポイントのみを公開しています。
入会するとレポート全文をお読みいただけます。

サイバーセキュリティイニシアティブジャパン（CSIJ）
2025 年 10 月 3 日

目次

1. 本調査の概要

1.1. 調査目的

CSIJ 共通評価フレームワーク(OT 版)を活用し、企業のセキュリティ対策状況の現状を把握・分析する。製造業のセキュリティ対策の現状を把握・分析し、OT に関するセキュリティ対策状況を可視化し、企業の課題に対する対策を提言することで、日本の組織のセキュリティレベル向上を目指す。

1.2. 調査対象

工場やプラントなどの制御システムにおいて、セキュリティ対策の企画・実施判断や管理・運用に携わった経験がある担当者および意思決定者

1.3. 調査方法

「1.2. 調査対象」の範囲となる担当者や意思決定者を対象に、CSIJ 共通フレームワーク(OT 版)を活用したアンケート調査を実施した。

なお、調査方法の詳細については本レポートの末尾に記載している。

2. 総評

本調査では、企業の基本的なセキュリティ対策を「ガバナンス」、「インシデントレスポンス」、「テクノロジー&オペレーション」、「データ保護」の 4 カテゴリに分類し、それぞれの対策状況について調査を実施した。CSIJ によるアンケートの回答結果を基に、各カテゴリの遵守率および相関係数を算出した。その分析によって特に注目すべき点が以下の通りとなる。

1 OT 領域における対策の難しさ

CSIJ にて公開したクラウド版、セキュリティ体制版と比較し、類似するカテゴリいずれも遵守率が下回る結果となった。特にインシデントレスポンスは 61.2%と最も遵守率が低く、サイバー攻撃による機械の災害等への備えや連絡体制など、工場特有の特性があることに起因すると考えられる。

2 ガバナンス

相関分析において、特に人材育成との遵守率との関係性が強いことが明らかになった。ガバナンスの強化が教育や人材の成熟度向上に繋がると言えるだろう。サイバーセキュリティフレームワーク 2.0 において、ガバナンスは他のカテゴリをどのように実装するかを示す役割を持つとされている（※1）。そのため、OT 領域においても、ガバナンスの強化が他カテゴリの遵守率も向上する第一歩ではないだろうか。

※1 サイバーセキュリティフレームワーク（CSF） 2.0
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.jpn.pdf

3 OT 環境における外部連携の重要性

相関分析において、脆弱性対応に関連する設問群の間で強い相関が見られ、情報収集から適用・管理までの一連のプロセスが強く結びついて進められていることを示していた。 一方で、外部委託の選定・管理基準に関する設問の遵守率は 62.0%と全項目の中で 3 番目に低く、外部依存の大きい OT 環境における課題の一端を示している。
OT 環境では、制御システムに関わる技術や製品はベンダー依存度が高く、外部との協力が不可欠であると考える。よって、セキュリティベンダーや保守ベンダーと密に連携を取り、脆弱性情報の入手や、適用管理の体制を整備することが重要であると考えられる。

以上の結果から、 IT と比較すると OT 特有の性質により、対策が進んでいない企業が多いことが分かった。また、ガバナンスを強化することで、技術的対策やインシデント体制の強化に結び付くと推察されることから、OT 環境においては、ガバナンスから優先的に着手することで、着実に遵守率が向上するのではないだろうか。今後、CSIJ としては、こうした状況を踏まえ、企業規模や業界特性に応じて現実的に取り組める改善の方向性を提示し、各企業が一歩ずつ体制を強化できるよう支援していきたい。

3. 調査分析結果

3.1. カテゴリ別遵守率分析

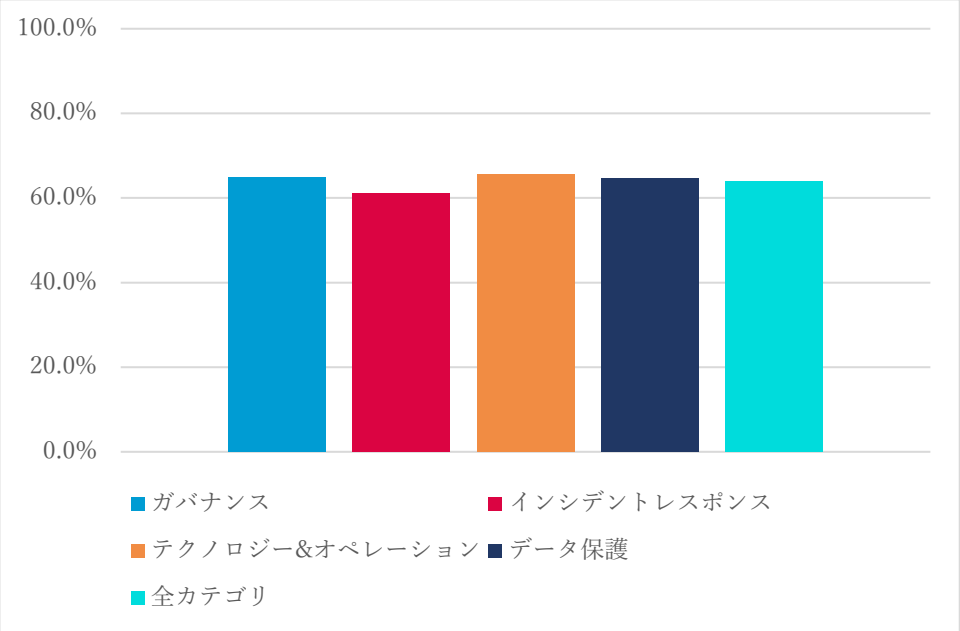
3.1.1. 全体のカテゴリ別遵守率分析

全体の遵守率を以下の表に示す。

[表 3.1.1] 全体のカテゴリ別遵守率

ガバナンス	インシデント レスポンス	テクノロジー & オペレーション	データ保護	全カテゴリ
64.8%	61.2%	65.7%	64.6%	64.0%

[図 3.1.1] 全体のカテゴリ別遵守率グラフ



本調査の全体平均遵守率は 64.0%であった。設問はいずれも OT を運用する企業が最低限取り組むべき対策を問うものだが、理想的な 100%には遠い状況となっている。

カテゴリ別にみると、「テクノロジー&オペレーション」カテゴリの遵守率が 65.7%で最も高く、「インシデントレスポンス」が 61.2%と最も低い。ただし両者の差は 4.5%であり、全体としては 4 カテゴリがほぼ横並びの水準にある。

このようにカテゴリごとに大きな差が生じていない背景には、法規制や取引先からの要求、ベンダーが提供するパッケージサービスの普及などにより、特定分野だけが先行するのではなく、全体的な底上げが進んでいることが一因と考えられる。

一方で、「インシデントレスポンス」カテゴリの遵守率はやや低い水準にとどまっており、引き続き重点的な強化が求められる領域である。

また、以下は過去に回答を収集した、「クラウド版」「セキュリティ体制版」の全体平均遵守率である。

[表 3.1.2] クラウド版のカテゴリ別遵守率

ガバナンス	インシデントレスポンス	コンプライアンス	設定・脆弱性管理	認証・アカウント管理	データ保護・通信保護	全体平均
68.3%	66.4%	67.8%	66.8%	69.3%	66.8%	67.6%

[表 3.1.3] セキュリティ体制版のカテゴリ別遵守率

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
79.9%	74.7%	74.3%	79.4%	76.7%

上記と OT 版の結果を比較すると、OT 領域の遵守率が最も低く、対策の取りづらい領域であるということが考えられる。また、全体平均の遵守率について、クラウド版とは 3.6 ポイントの差であり、一方でセキュリティ体制版とは、13.7 ポイントと大きな差があることから、技術対策を含む領域の対策は比較的、対策が進みづらい状況にあると推測される。

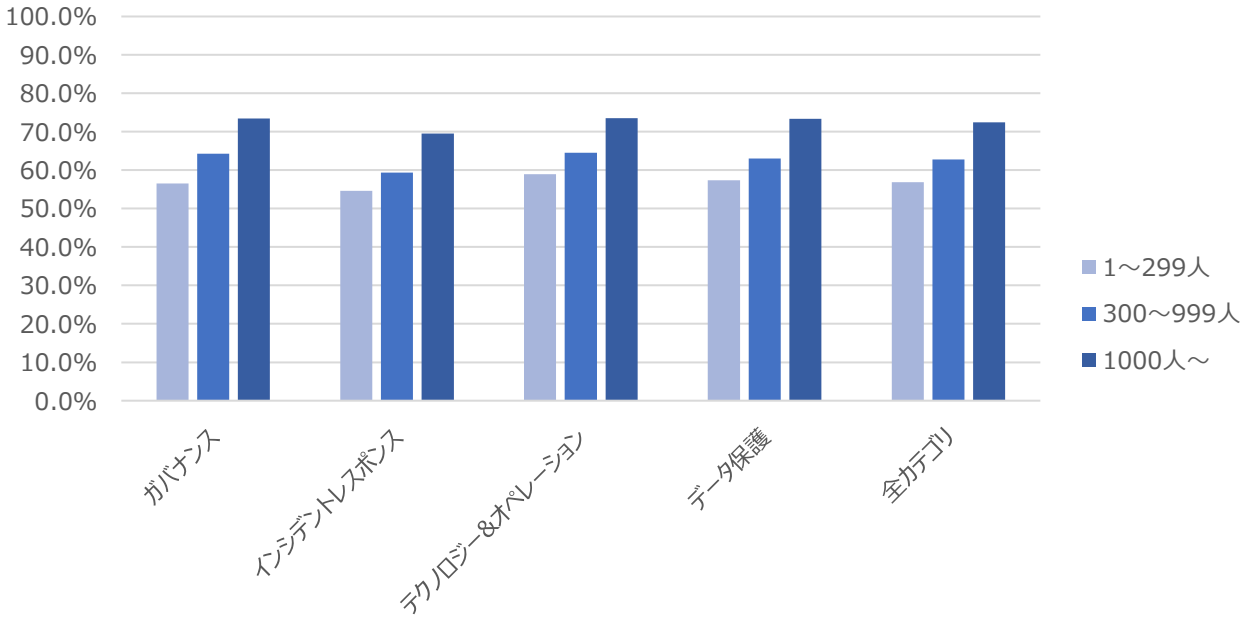
3.1.2. 従業員規模ごとのカテゴリ別遵守率

従業員規模ごとのカテゴリ別遵守率を以下の表に示す。

[表 3.1.4] 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	テクノロジー&オペレーション	データ保護	全カテゴリ
1～299 人	56.5%	54.6%	58.9%	57.4%	56.9%
300～999 人	64.3%	59.4%	64.5%	63.0%	62.8%
1000 人～	73.5%	69.5%	73.6%	73.4%	72.5%
総計	64.8%	61.2%	65.7%	64.6%	64.0%

[図 3.1.2] カテゴリごとの従業員規模別遵守率グラフ



従業員規模別に平均遵守率を比較すると、「1～299 人」の小規模企業は 56.9%、「300～999 人」の中規模企業は 62.8%、「1000 人以上」の大規模企業は 72.5%となり、規模の拡大に伴い数値が上昇した。大規模企業は各カテゴリでおおむね 70%前後を達成しているのに対し、小規模企業はいずれのカテゴリも 50%台にとどまり、規模による取組度合いの差が顕著である。

カテゴリ別にみても、いずれのカテゴリでも従業員規模が大きくなるほど遵守率が高まる傾向がみられる。これは、規模の拡大に伴いリソースや体制が充実し、専門人材の確保や全社的なセキュリティ推進力の強化が図られているため、全カテゴリでの取り組み度合いの底上げにつながっていると考えられる。

一方で、「インシデントレスポンス」は他カテゴリと比較して全体的に遵守率が低い水準で推移している。その主な要因としては、初動対応の標準化や継続的な訓練体制の整備など、専門的知識やリソースが必要となる点が挙げられる。特に小規模企業では、OT に特化した人材や予算が限られており、優先度の高い対策に比べ、インシデントレスポンス関連の取り組みが後回しになりやすいことが考えられる。大規模企業でも、工場ごとに独立した制御環境が存在するため、拠点単位でインシデント対応要員を確保・標準化することが難しく、これが全体の遵守率の伸び悩みに影響していると考えられる。

3.1.3. 業界ごとのカテゴリ別遵守率

業界ごとのカテゴリ別遵守率を、全カテゴリの遵守率が高い順に以下の表に示す。

[表 3.1.5] 業界ごとのカテゴリ別遵守率

業界	ガバナンス	インシデントレスポンス	テクノロジー&オペレーション	データ保護	全カテゴリ	回答数
はん用機械器具製造業	83.1%	85.0%	82.0%	75.0%	81.3%	5
情報通信機械器具製造業	78.3%	75.0%	80.0%	71.9%	76.3%	8
輸送用機械器具製造業	72.6%	67.5%	75.6%	77.0%	73.2%	25
業務用機械器具製造業	74.7%	69.6%	74.5%	73.2%	73.0%	7
電気機械器具製造業	71.7%	67.9%	73.5%	72.3%	71.4%	28
印刷・同関連業	74.0%	66.7%	66.2%	68.8%	68.9%	6
生産用機械器具製造業	63.4%	71.4%	67.9%	65.2%	67.0%	14
電子部品・デバイス・電子回路製造業	65.7%	62.9%	70.0%	69.0%	66.9%	29
電気・ガス・熱供給・水道業	68.6%	64.1%	63.7%	62.5%	64.7%	24
鉄鋼・金属・非鉄金属製造業	65.1%	58.0%	69.7%	64.3%	64.3%	28
その他の製造業	61.1%	55.3%	61.4%	59.2%	59.2%	57
運輸業	57.7%	57.8%	58.6%	56.3%	57.6%	32
繊維工業	55.0%	56.8%	54.7%	59.1%	56.4%	11
化学・石油・プラスチック・ゴム製品製造業	53.9%	47.6%	51.9%	58.2%	52.9%	26
総計	64.8%	61.2%	65.7%	64.6%	64.0%	300

業界別にみると全体平均遵守率に大きな差が生じていることが明らかとなった。たとえば、「はん用機械器具製造業」では 81.3%、「情報通信機械器具製造業」では 76.3%、「輸送用機械器具製造業」では 73.2%と高い水準を示している。一方で、「運輸業」では 57.6%、「化学・石油・プラスチック・ゴム製品製造業」では 52.9%と、遵守率が高い業界と比べて 20～30 ポイントの差が生じている。なお、はん用機械器具製造業や情報通信機械器具製造業は回答数が一桁台と少なく、統計的な信頼性に留意が必要であるが、全体として業界間で大きな開きがみられる。

各業界内で 4 カテゴリを比較すると、強みと弱みがはっきり分かれる傾向が見受けられる。たとえば、「輸送用機械器具製造業」では「テクノロジー&オペレーション」や「データ保護」が 70%台後半と高い一方、「インシデントレスポンス」は 67.5%とやや低めである。また、「生産用機械器具製造業」では「インシデントレスポンス」が 71.4%と最も高く、他のカテゴリはいずれも 60%台にとどまっている。このように、業界ごとに優先的に強化されているカテゴリの違いが明確に示されている。

さらに業界間でカテゴリごとに比較しても、ばらつきの大きさが際立つ。「ガバナンス」では「はん用機械器具製造業」が 83.1%、「化学・石油・プラスチック・ゴム製品製造業」が 53.9%と約 30 ポイントの開きがある。「インシデントレスポンス」に至っては、「はん用機械器具製造業」が 85.0%、「化学・石油・プラスチック・ゴム製品製造業」が 47.6%と約 40 ポイントの差が見られる。「テクノロジー&オペレーション」でも「はん用機械器具製造業」が 82.0%で、「繊維工業」が 54.7%と約 30 ポイントの開きがあり、「データ保護」でも「輸送用機械器具製造業」が 77.0%、「運輸業」が 56.3%と約 20 ポイントの差となっている。

このように業界間で全体遵守率やカテゴリごとに 20～40 ポイントの差が生じた要因として、まずサプライチェーンや国際規格への対応圧力が挙げられる。高い遵守率を示す「はん用機械器具製造業」や「輸送用機械器具製造業」「情報通信機械器具製造業」などの業界は、グローバル OEM や大手メーカーとの取引条件として厳格なセキュリティ基準が求められるケースが多く、ガバナンスから技術対策まで他業界よりも早期に整備が進んでいると推察される。一方、「化学・石油・プラスチック・ゴム製品製造業」のようにプラント制御を扱う業界では、危険物や物理的事故防止を最優先する傾向が強く、サイバー面のインシデントレスポンス体制やネットワーク防御への取り組みが後手に回りがちである。そのため、インシデントレスポンスやテクノロジー&オペレーションの遵守率が他業界よりも低くなっている可能性が高い。

このような業界ごとの違いを踏まえ、各業界の特性やリスクに応じた対策の強化が今後も重要となる。

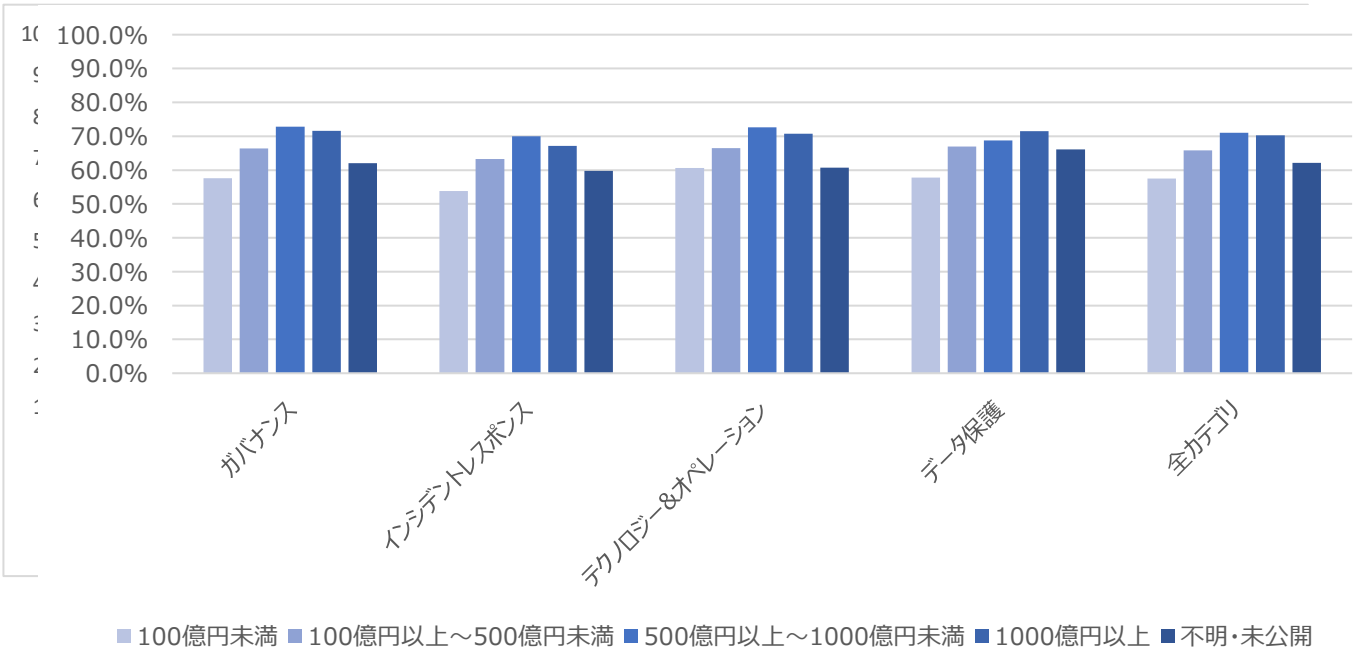
3.1.4. 売上高ごとのカテゴリ別遵守率

売上高ごとのカテゴリ別遵守率を以下の表に示す。

[表 3.1.6] 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	テクノロジー&オペレーション	データ保護	全カテゴリ
100 億円未満	57.6%	53.8%	60.6%	57.8%	57.5%
100 億円以上～500 億円未満	66.4%	63.3%	66.5%	67.0%	65.8%
500 億円以上～1000 億円未満	72.8%	70.0%	72.7%	68.8%	71.1%
1000 億円以上	71.6%	67.1%	70.7%	71.5%	70.2%
不明・未公開	62.1%	59.8%	60.7%	66.1%	62.2%
総計	64.8%	61.2%	65.7%	64.6%	64.0%

[図 3.1.3] カテゴリごとの売上高別遵守率グラフ



売上高別にみると、最も高かったのは「500 億円以上～1000 億円未満」で 71.1%、次いで「1000 億円以上」の 70.2%が続いた。一方、「100 億円未満」は 57.5%と最も低く、概ね売上高が大きいほど遵守率が高い傾向が確認できる。ただし 1000 億円以上の層でわずかに数値が下がったのは、拠点・事業領域の多様化に伴い統制が難しくなる影響と考えられる。

カテゴリ別にみると、「100 億円未満」でも「テクノロジー&オペレーション」が 60.6%と比較的高いが、「インシデントレスポンス」は 53.8%と低い。「100 億円以上~500 億円未満」では各カテゴ

リが 60%台半ばとなっているが、「インシデントレスポンス」が 63.3%と少し低い。「500 億円~1000 億円未満」は 4 カテゴリが 70%台前後に到達しているが、「1000 億円以上」では「インシデントレスポンス」が 67.1%と再び開きが生じた。このことから、売上規模に関わらず「インシデントレスポンス」は概ね他カテゴリよりも遵守率が低い傾向がみられた。

テクノロジー＆オペレーションが他のカテゴリと比較して取り組まれやすいのは、製品導入や外部ベンダー支援により比較的短期間で成果が得られる領域だからだと考えられる。 ただし、売上「1000 億円以上」の企業よりも、「500 億円~1000 億円未満」の方が、遵守率が高くなっており、金銭的に余裕があるからと言って、セキュリティ製品やベンダー支援への投資が行われているとは限らないと思われる。このような結果になる要因の一つには、制御機器等の整備など生産ラインの運用維持や効率化に投資する必要があり、セキュリティ対策が後回しにされるケースもあるものではないかと推測する。

一方で、インシデントレスポンスは、体制構築や訓練といった人的リソース投資が不可欠で費用対効果が見えにくく、売上規模が大きくても後回しになりがちだと考えられる。したがって、遵守率が全体的に低くなっているのだと思われる。

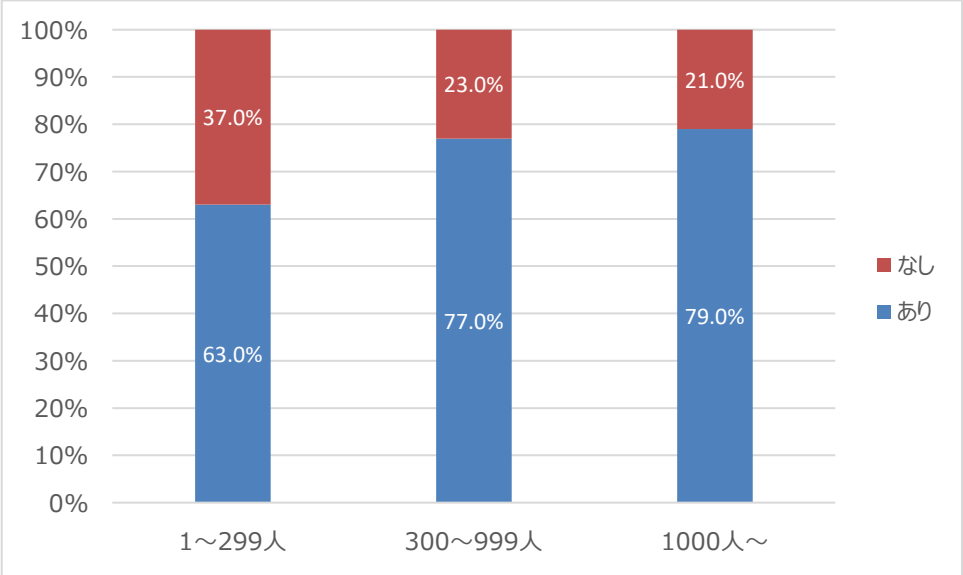
3.1.5. セキュリティ対策に関する外部レビュー/評価サービスの利用状況とカテゴリ別遵守率

制御システムのセキュリティ施策推進に関する、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評価のサービス（例えば監査や診断等）の利用経験の有無について、企業規模別で比較した結果を以下に記す。

[表 3.1.7] 従業員規模とセキュリティ対策に関する外部レビュー/評価サービスの過去３年以内の利用状況

従業員規模	あり	なし
1～299 人	63.0%	37.0%
300～999 人	77.0%	23.0%
1000 人～	79.0%	21.0%
総計	73.0%	27.0%

[図 3.1.4] 従業員規模とセキュリティ対策に関する外部レビュー/評価サービスの過去３年以内の利用状況割合



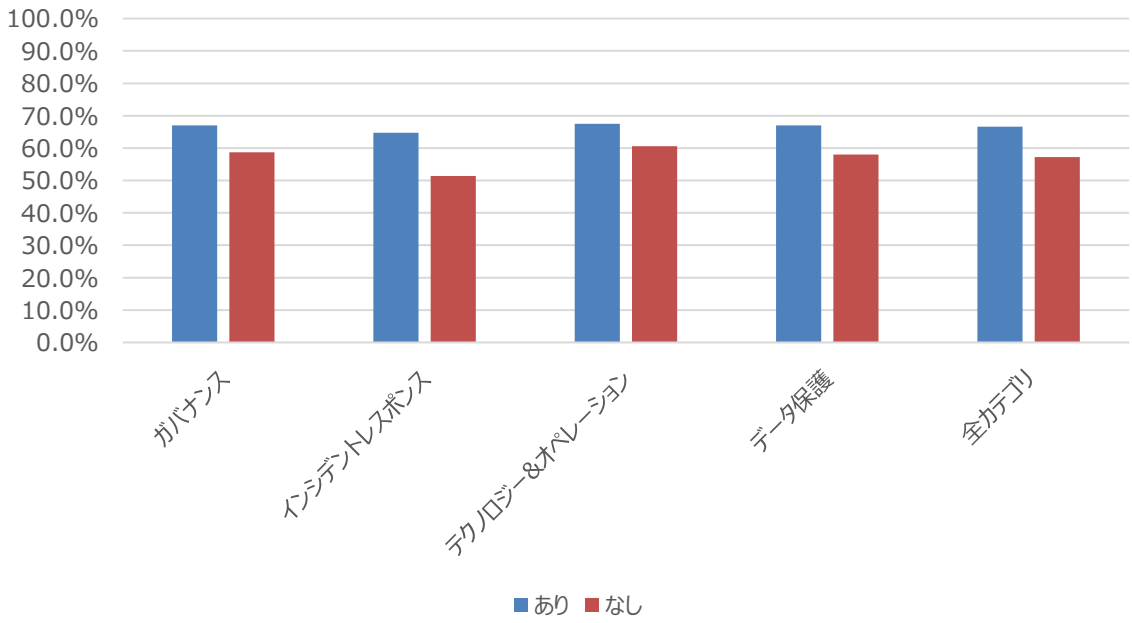
制御システムのセキュリティ施策推進に関し、外部の専門家によるセキュリティ対策に関するレビューや評価のサービス利用経験がある企業は、全体の 73.0%にのぼった。また、従業員規模が大きくなるほど、外部レビュー/評価サービスの利用率が高くなる傾向が見られる。ただし、「300～999 人」の企業と、「1000 人～」の企業の利用率の差は 2 ポイントに留まっている。

また、制御システムのセキュリティ施策推進に関し、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評価のサービス（例えば監査や診断等）の利用経験の有無についての、カテゴリ別の遵守率を以下に記す。

[表 3.1.8] 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/評価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	テクノロジー&オペレーション	データ保護	全カテゴリ
「あり」と回答した企業の平均遵守率	67.0%	64.8%	67.5%	67.0%	66.6%
「なし」と回答した企業の平均遵守率	58.7%	51.4%	60.6%	58.0%	57.2%
総計	64.8%	61.2%	65.7%	64.6%	64.0%

[図 3.1.5] 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



過去 3 年以内に外部レビューや評価サービスを利用している企業の全体平均遵守率は 66.6%と、総計を上回る結果となった。一方、利用していない企業の平均遵守率は 57.2%にとどまり、約 9%の差がみられた。外部レビューを利用している企業の方が、全般的にセキュリティ対策が進んでいる傾向が明確である。

カテゴリ別にみると、外部レビューを「利用している」企業は全カテゴリで高い遵守率を示し、特に「インシデントレスポンス」では総計を上回った。一方、「利用していない」企業は全カテゴリで総計を下回っており、特に「インシデントレスポンス」は総計から 10%以上低い結果となっている。「利用している」企業と「利用していない」企業でカテゴリ別遵守率を比較すると、「インシデントレスポンス」が13.4%と最も大きな差が出ており、次いで「ガバナンス」「データ保護」と続き、「テクノロジー&オペレーション」でも約 7%の差がみられた。こうした結果から、専門家による外部支援はどのカテゴリでも効果があるが、特に「インシデントレスポンス」で著しい効果が発揮されている。

このような結果となった理由として、外部の専門家から客観的な指摘やアドバイスを受けることで、自社内では気づきにくい脆弱性や改善点を把握しやすくなることが考えられる。特に「インシデントレスポンス」分野は、緊急時対応フローや定期訓練の設計などが自社だけでは難しいため、外部知見の導入が有効に機能する。また、外部レビューを導入する企業は、そもそも経営層がセキュリティに対して高い関心や意識を持っている傾向があると考えられる。そのため、ガバナンスやデータ保護などの他カテゴリについても、全体的に取り組みが進みやすい可能性がある。

結論として、OT のセキュリティ体制を強化するためには外部専門家の支援・ノウハウを適切に取り入れることが有効である。特に「インシデントレスポンス」においては自社のみでの限界を認識し、外部支援の活用を今後の施策として積極的に検討すべきである。

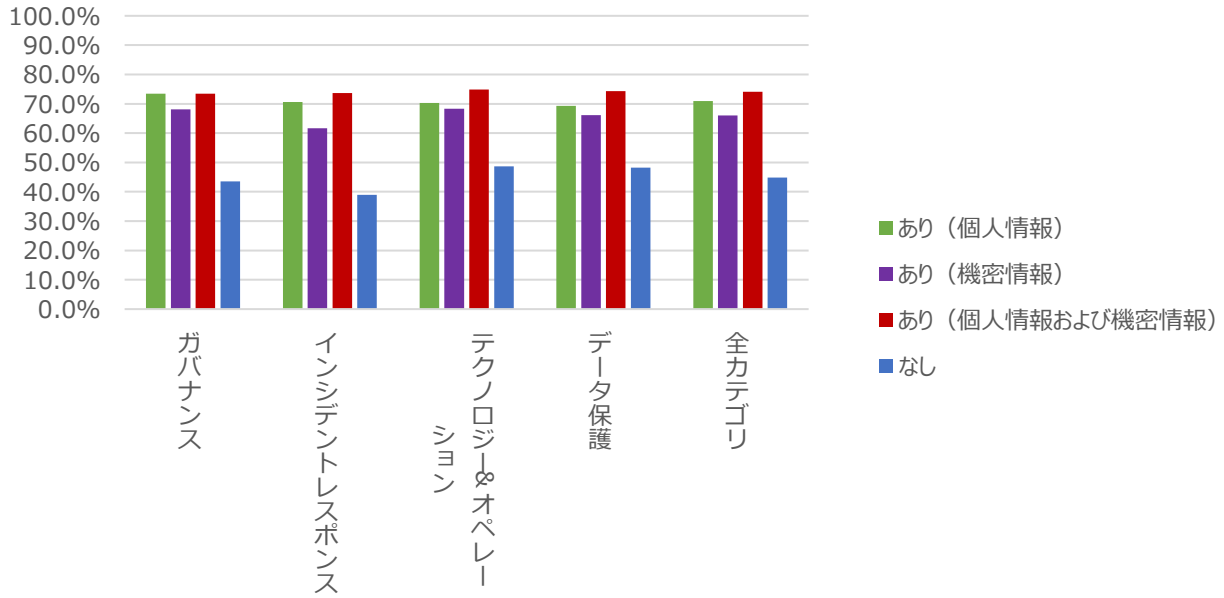
3.1.6. 個人情報・機密情報の取り扱い有無とカテゴリ別遵守率

「個人情報」「機密情報」に該当する情報の伝送、処理、または保存があるか否かの、カテゴリ別の遵守率を以下に記す。

[表 3.1.9] 個人情報・機密情報の取り扱い有無とカテゴリ別遵守率

取り扱い有無	ガバナンス	インシデントレスポンス	テクノロジー&オペレーション	データ保護	全カテゴリ
あり（個人情報）	73.5%	70.6%	70.3%	69.3%	70.9%
あり（機密情報）	68.1%	61.7%	68.3%	66.2%	66.0%
あり（個人情報および機密情報）	73.4%	73.6%	74.9%	74.3%	74.1%
なし	43.5%	38.9%	48.6%	48.2%	44.8%
総計	64.8%	61.2%	65.7%	64.6%	64.0%

[図 3.1.6] 取り扱い情報ごとのカテゴリ別遵守率



全体平均遵守率が最も高いのは「あり（個人情報および機密情報）」と回答した企業の 74.1%で、最も低いのは「なし」と回答した企業の 44.8%となり、約 30 ポイントの差が生じた。また、「あり（個人情報のみ）」と回答した企業は 70.9%、「あり（機密情報のみ）」と回答した企業は 66.0%で、個人情報を扱う企業の方が高い遵守率を示す傾向がみられた。

カテゴリ別にみても、「あり」と回答した企業群はいずれのカテゴリでも「なし」と回答した企業より大幅に高い遵守率となっている。特に「インシデントレスポンス」は「あり（個人情報および機密情

報）」が 73.6%、一方「なし」は 38.9%と約 35 ポイントの開きが最も顕著であった。「あり（個人情報のみ）」と「あり（機密情報のみ）」を比較しても、前者の方が高い遵守率を示している。

このような結果となった背景には、個人情報を扱う企業では個人情報保護法などの法規制による強制力が早期から対策整備の推進力となっていることがある。一方で、機密情報のみ扱う企業は主に競争優位性の維持や顧客契約の履行が対策強化の動機となるが、法的拘束力の強さや社会的影響度の違いから、個人情報のみを扱う企業ほど遵守率が高くなっていると推察される。逆に、個人情報も機密情報も取り扱わない企業では情報漏えいリスクへの認知が低く、法規制も直接適用されないため、セキュリティ投資が後回しになり、全体的な対策整備が遅れている状況と考えられる。

3.1.7. 総括

本章で分析した各切り口（全体、従業員規模、業界、売上高、外部レビュー利用、情報取扱区分）を通じて共通して浮かび上がるのは、「インシデントレスポンス」カテゴリの遵守率が全体的に他カテゴリよりも低い傾向が見られることである。これは、体制整備や訓練、初動対応の標準化など、専門的かつ継続的なリソースが必要となる取り組みが多いこと、また、実際の効果が可視化しにくいことが要因として挙げられる。特に小規模企業や情報取扱が限定的な企業では、リソースや認識の面で課題が大きい。

今後は、組織規模や業界特性、情報取扱状況を問わず、「インシデントレスポンス」を中心に体制強化・訓練・手順整備の底上げを図るとともに、外部専門家のノウハウ活用や、ガイドライン・標準の参照、現場で実行可能な訓練プログラムの導入など、現実的かつ段階的な取組を推進していくことが重要である。また、OT 領域においては、サイバー攻撃による機械の災害等にも備える必要があるため、連絡体制などについて工場特有の特性があることを念頭におく必要があるだろう。

3.2. 相関係数を用いた分析 - 相関関係の高い項目に着目

【会員限定公開部分】

相関関係の高い項目として、ガバナンスと人材、脆弱性マネジメント、
境界防御とアクセス制御、外部連携についての
それぞれの相関における傾向の記述

3.3. 相関係数を用いた分析 – 遵守率の低い項目に着目

【会員限定公開部分】

遵守率の低い項目として、委託先管理、インシデント対応体制に
ついてのそれぞれの相関における傾向の記述

4. 集計結果より提言

本調査から、セキュリティベンダーや保守ベンダーとの連携体制を整備することで、パッチマネジメントなどのプロセスを成熟させることが可能であると考える。また、ガバナンスを強化が、前述のような体制強化や技術対策の実践に結び付く傾向にあるため、ガバナンスカテゴリの遵守率向上が OT 領域全体のセキュリティ向上に直結すると考える。

① ガバナンス強化

上述の通り、OT システムの技術的な対策、セキュリティ事故の対応を推進するには制度や仕組み 作りから優先的に着手すべきだと考える。一方、OT 特有の課題が存在し、制御システムといった IT システムとは性質の異なるシステムや装置を取扱うため、現場との協力体制を敷き、現実的な制度作りを行うと良いだろう。

② 外部サービスの活用

上述の通り、OT システムは IT システムとは異なる性質を持ち、特に技術的対策においては、専門的な知見を要する場合が多い。調査結果からも外部レビューや評価サービスを利用している企業の方が、利用していない企業よりも遵守率が高い結果が出ている。特に、中小企業においては、体制準備も容易ではないと思われるため、セキュリティベンダーを頼ることも重要であると考える。

本フレームワークを活用することで、自社 OT 環境における課題を可視化することができる。また。CSIJ 評価分科会各社は課題解決に向け多様なサービスを提供している。各社サービスにご興味のある方は、ぜひご連絡をいただきたい。

各社連絡先（リンク先に記載）：

https://www.csi-japan.org/evaluation/evaluation-guid

5. CSIJ の活動

昨今のサイバーセキュリティにおいては、予防的観点からも考慮された適切かつ継続的な対応を行い、安全・安心な事業継続を図ることが重要であるとともに、これらの対策を行いうる人材の確保も大きな課題となっている。

このような状況における課題解決に向けて、CSIJ では環境変化を常にキャッチアップし、これからの将来を見据えて企業が行うべき必要かつ現実的で、さらには日本の市場特性も考慮した「サイバーセキュリティ対応」の提言と、実効性のある実装にむけた支援を行い、この「サイバーセキュリティ対応・実装」に必要な人材輩出に向けた活動も実施している。

5.1. CSIJ 調査レポートの活用

今回の調査においては、インシデントレスポンスの遵守率が低いことが明らかとなった。特に、サイバー攻撃による機械の停止や災害発生時の対応準備、さらには緊急時の連絡体制の整備不足といった課題が、工場という産業特有の環境要因に起因していると考えられる。

また、CSIJ ではセキュリティ体制に関する調査も実施しており、全体傾向の分析に加えて企業規模別のベースラインも掲載している。本調査結果を理解する際には、これらのデータをあわせて参照することで、自組織の位置づけや改善の方向性を検討する際の参考となる。

・CSIJ 共通評価フレームワーク（セキュリティ体制版）アンケート調査結果レポート
https://www.csi-japan.org/_files/ugd/e66227_5d77080aa4354852b5b2e0a2278f421a.pdf

5.2. CSIJ は評価フレームワークを通して、企業の対策のサポートを実現

CSIJ では環境変化を常にキャッチアップし、これからの将来を見据えて企業が行うべき必要かつ現実的、さらに、日本の市場特性も考慮した「サイバーセキュリティ対応」を提言するだけではなく、実装にむけての支援を行っている。加えて、この「サイバーセキュリティ対応・実装」に必要な人材輩出に向けた活動も実施している。

現在、CSIJ では「共通対策評価フレームワーク分科会」および「サイバーセキュリティプロフェッショナル人材フレームワーク分科会」の二つの分科会が活動している。

共通対策評価フレームワーク分科会では下記の観点で共通対策評価フレームワークを作成している。

- 新領域（クラウド、ゼロトラスト等）利用にフォーカスし、日本特有環境を踏まえ広範に企業が活用できる内容とする。
- 既存の各種国際・国内基準、ガイドラインの内容をベースとしつつ、具体的・網羅的かつシンプルに重要ポイントを押さえた内容とする。
- この「セキュリティ対策評価フレーム」評価結果を踏まえた具体的な対策支援が、会員企業から顧客企業に提供できるよう連携を図る。
- 評価データを蓄積し、企業（業種別、規模別など）セキュリティレベルの実状概況を把握可能とする（予定）。

CSIJ の活動詳細は下記リンク（CSIJ 公式ウェブサイト）の活動内容をご覧ください。

- CSIJ 活動内容
https://www.csi-japan.org/active

5.3. 本アンケート調査方法の詳細

調査目的	製造業のセキュリティ対策の現状を把握・分析し、OT に関するセキュリティ対策状況を可視化することで、国内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	工場やプラントなどの制御システムにおいて、セキュリティ対策の企画・実施判断や管理・運用に携わった経験がある担当者および意思決定者
調査内容	回答者の属性を調査する設問(13 問)と、企業の制御システムおよびそのセキュリティ対策状況を問う 4 つのカテゴリ(※1)の設問(37 問)を用いた調査。 (※1) <評価カテゴリ> 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 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 ③ テクノロジー&オペレーション…システム運用における構成管理・脆弱性対策の実施状況を確認するカテゴリ ④ データ保護…マルウェア対策やデータのバックアップ等、データの保護状況を確認するカテゴリ
分析方法	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) (※2)<回答と点数の換算> ◎…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） (※3)<遵守率の算出方法> 遵守率…評価による点数の合計/総得点数(単位: %)
サンプル数	総計 300 サンプル
調査時期	2024 年 12 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

■ 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 広瀬　真一 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
持田　啓司（CSIJ 事務局長） 奥野　康城（評価分科会リーダー） 秋山　真菜 岡本　大輝 谷口　諒之介 田中　伶佳 藤原　青空	株式会社ラック

■ 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/