2023 年度
産業制御システムを対象とした SIRT（制御系 SIRT）の実態に関する調査報告書
- 一般製造業 -

一般社団法人 JPCERT コーディネーションセンター

2024 年 9 月 27 日

JPCERT CC®

目次

1. はじめに

1.1 調査背景

産業制御システムへのセキュリティ対策については、当該システムにおいて被害が起こった場合の社会的な影響が甚大なこと等を鑑み、近年その取り組みが推進されてきている。また、産業制御システムにおいてインシデントが発生した際には、そのインシデントに対応する組織機能（いわゆる SIRT 機能）が必要となるが、昨今この産業制御システムを対象とした SIRT（以下、「制御系 SIRT」という。）の必要性が取り上げられるようになるとともに、組織の立ち上げが進んできている状況が推察される。一方でこの制御系 SIRT については、先行して構築・運用が進められてきている CSIRT や PSIRT の状況とは異なり、すでに存在する活動の定義や構築・運用におけるベストプラクティスが確立されておらず、手探りでの構築や運用がされていることが考えられる。

1.2 調査目的

そこで本実態調査事業では、一般製造業者における制御システムを対象としたインシデント対応関係者（「制御系 SIRT」または制御システムを対象とするインシデント対応体制の担当者）へのアンケート調査により現在の制御系 SIRT の実態を把握するとともに、制御システムインシデントの経験がある事業者や制御系 SIRT の構築が進む事業者へのヒアリングにより各組織が抱える課題を明らかにすることを目的とした調査を行う。さらにこれらの調査結果の分析をもとに課題やその改善策を検討する。これらの調査・分析結果や改善策の検討結果から、制御系 SIRT を構築・運用していく組織が今後進めるべき活動・方向性についての提言を取りまとめる。以上のアンケート調査およびその分析結果や提言の取りまとめまでを「産業制御システムを対象とした SIRT（制御系 SIRT）の実態に関する調査」（以下、「本実態調査」という。）として実施する。
なお、本実態調査の調査結果の文書構成は、次のとおりである。

- 2023 年度産業制御システムを対象とした SIRT（制御系 SIRT）の実態に関する調査報告書 - 一般製造業 -（本書）
  - 本実態調査の「調査背景」「調査概要」「詳細ヒアリング結果」「調査結果に基づく分析」および「提言」
- 2023 年度産業制御システムを対象とした SIRT（制御系 SIRT）の実態に関する調査_アンケート回答結果
  - 本実態調査のアンケート調査の回答結果を公表版として取りまとめたもの

2. アンケート調査

アンケート調査の概要は次のとおり。

2.1 アンケート調査先・規模および調査手法について

アンケートは、産業制御システムを対象としたインシデント対応の取り組みの実態を明らかにし、課題改善策についての検討に資することを目的としたものである。このため、アンケート内容としては、制御システムのセキュリティ対応や特にインシデント発生時の対応等に関する内容を主とし、対象者としては、これらの対応に当たる可能性のある一般製造業者（石油、化学、鉄鋼・製紙、電機・精密、医薬、食品、自動車、機械等）の中で、制御システムを保有し、かつ制御システムを対象とした SIRT または準ずる活動を実施する事業者の担当者を対象とした。
アンケート調査先の選定に当たっては、これらの対象者をいかにして抽出するかが重要となる。このため、企業データベースから一般製造業者を広く抜き出すとともに、いくつかの母集団を組み合わせることとした。表 1 に企業データベースから抽出したアンケート送付先の業種別件数を示す。

表 1 企業データベースから抽出したアンケート送付先の業種別件数

業種名称	件数
食料品製造業	326
飲料・たばこ・飼料製造業	56
繊維工業	65
木材・木製品製造業（家具を除く）	19
家具・装備品製造業	31
パルプ・紙・紙加工品製造業	79
印刷・同関連業	64
化学工業	357
石油製品・石炭製品製造業	18
プラスチック製品製造業（別掲を除く）	126
ゴム製品製造業	53
なめし革・同製品・毛皮製造業	4
窯業・土石製品製造業	95
鉄鋼業	93
非鉄金属製造業	72
金属製品製造業	190
はん用機械器具製造業	174
生産用機械器具製造業	230
業務用機械器具製造業	127
電子部品・デバイス・電子回路製造業	207
電気機械器具製造業	250
情報通信機械器具製造業	108
輸送用機械器具製造業	378
その他の製造業	88
合計	3,210

実際のアンケート実施概要を表 2 に示す。

表 2 アンケート実施概要

送付数	
企業データベースから抽出した一般製造業者	3,210 件
一般製造業者が加盟する業界団体会員企業	約 1,000 件
制御システムセキュリティ関連イベント参加者	595 件
回答数	
有効回答数	185 件
（回答者の属性別内訳）	
セキュリティ関係者	68 件
（内、制御システムセキュリティ関係者）	（26 件）
（内、その他セキュリティ全般の関係者）	（42 件）
情報システム関係者	56 件
生産企画・生産管理関係者	12 件
開発関係者	5 件
保守・品質管理関係者	4 件
その他	40 件

※ 「セキュリティ関係者」は、制御システムセキュリティ関係者、情報システムセキュリティ関係者、インシデント担当者、製品セキュリティ関係者、セキュリティ全般の関係者などを含んだ総数である。

2.2 アンケート内容について

実際に実施したアンケートの大項目レベルの構成を表 3 に示す。実際のアンケート調査票としては中小項目に展開した設問を設定しており、これらのアンケート調査票を通じて、次の点を明らかにする内容としている。

- 制御系 SIRT 構築の進捗状況
- 制御系 SIRT の機能、役割、関係する部門組織
- 制御系 SIRT の活動内容、活動実績（制御システムインシデント対応事例）
- 制御系 SIRT として現状抱えている課題

表 3 アンケートの構成（大項目レベル）

No.	カテゴリー	設問	設問の目的
1.	基本情報	1-1 回答者情報（企業名、回答者所属、連絡先）	アンケート回答者の連絡先把握
2.		2-1 企業情報（企業概要、企業諸元）	アンケート回答者の属性把握
3.	製造システムの保有状況	3-1 FA 製造システムの保有状況	アンケート対象者の選別（FA システム保有者）
		3-2 PA 製造システムの保有状況	アンケート対象者の選別（PA システム保有者）
		3-3 その他製造システムの保有状況	アンケート対象者の選別（その他システム所有者）
4.	「制御システムインシデント」に備えた体制作りの取組状況	4-1 制御システムインシデントを対象とした取組体制やルール	インシデント発生時の社内の対応ルール・組織・体制の実態把握
		4-2 制御システムインシデント対応体制の取組の対象システム	対応体制が対象とするシステムそのものおよびシステムの重要度の把握
		4-3 制御システムインシデント対応体制の取組内容	平時における制御システムインシデント発生時の取り組み検討、整備具合の把握
		4-4 制御システムインシデントへの取組理由や現状評価、将来像等	制御システムインシデントに対する対策のきっかけ、今後の課題の把握
5.	実際の制御システムインシデントへの対応状況	5-1 制御システムインシデントの発生状況	具体的な被害発生状況の把握
		5-2 制御システムインシデントの被害内容	具体的な被害内容の把握
		5-3 制御システムインシデントの発見経緯と対応内容	具体的な被害発生経緯および被害対応の把握
		5-4 制御システムインシデントへの対処内容	インシデントの収拾対処の把握
		5-5 制御システムインシデントに対する追加のセキュリティ対策やその評価	被害対応の評価の把握

2.3 アンケートの依頼・回収について

2.3.1 アンケートの依頼方法

上述した表 2 アンケート実施概要の送付数に示した対象者に対してアンケート依頼を実施した。次のような形で、依頼および回収を実施している。

（1） 依頼方法

アンケート依頼は対象者の母集団により、書面または電子メール等で実施した。

（2） 回収方法

いずれの対象者に対しても、回収方法は同一で、アンケート事業者の用意したアンケートサイトへの回答入力の他、同じくアンケート事業者の用意した回答受け付け用メールアドレスへの電

子メールでの送付の 2 種類の回収方法を用意した。

2.3.2　アンケート依頼に際した関連資料の作成

アンケート実施に当たっては、以下の各資料を作成した。

- アンケート調査票（エクセル様式、印刷用 PDF）
- 依頼状
- 回答方法のお知らせ
- 個人情報の取り扱いについてのお知らせ

2.4　アンケート調査結果について

これまで記載した方法等を用いて実施したアンケート調査の結果は、本書とあわせて公開した「2023 年度産業制御システムを対象とした SIRT（制御系 SIRT）の実態に関する調査_アンケート回答結果」を参照いただきたい。
また、本書の 3 章には、アンケート調査後に実施した「詳細ヒアリング」について、4 章には、「2023 年度産業制御システムを対象とした SIRT（制御系 SIRT）の実態に関する調査_アンケート回答結果」をベースにして、特に注目した点の分析（単純集計、クロス集計含む）を記載している。

3. アンケート後の詳細ヒアリング

アンケートの回答を得た組織のうち 9 組織を対象に、以下のとおり詳細ヒアリングを実施した。

3.1 詳細ヒアリングの概要

本実態調査は、制御システムへのインシデントに際して、どのような組織がどのような対応を行い、それが制御システムを対象とした SIRT によるものなのか、その組織状況やインシデントに向けた準備・日常の活動の状況などを明らかにするとともに、今後の施策に活かすことを目的としている。
このため、詳細ヒアリング対象の選定に当たっては、次の要件を持つことを基準とすることとした。

- 制御システムインシデントの経験を持つこと（実際に対応に当たった経験を持つこと）
- 制御系 SIRT（準ずる体制含む）を持つこと
- 制御系 SIRT の構築を検討していること

この要件に 1 つでも合致し、かつ打診に応じた次の 9 社に詳細ヒアリングを実施した。詳細ヒアリングの対象者を表 4 に示す。

表 4 詳細ヒアリングの対象者

制御システムインシデントの経験	対応体制	社数
あり（6 社）	制御系 SIRT あり	2
	制御系 SIRT 構築を検討中	1
	CSIRT を中心に検討中	1
	製造システムが対応	1
	状況に応じて都度対応	1
なし（3 社）	制御系 SIRT あり	2
	制御系 SIRT 構築を検討中	1

3.2 詳細ヒアリング実施結果

詳細ヒアリングの結果、各社における製作所や工場を対象とした SIRT の体制が多種多様であることが確認できた。制御系 SIRT という名称ではないが、実質的に同様の組織が構築されているケースもあれば、CSIRT などの既存組織が役割を担うケースもあった。
制御系 SIRT の実態という観点では、以下の 3 つのフェーズでヒアリング対象企業がどのような取り組みや課題を持っているかを表 5 のとおりに確認した。

- 制御系 SIRT の構築に向けて
  制御系 SIRT を含めた SIRT の構築を検討している段階

- 制御系 SIRT を構築中
  CSIRT や情報システム部門などにおいて制御系 SIRT の役割を担っているが、制御独自の内容を独立して検討できる体制ではない。
- 制御系 SIRT を構築済み
  制御系 SIRT と同等組織を構築済みであり、制御独自のセキュリティ対策やインシデント対応を検討できる体制である。

制御系 SIRT の構築に向けた活動として、多くの企業から制御系 SIRT 構築のきっかけとなった活動・事象を確認することできた。その内容として、自社インシデント、他社インシデント、親会社からの要求、ガイドライン・業界基準・規格からの要求の大きく 4 点を確認することができた。自社インシデントと親会社からの要求は企業内の事情である一方で、他社インシデント、ガイドライン・業界基準・規格からの要求など、外部情報を参照しているケースも多くの企業においてきっかけになっていた。

制御系 SIRT を構築中の企業の活動として、制御システムインシデントにおける対応体制の状況を確認することができた。ヒアリングしたほぼすべての企業において、制御システム部門や情報システム部門が単独で対応するような事例はなく、IT／OT の連携が実施できるような体制が構築されている。一方で、連携体制は、製造システム部門中心、情報システム部門中心、新たな組織の構築など、企業によって多種多様であった。また、ほぼすべての企業において、本社と工場現場間での情報共有の会合を開催し、セキュリティの重要性や工場の現状について情報交換が行われていた。実態とともに、制御系 SIRT 構築中の企業の課題も確認できた。さまざまな課題が確認できた中で、サイバー攻撃が制御システムにおける不具合等の原因になり得るという認識が工場現場に十分浸透していないという課題が多くの企業において確認できた。

制御系 SIRT を構築済みの企業の活動として、制御系 SIRT が構築された後の平時の活動状況を確認することができた。ヒアリングしたほぼすべての企業において、資産管理が実施されていた。一方で、資産管理の粒度はさまざまであり、機器と IP アドレスの対応のみを確認している場合や、OS・ソフトウェア・アプリケーションまで確認している場合もあった。また、セキュリティ教育についても多くの企業で実施されていた。実態とともに、制御系 SIRT を構築済みの企業の課題も確認できた。さまざまな課題が確認できた中で、多くの企業から脆弱性対応に関する意見があった。具体的には、資産管理を実施したことで脆弱性の特定まではできているが、脆弱性対応（パッチ適用など）を行うハードルが高いことが確認できた。ハードルが高い原因としては、工場の稼働を止められないことや制御設備・製品メーカーに問い合わせても対応が難しいと回答されるケースが多い。

表 5 制御系 SIRT の各フェーズにおける活動・課題

	制御系 SIRT の構築に向けて	制御系 SIRT を構築中	制御系 SIRT 構築済み
活動	● IT へのサイバー攻撃をきっかけに、IT／OT が分離できていない状況が判明し、制御系 SIRT の構築に至った ● 経営ガイドラインをもとに CSIRT を構築し、制御系のインシデントにも対応している ● 業界関連規格によってセキュリティの重要性が高まっている ● 親会社からの要求によって SIRT 構築の検討を本格化した ● 製造停止につながる事例が増えてきたことから SIRT の構築が検討された ● 制御系 SIRT を構築できていないが、制御システム・情報システムで連携できる体制の構築を目指している	● エスカレーション方法や工場停止ルールなどのインシデントの対応方法を検討中 ● インシデント報告は制御系 SIRT に統一している ● インシデント対応体制に制御関連部門・CSIRT などと連携している ● 制御系 SIRT を本社に設置し、現場でインシデントの実対応を行うことを想定している ● 制御関連部門と情報関連部門で定期的な情報共有を行っている ● IT／OT 連携箇所のみを監視している ● 親会社におけるセキュリティガイドラインをもとにセキュリティルールや規定を作成している ● OT 領域限定のセキュリティ教育を実施し、セキュリティの重要性を工場に浸透させている ● 制御システムセキュリティに関する協議会を設置し、ガイドラインを構築している ● 各拠点にセキュリティ担当者を設けて、定期	● 各種ガイドライン・規格をベースにガイドラインとチェックリストを作成している ● 工場におけるセキュリティ責任者を設置している ● セキュリティを取り入れた製造系のキャリアパス構築を検討 ● 資産管理とネットワークの状況を確認し、脆弱性の特定を行っている ● 制御ネットワーク内に SOC を設置する ● サイバー攻撃を起因としたインシデントレスポンス訓練を予定している ● 工場の必要な機器に対して EDR 等を導入している ● 制御系ネットワークのパケットモニタリングを実施している

		的にコミュニケーションをとっている ● 制御システムとサイバーセキュリティの兼任者を設置し、連携をスムーズにしている	
課題	● IT/OT の連携箇所のみの状況把握で、OT 設備を把握できていない ● 生産技術の担当者の巻き込みが体系立てられていない ● 制御系インシデントの全体管理ができるほどの情報がない	● 会社の体制上、工場へ対策を強制できない ● 本社と現場でサイバーセキュリティに関する認識のずれがあり、連携が難しい ● セキュリティルールや規定は策定できているが、運用が難しい ● インシデントが多様であるため、関係者との連携が明示的にルール化できていない ● インシデントによる製品への影響があるかを確認するのが難しい ● 故障とサイバーインシデントの見分けが現場でできない	● 制御系機器の脆弱性情報管理が実施できていない ● 既存工場への対策が難しい ● OS 等の情報が製品仕様に記載されていない ● 脆弱性対応が工場の継続稼働や設備・製品メーカーのサポート不足などで実施できない ● IOC の情報を収集できていない ● 工場の継続稼働とセキュリティ対策のバランスが難しい ● DX 化で社外接続が求められるが、検討するための人員が足りない

4. アンケート回答結果の分析

アンケート回答結果をベースとして、特に注目した点の分析（単純集計、クロス集計含む）を実施した。その分析結果を以下で紹介する。なお、アンケート回答結果の全体については「2023 年度産業制御システムを対象とした SIRT（制御系 SIRT）の実態に関する調査_アンケート回答結果」を参照されたい。

4.1 アンケート回答結果の分析について

アンケートの回答結果をベースとして、特に注目した点の分析に当たり、単純集計、クロス集計を実施した。
単純集計では、分析対象事業者の組織構成、運用状況、平時の取り組み、インシデント対応経験について実態を整理し、分析に必要な一部の集計結果を 4.1.1 回答者の属性情報以降に掲載した。（単純集計の全体は「2023 年度産業制御システムを対象とした SIRT（制御系 SIRT）の実態に関する調査_アンケート回答結果」を参照）
クロス集計では、上記単純集計の結果をもとに、各組織間の差異や特徴を明らかにするために、以下を比較対象とした分析を実施した。
「クロス集計における比較対象（制御システムを対象としたセキュリティの取り組みの実施主体）」

- 「制御系 SIRT が担当している事業者」
- 「制御系 SIRT を中心とした組織体制を検討中の事業者」
- 「CSIRT が担当している事業者／CSIRT を中心とした組織体制を検討中の事業者」
- 「情報システム部門が担当している事業者／情報システム部門を中心とした組織体制を検討中の事業者」
- 「製造システム部門が担当している事業者／製造システム部門を中心とした組織体制を検討中の事業者」

4.1.1 回答者の属性情報

回答した事業者の属性情報（業種、製造拠点、売上高）は図 1～図 3 のとおりである。業種については「その他の製造業」を除き、「化学工業」が 22 社と最も多かった。また製造拠点を複数持つ事業者が約 85%であり、「5 拠点以上」の製造拠点を持つ事業者の割合が 60.5%と最も多かった。また、売上高は「100 億円以上」と回答した事業者が 80.5%と最も多かった。

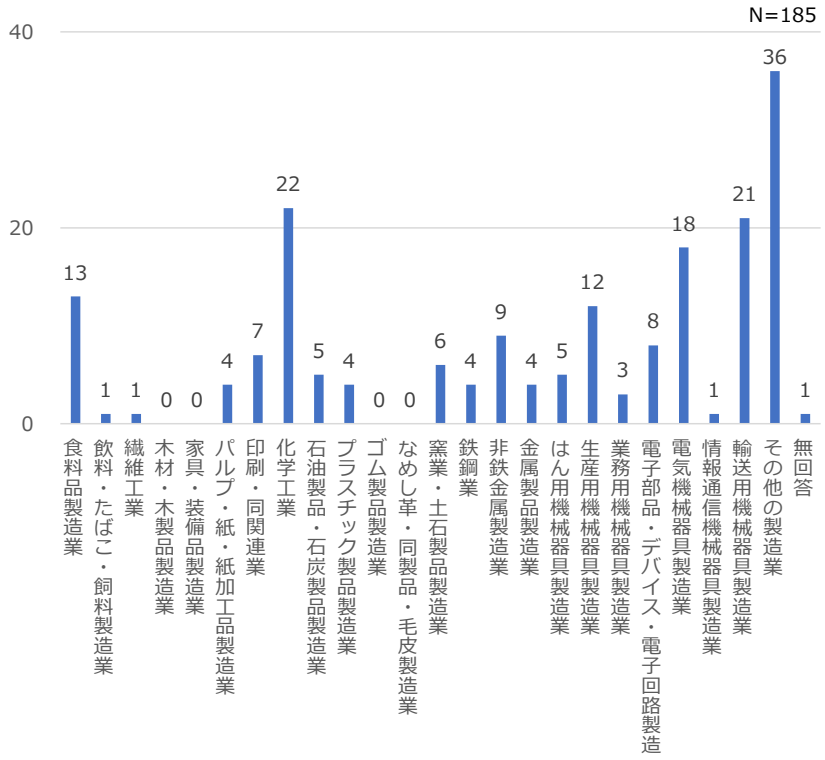


図 1 回答者の属性情報（業種）

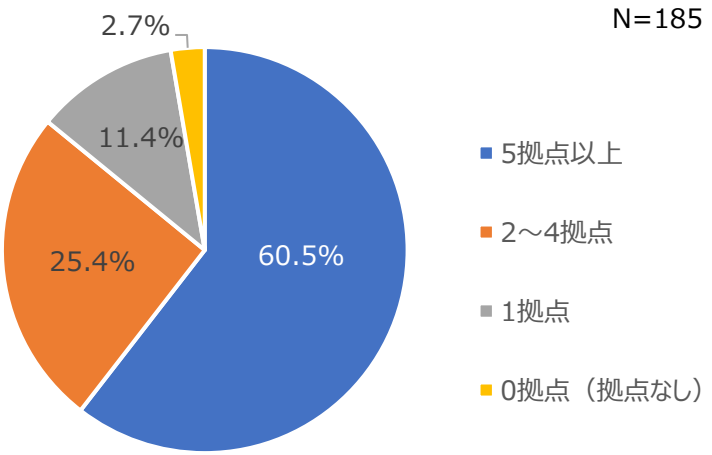


図 2 回答者の属性情報（製造拠点）

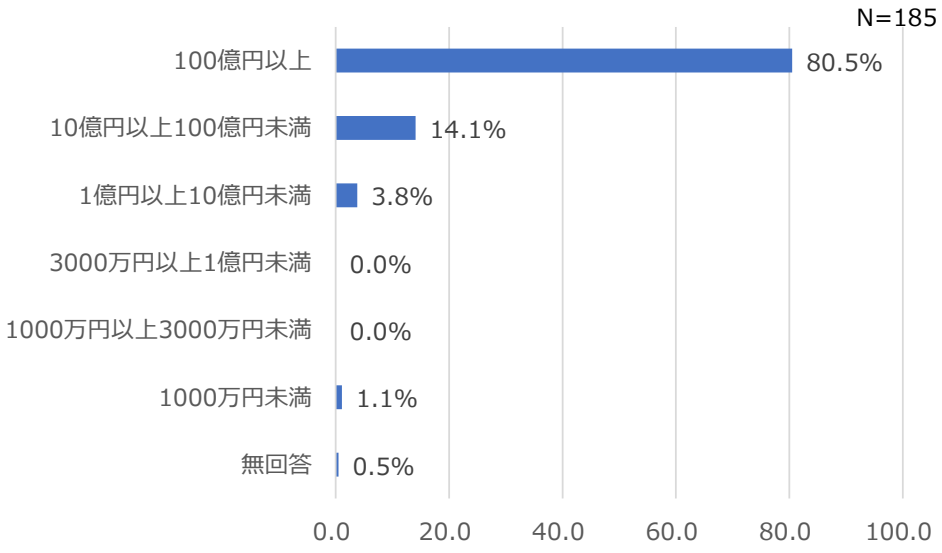


図 3 回答者の属性情報（売上高）

4.2 分析における注目点

4.2.1 制御システムインシデント対応体制

(1) 制御システムインシデント対応体制

設問番号	4-1-1
設問	貴社の制御システムでセキュリティインシデントが起きた場合、主に対応する組織・体制（以下、「制御システムインシデント対応体制」という）は、選択肢の中でどこでしょうか（実体組織以外に仮想的な体制も含みます）。現時点で対応体制はないが、検討中の場合についても、その旨をお答えください。
回答形態	単一回答

- 単純集計結果

本設問への回答結果（単純集計）を図 4 に示す。制御システムでセキュリティインシデントが起きた場合、主に対応する制御システムインシデント対応体制として、「主に情報システム部門が担当している。」と回答した事業者が 23.8%と最も多く、次点で、「主に製造システム部門が担当している。」と回答した事業者が 17.5%、「固定的な組織はなく検討も行っておらず、状況に応じて都度対応を検討する。」と回答した事業者が 16.8%であった。

「制御系 SIRT が担当している。」「制御系 SIRT を中心とした組織を検討している。」と回答した事業者は合計で 13 社であり、全体の 1 割未満にとどまる。

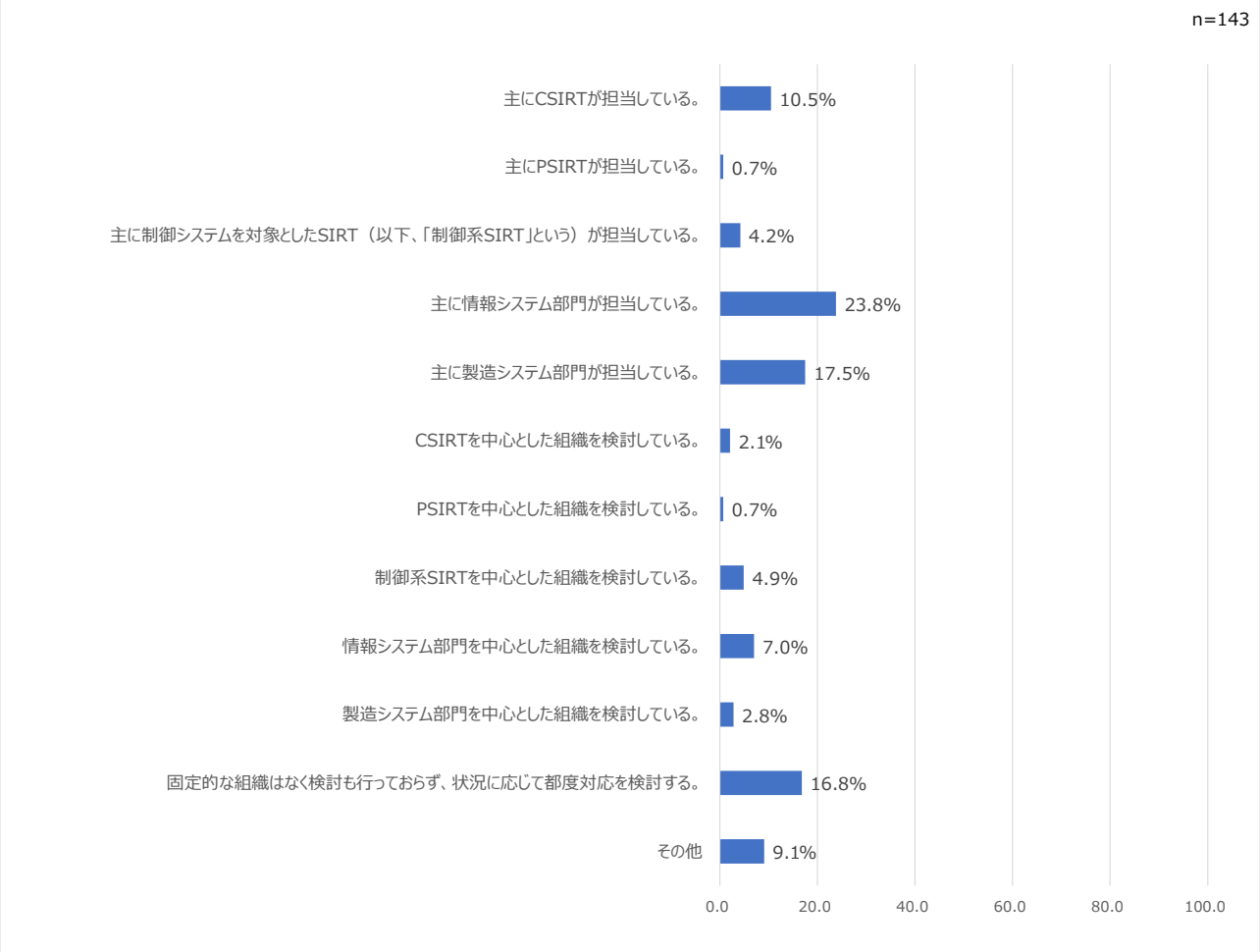


図 4 制御システムインシデント対応体制

(2) 制御システムインシデント対応体制の所属員数

設問番号	4-1-2
設問	貴社の制御システムインシデント対応体制の所属員数、そのうちの専任者数をお答えください。
回答形態	自由記述

- 自由記述回答集計結果

本設問への回答結果（自由記述集計）を図 5 に示す。制御システムインシデント対応体制の所属員数について、「所属員数が 0 人」と回答した事業者が 37.7%と最も多く、次点で「所属員数が 1 人以上 5 人未満」と回答した事業者が 19.7%であった。

専任者のみで構成されている組織は 4 社のみであり、全体の 1 割未満にとどまる。

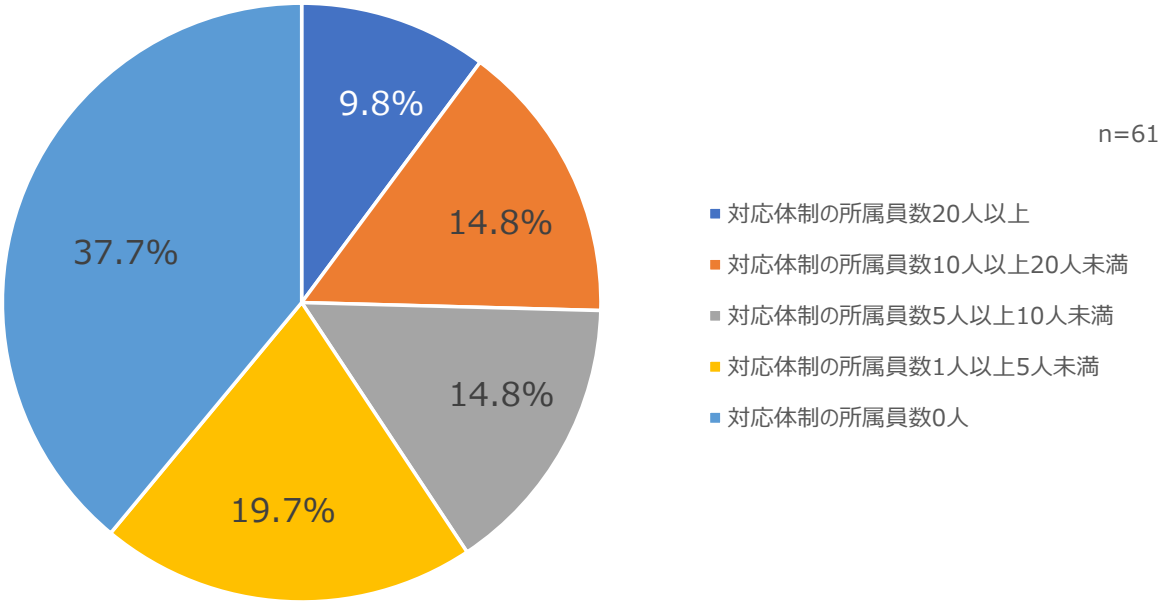


図 5 制御システムインシデント対応体制の組織構成（規模）

(3) 制御システムインシデント対応体制の兼任者の所属部署

設問番号	4-1-3
設問	貴社の制御システムインシデント対応体制の兼任者の所属部署をお答えください。
回答形態	複数回答

- 単純集計結果

本設問への回答結果（単純集計）を図 6 に示す。制御システムインシデント対応体制の兼任者の所属部署について、「情報システム部門」と回答した事業者が 65.5%と最も多く、次点で「製造システム部門」と回答した事業者が 36.1%であった。

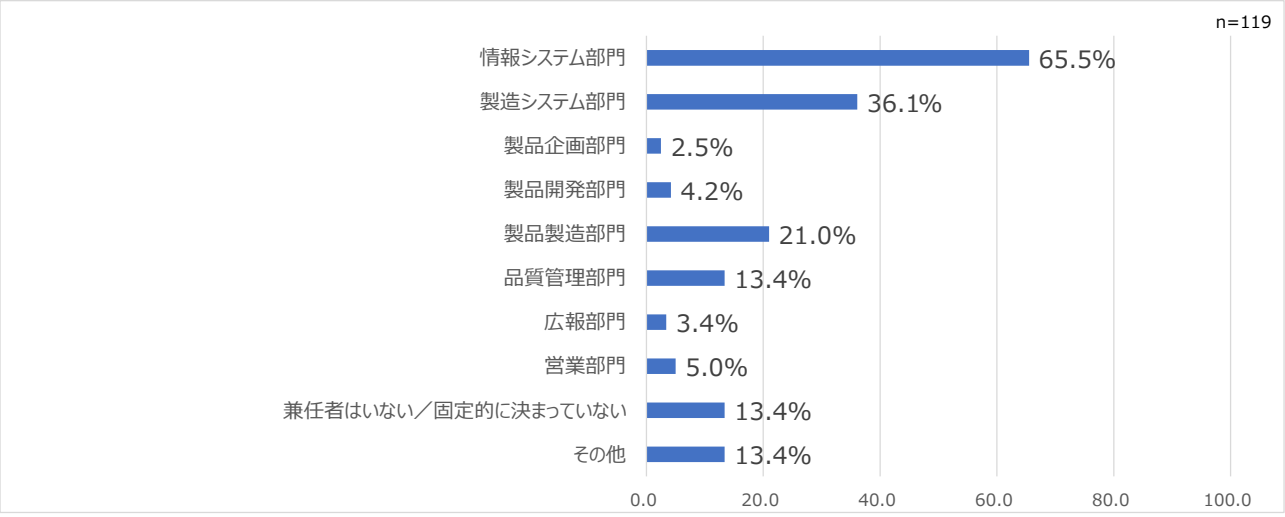


図 6 制御システムインシデント対応体制の組織構成（兼任構成）

● クロス集計結果

本設問への回答結果（クロス集計）を図 7 に示す。

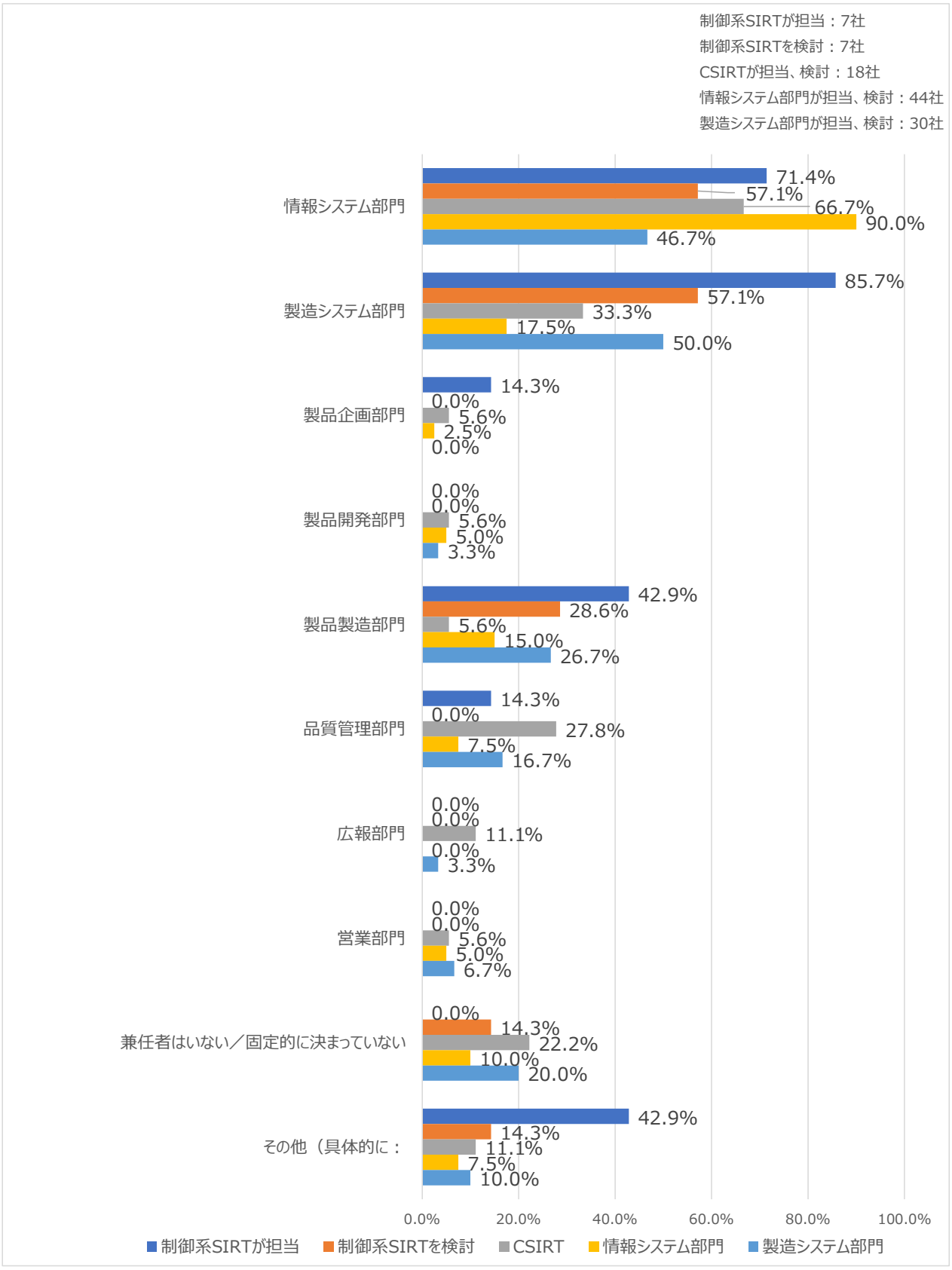


図 7 制御システムインシデント対応体制の組織構成（兼任構成） （クロス集計）

図 7 をもとに、制御システムインシデント対応体制の兼任者の所属部署に関する各組織の特徴について以下に示す。

「制御系 SIRT が担当している事業者」では、「製造システム部門」と回答した事業者が 85.7%（7 社中 6 社）と最も多く、次点で情報システム部門との連携が 71.4%（7 社中 5 社）であった。また、他の製造に関連する部門では、製品製造部門との兼任の割合が 42.9%（7 社中 3 社）であった。

「制御系 SIRT を中心とした組織体制を検討中の事業者」では、製造システム部門・情報システム部門との兼任が 57.1%（7 社中 4 社）であった。他の製造に関連する部署との兼任については、製品製造部門との兼任の割合は 28.6%（7 社中 2 社）にとどまっている。

「CSIRT が担当している事業者/CSIRT を中心とした組織体制を検討中の事業者」では、情報システム部門との兼任が 66.7%（18 社中 12 社）であり、製造に関連する部署との兼任については、「製造システム部門」33.3%（18 社中 6 社)、「品質管理部門」27.8%（18 社中 5 社）にとどまっている。

「情報システム部門が担当している事業者/情報システム部門を中心とした組織体制を検討中の事業者」では、情報システム部門との兼任が 90.0%（40 社中 36 社）であった。他方、製造に関連する部署との兼任については、「製造システム部門」17.5%（40 社中 7 社)、「製品製造部門」15.0%（40 社中 6 社）にとどまっている。

「製造システム部門が担当している事業者/製造システム部門を中心とした組織体制を検討中の事業者」では、製造システム部門との兼任が「50%」(30 社中 15 社)、情報システム部門との兼任が「46.7%」（30 社中 14 社）であった。

「制御系 SIRT が担当している事業者」では、他の対応体制と比較し、製造システム部門との兼任の割合が一番高く、また他の製造に関連する部門(製品製造部門) と兼任していると回答した事業者が 42.9%（7 社中 3 社）と一番高い。すなわち、製造に関連する部門との連携を強化する上では、制御系 SIRT のような存在が必要であると示唆される。

(4) 制御システムインシデント対応体制の連携先の所属部署

設問番号	4-1-4
設問	貴社における「制御システムインシデント」への対応準備に当たって、制御システムインシデント対応体制が連携する (連携する可能性のある) 部署はどこですか (例えば、連携先としてルール等で定められている部署はどこですか)。
回答形態	複数回答

- 単純集計結果

本設問への回答結果（単純集計）を図 8 に示す。制御システムインシデント対応体制の連携先の部署について、「情報システム部門」と回答した事業者が 79.8%と最も多く、次点で「経営層（マネジメント上層部：社長、担当役員、CISO、工場長、ライン長、等)」と回答した事業者が 71.4%であった。

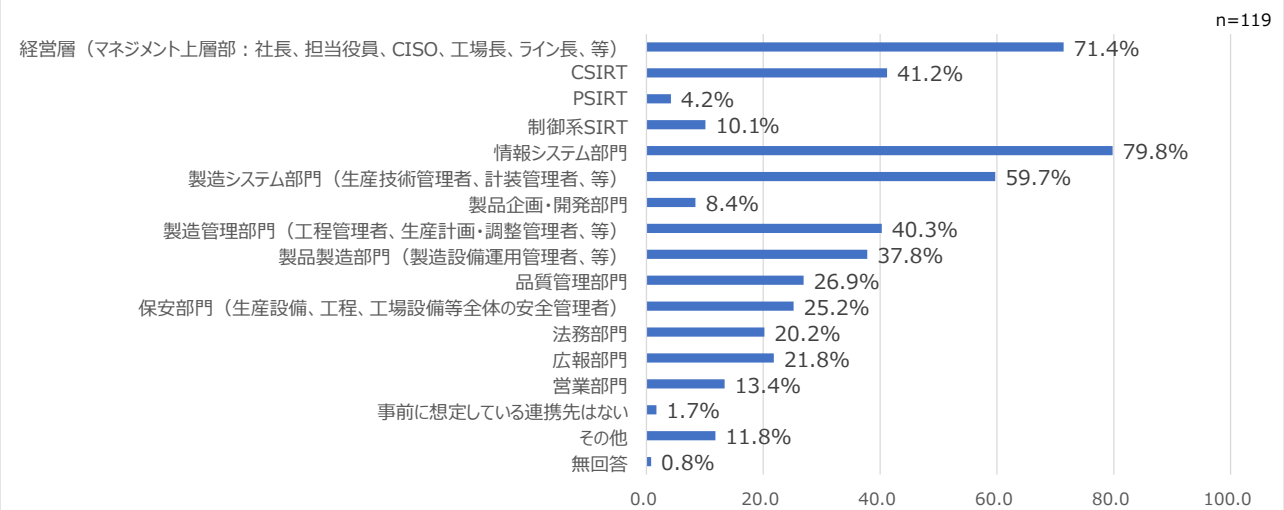


図 8 制御システムインシデント対応体制の組織構成（連携先）

● クロス集計結果

本設問への回答結果（クロス集計）を図９に示す。

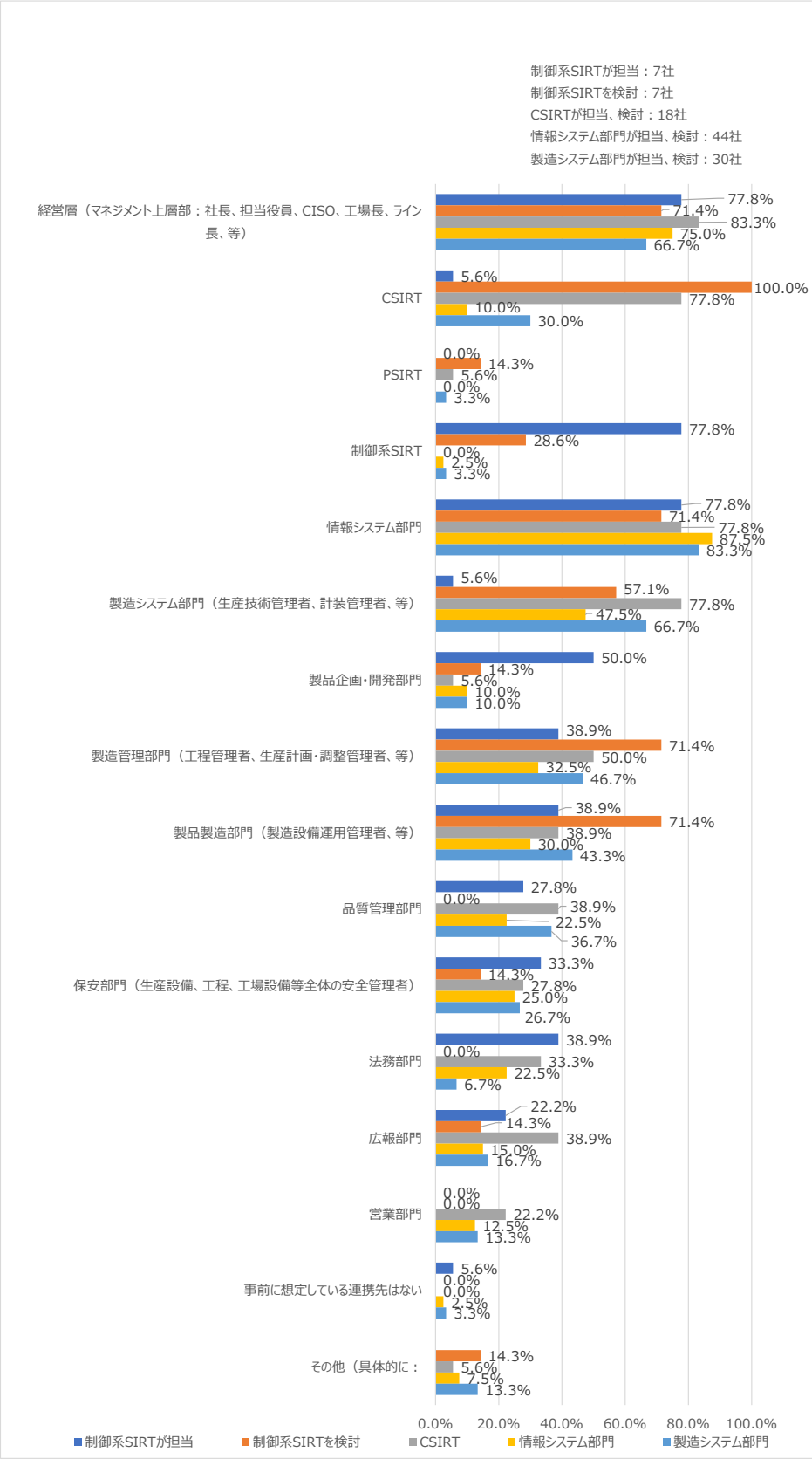


図９ 制御システムインシデント対応体制の組織構成（連携先）（クロス集計）

図 9 をもとに、制御システムインシデント対応体制の連携先の部署に関する各組織の特徴について以下に示す。

制御システムインシデント対応体制の連携先の部署について、「制御系 SIRT が担当している事業者」の内、全事業者（7 社中 7 社）が「CSIRT」「情報システム部門」「製造システム部門（生産技術管理者、計装管理者、等）」と連携を実施していると回答した。また、「経営層（マネジメント上層部：社長、担当役員、CISO、工場長、ライン長、等）」と連携を実施していると回答した事業者が 85.7%（7 社中 6 社）であり、「製造管理部門（工程管理者、生産計画・調整管理者、等）」「製品製造部門（製造設備運用管理者、等）」「保安部門（生産設備、工程、工場設備等全体の安全管理者）」のような製造に関連する部門との連携を実施していると回答した事業者が 57.1%（7 社中 4 社）であった。

「制御系 SIRT を中心とした組織体制を検討中の事業者」の内、全事業者（7 社中 7 社）が「CSIRT」と連携を実施していると回答した。また、「経営層（マネジメント上層部：社長、担当役員、CISO、工場長、ライン長、等）」「情報システム部門」「製造管理部門（工程管理者、生産計画・調整管理者、等）」「製品製造部門（製造設備運用管理者、等）」との連携を実施していると回答した事業者が 71.4%（7 社中 5 社）であった。

「CSIRT が担当している事業者/CSIRT を中心とした組織体制を検討中の事業者」では、「経営層（マネジメント上層部：社長、担当役員、CISO、工場長、ライン長、等）」と連携を実施していると回答した事業者が 83.3%（18 社中 15 社）であった。

「情報システム部門が担当している事業者/情報システム部門を中心とした組織体制を検討中の事業者」では、「情報システム部門」と連携を実施していると回答した事業者が「87.5%」（40 社中 35 社）であった。「経営層（マネジメント上層部：社長、担当役員、CISO、工場長、ライン長、等）」との連携を実施していると回答した事業者は 75.0%（40 社中 30 社）であった。

「製造システム部門が担当している事業者/製造システム部門を中心とした組織体制を検討中の事業者」では、「情報システム部門」と連携を実施していると回答した事業者が 83.3%（30 社中 25 社）であり、次点で「経営層（マネジメント上層部：社長、担当役員、CISO、工場長、ライン長、等）」「製造システム部門（生産技術管理者、計装管理者、等）」と連携を実施していると回答した事業者が 66.7%（30 社中 20 社）であった。

クロス集計の対象の事業者の内、経営層・情報システム部門との連携を実施していると回答した事業者は少なくとも 6 割以上であるが、製造に関連する部門との連携は限定的である。他方、「制御系 SIRT が担当している事業者」では、他の対応体制と比較し、多様な部門との連携が実施されている。すなわち、製造に関連する部門との連携を強化する上では、制御系 SIRT のような存在が必要であると示唆される。

(5) 制御システムインシデント対応体制の制御システムインシデントに向けたベンダー等との連携体制

設問番号	4-3-3
設問	貴社の制御システムインシデント対応体制は、制御システムインシデントに備えてベンダ等とどのような日常の連携体制を構築しているか、その程度と併せてお答えください。
回答形態	複数回答

- 単純集計結果

本設問への回答結果（単純集計）を図 10 に示す。制御システムインシデント対応体制の制御システムインシデントに向けたベンダー等との連携体制について、「制御システムに係るシステムベンダや機器ベンダとの保守契約等により、セキュリティ上の緊急時にもすぐに連携可能である。」「制御システムに係るシステムベンダや機器ベンダとは、セキュリティ上の緊急時にスポット対応の依頼が可能である。」は同率の 35.8%であった。

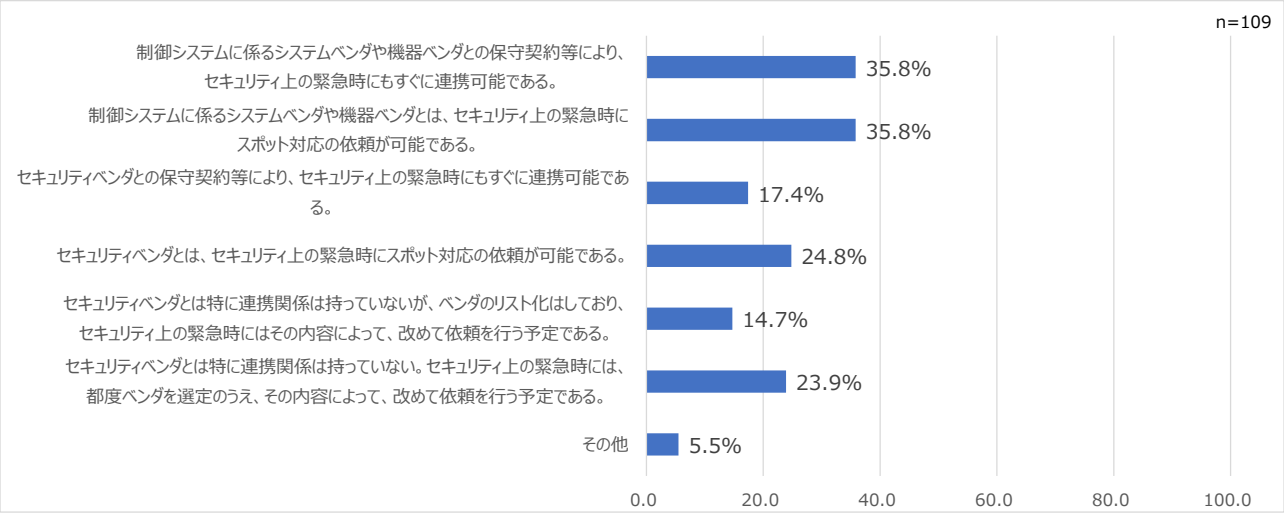


図 10 制御システムインシデントに向けたベンダー等との連携体制

● クロス集計結果

本設問への回答結果（クロス集計）を図 11 に示す。

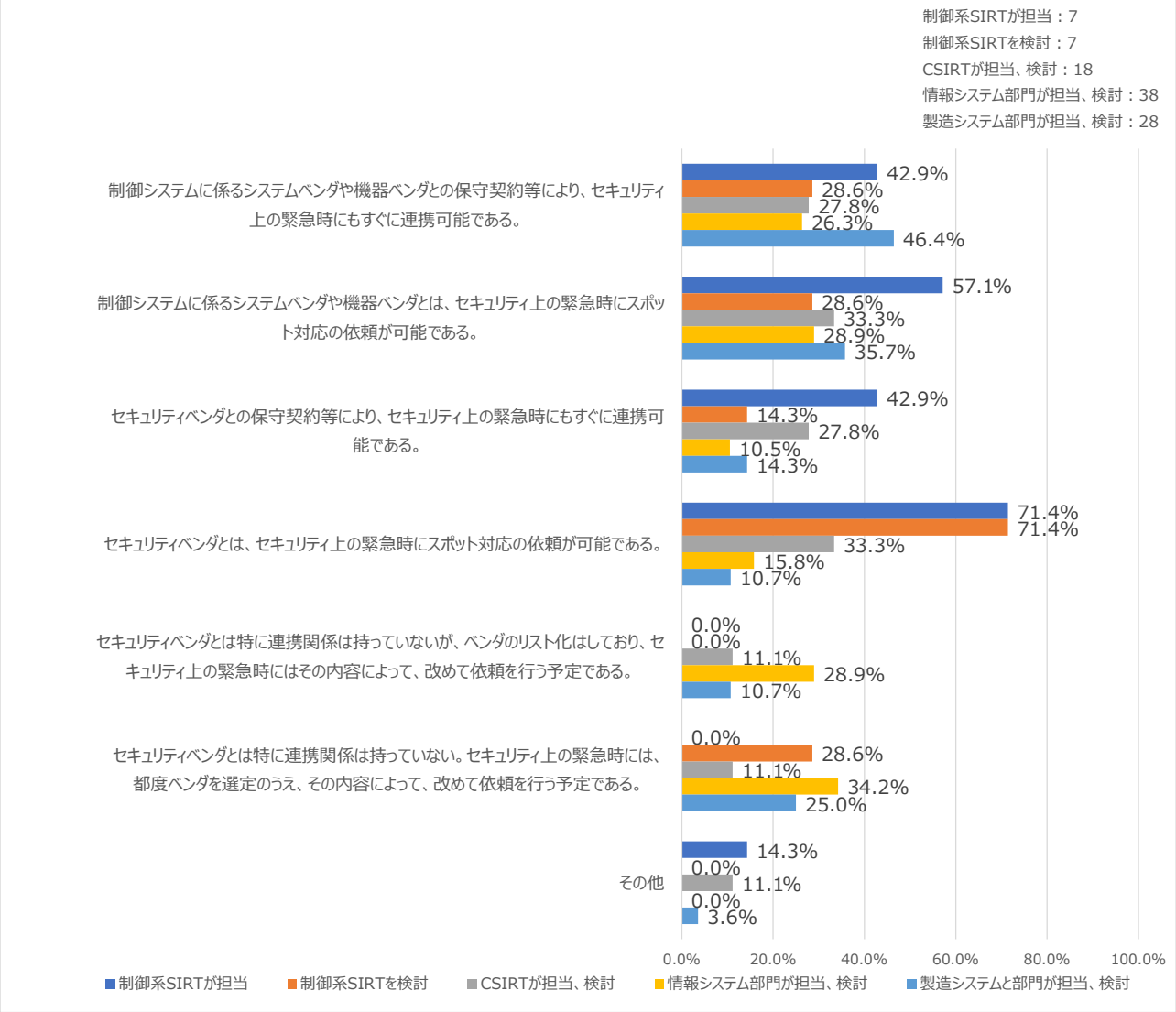


図 11 制御システムインシデントに向けたベンダー等との連携体制（クロス集計）

図 11 をもとに、制御システムインシデントに向けたベンダー等との連携体制に関する各組織の特徴について以下に示す。

制御システムインシデントに向けたベンダー等との連携体制について、「制御系 SIRT が担当している事業者」の内、全事業者（7 社中 7 社）が制御システムに関わるシステムベンダー、機器ベンダー、セキュリティベンダーと何かしらの連携を行っている。「制御系 SIRT が担当している事業者」の内、「セキュリティベンダとは、セキュリティ上の緊急時にスポット対応の依頼が可能である。」と回答した事業者が 71.4%（7 社中 5 社）であった。また、「制御システムに係るシステムベンダや機器ベンダとは、セキュリティ上の緊急時にスポット対応の依頼が可能である。」と回答した事業者が 57.1%（7 社中 4 社）であり、「制御システムに係るシステムベンダや機器ベンダとの保守契約等により、セキュリティ上

の緊急時にもすぐに連携可能である。」と回答した事業者が 42.9%（7 社中 3 社）である。
「制御系 SIRT を中心とした組織体制を検討中の事業者」の内、「セキュリティベンダとは、セキュリティ上の緊急時にスポット対応の依頼が可能である。」と回答した事業者が 71.4%（7 社中 5 社）であった。他方、「制御システムに係るシステムベンダや機器ベンダとの保守契約等により、セキュリティ上の緊急時にもすぐに連携可能である。」や、「制御システムに係るシステムベンダや機器ベンダとは、セキュリティ上の緊急時にスポット対応の依頼が可能である。」と回答した事業者は 28.6%（7 社中 2 社）、「セキュリティベンダとの保守契約等により、セキュリティ上の緊急時にもすぐに連携可能である。」と回答した事業者は 14.3%（7 社中 1 社）にとどまっている。
「CSIRT が担当している事業者/CSIRT を中心とした組織体制を検討中の事業者」では、「制御システムに係るシステムベンダや機器ベンダとは、セキュリティ上の緊急時にスポット対応の依頼が可能である。」「セキュリティベンダとは、セキュリティ上の緊急時にスポット対応の依頼が可能である。」と回答した事業者が 33.3%（18 社中 6 社）がであった。ベンダーとの連携ルールを定める事業者は、最高でも全体の 3 割程度にとどまっている。
「情報システム部門が担当している事業者/情報システム部門を中心とした組織体制を検討中の事業者」では、「セキュリティベンダとは特に連携関係は持っていない。セキュリティ上の緊急時には、都度ベンダを選定のうえ、その内容によって、改めて依頼を行う予定である。」と回答した事業者が 34.2%（38 社中 13 社）であり、他の組織体制と比較した際に最も多い。
「製造システム部門が担当している事業者/製造システム部門を中心とした組織体制を検討中の事業者」では、「制御システムに係るシステムベンダや機器ベンダとの保守契約等により、セキュリティ上の緊急時にもすぐに連携可能である。」と回答した事業者が 46.4%（28 社中 13 社）であり、他の組織体制と比較した際に最も多い。
クロス集計対象の事業者の内、「制御系 SIRT が担当している事業者」「制御系 SIRT を中心とした組織体制を検討中の事業者」においては、「セキュリティベンダとは、セキュリティ上の緊急時にスポット対応の依頼が可能である。」と回答した事業者が 71.4%であった。また、「製造システム部門が担当している事業者/製造システム部門を中心とした組織体制を検討中の事業者」においては、「制御システムに係るシステムベンダや機器ベンダとの保守契約等により、セキュリティ上の緊急時にもすぐに連携可能である。」と回答した事業者が 46.4%であり、他の組織体制と比較した際に最も多い。
すなわち、ベンダー等との連携においては、製造に関連する部門を中心に取り組まれていることが推察される。そのため、ベンダーとの連携においては、制御系 SIRT のような存在の構築が望まれる他、製造に関連する部門との連携が望まれる。他方、CSIRT においては、現状 7 割程度の兼任先・連携先が製造システム部門であり、ベンダー等との連携を行う上では、連携の内容や方法に関する今後の課題が示唆される。

(6) 制御システムインシデント対応体制の組織化の背景

設問番号	4-4-1
設問	貴社において制御システムインシデント対応体制を組織したきっかけや背景について近いものをお答えください。
回答形態	複数回答

- 単純集計結果

本設問への回答結果（単純集計）を図 12 に示す。制御システムインシデント対応体制の組織化の背景について、「業界的レベルでの制御システムのサイバーセキュリティ対策への機運の高まり、啓発活動等を踏まえて、自社の取組の必要性を感じるようになった。」は 43.1%と最も多かった。

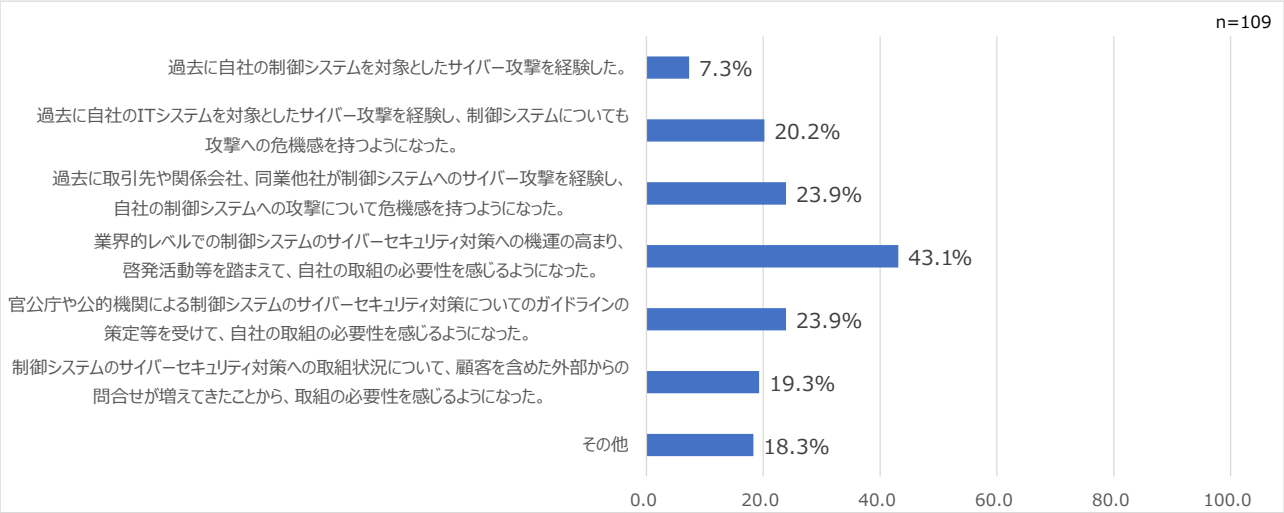


図 12 制御システムインシデント対応体制の組織化の背景

● クロス集計結果

本設問への回答結果（クロス集計）を図 13 に示す。

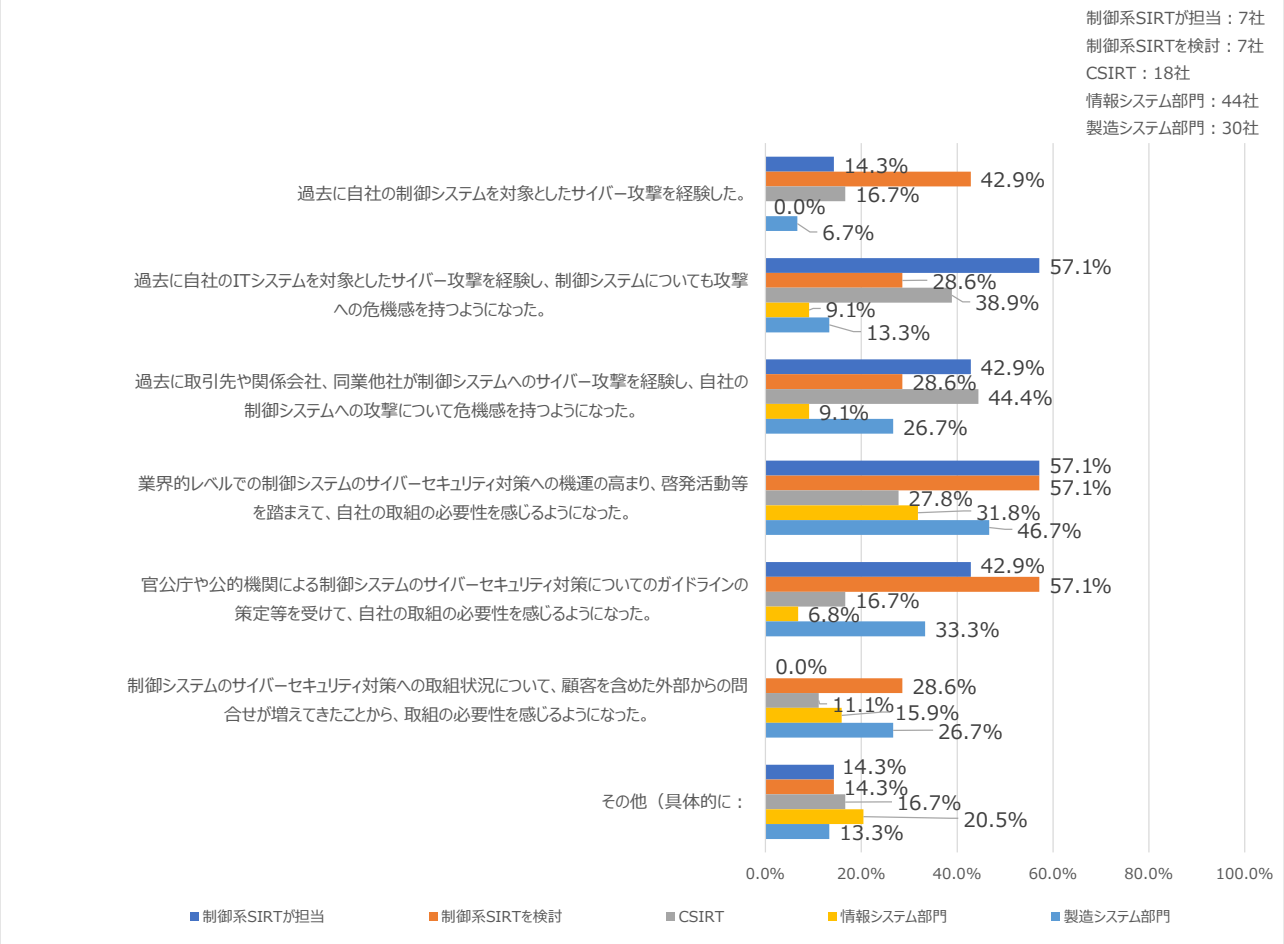


図 13 制御システムインシデント対応体制の組織化の背景（クロス集計）

図 13 をもとに、制御システムインシデント対応体制の組織化の背景に関する各組織の特徴について以下に示す。

制御システムインシデント対応体制の組織化の背景について、「制御系 SIRT が担当している事業者」の内、「過去に自社の IT システムを対象としたサイバー攻撃を経験し、制御システムについても攻撃への危機感を持つようになった。」「業界的レベルでの制御システムのサイバーセキュリティ対策への機運の高まり、啓発活動等を踏まえて、自社の取組の必要性を感じるようになった。」と回答した事業者が 57.1%（7 社中 4 社）であり、次点で、「過去に取引先や関係会社、同業他社が制御システムへのサイバー攻撃を経験し、自社の制御システムへの攻撃について危機感を持つようになった。」と回答した事業者が 42.9%（7 社中 3 社）であった。

「制御系 SIRT を中心とした組織体制を検討中の事業者」の内、「業界的レベルでの制御システムのサイバーセキュリティ対策への機運の高まり、啓発活動等を踏まえて、自社の取組の必要性を感じるようになった。」「官公庁や公的機関による制御システムのサイバーセキュリティ対策についてのガイドラインの策定等を受けて、自社の取組の必要性を感じるようになった。」と回答した事業者が 57.1%（7 社中 4

社）であり、次点で「過去に自社の制御システムを対象としたサイバー攻撃を経験した。」と回答した事業者が 42.9%（7 社中 3 社）であった。
「CSIRT が担当している事業者/CSIRT を中心とした組織体制を検討中の事業者」では、「過去に取引先や関係会社、同業他社が制御システムへのサイバー攻撃を経験し、自社の制御システムへの攻撃について危機感を持つようになった。」と回答した事業者が 44.4%（18 社中 8 社）であり、次点で「過去に自社の IT システムを対象としたサイバー攻撃を経験し、制御システムについても攻撃への危機感を持つようになった。」と回答した事業者が 38.9%（18 社中 7 社）であった。
「情報システム部門が担当している事業者/情報システム部門を中心とした組織体制を検討中の事業者」では、「業界的レベルでの制御システムのサイバーセキュリティ対策への機運の高まり、啓発活動等を踏まえて、自社の取組の必要性を感じるようになった。」と回答した事業者が 36.8%（38 社中 14 社）であり、他の影響について回答している事業者は、2 割未満であった。
「製造システム部門が担当している事業者/製造システム部門を中心とした組織体制を検討中の事業者」では、「業界的レベルでの制御システムのサイバーセキュリティ対策への機運の高まり、啓発活動等を踏まえて、自社の取組の必要性を感じるようになった。」と回答した事業者が 46.4%（28 社中 13 社）であった。
クロス集計対象の事業者の内、「制御系 SIRT が担当している事業者」「制御系 SIRT を中心とした組織体制を検討中の事業者」では、IT システム、制御系システムに対する自社へのサイバー攻撃の経験が影響を与えたと回答している事業者が複数あることから、制御系 SIRT の構築に当たっては、自社へのサイバー攻撃の有無が影響を与えることが示唆される。また、単純集計結果に加え、個社の自由記述を確認すると、「制御系 SIRT が担当している事業者」「制御系 SIRT を中心とした組織体制を検討中の事業者」では、「製造システム部門と情報システム部門の連携体制だけでは責任部署があいまいで制御セキュリティ施策が進まない」「CSIRT 下の管理体制では不十分」「製造管理部門独自のシステムが存在し情報システム部門だけでは調査・復旧が困難」等の回答をする事業者が複数見られており、制御系 SIRT の構築に当たっては、体制への問題意識の明確化が重要である旨、示唆される。また、すべての組織体制において、割合は異なるものの、共通して業界や官公庁の取り組みに対し関心を示す層が一定数いる。加えて、個社の自由記述において、親会社からの指示で制御システムインシデント対応体制の組織化を検討するようになったと回答した事業者が複数存在した。すなわち、制御システムインシデント対応体制の組織化に当たっては「自社へのサイバー攻撃」「現状の組織体制に対する課題意識」「業界や官公庁、親会社のような外部からの刺激」が影響を与える旨、示唆される。

4.2.2 制御システムインシデント対応体制の機能、役割、活動内容

(1) 制御システムインシデント対応が実施する日常的な取り組み

設問番号	4-3-1
設問	貴社の制御システムインシデント対応体制が日常的な取組としてどのような活動を実施しているかお答えください。
回答形態	複数回答

● 単純集計結果

本設問への回答結果（単純集計）を図 14 に示す。制御システムインシデント対応体制が実施する日常的な取組について、「管理対象の制御システムに関する資産管理」と回答した事業者が 64.2%と最も多く、次点で「制御システムに係る社内関係者向けセキュリティ教育、普及啓発活動」と回答した事業者が 61.5%であった。

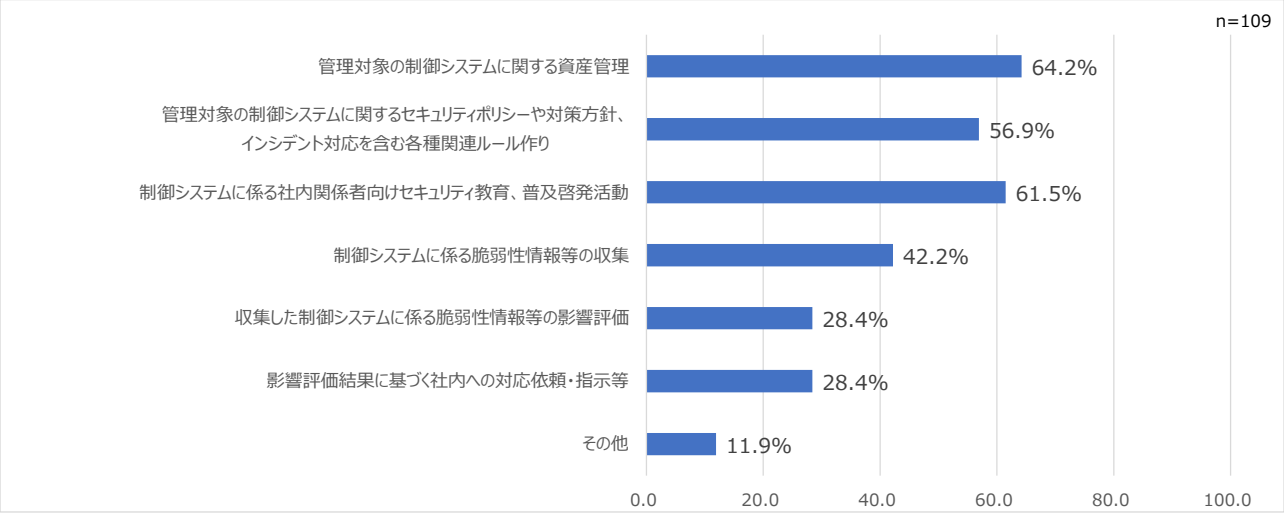


図 14 制御システムインシデント対応体制の日常の取り組み

● クロス集計結果

本設問への回答結果（クロス集計）を図 15 に示す。

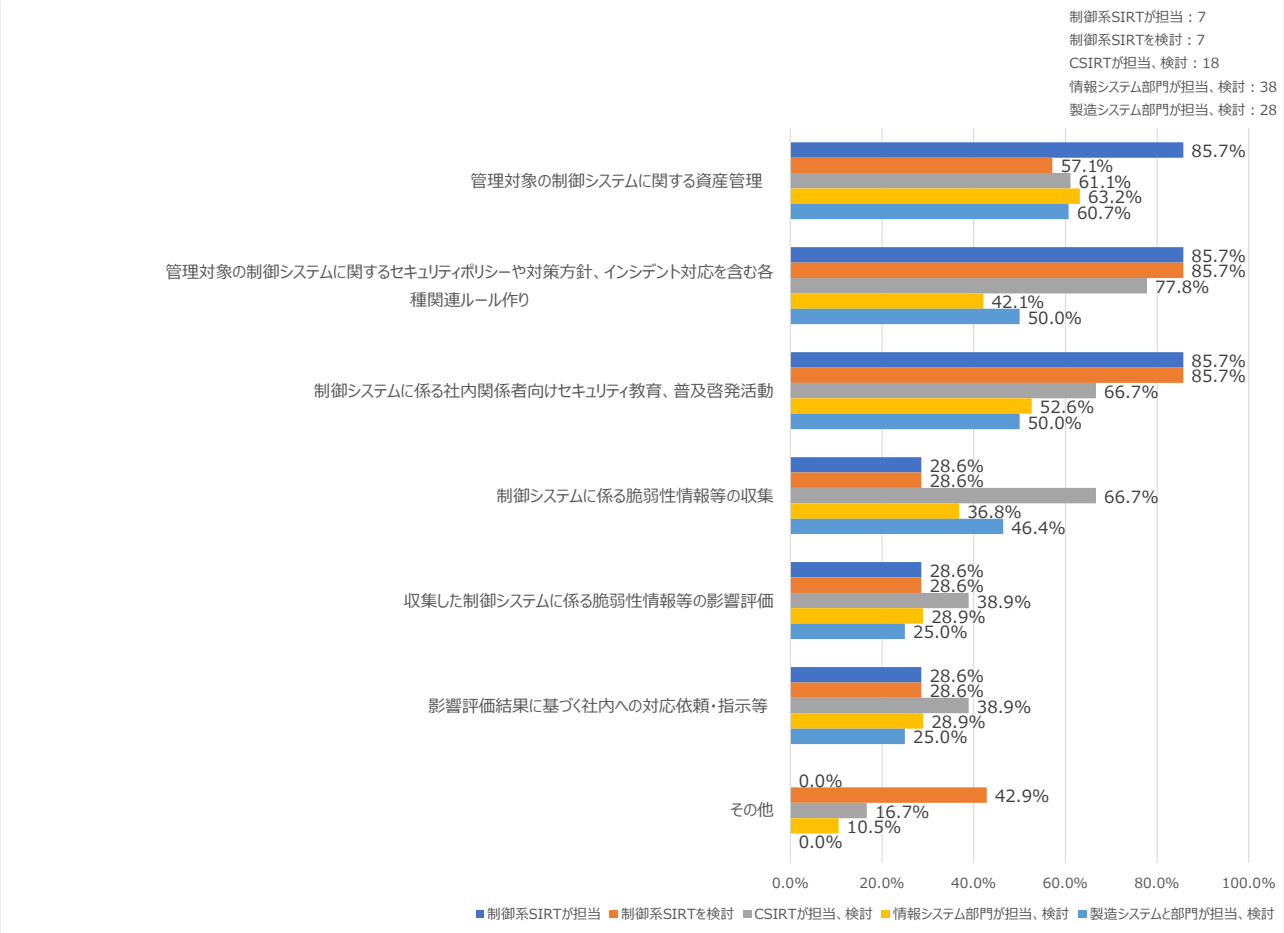


図 15 制御システムインシデント対応体制の日常の取り組み（クロス集計）

図 15 をもとに、制御システムインシデント対応体制の日常の取り組みに関する各組織の特徴について以下に示す。

制御システムインシデント対応体制が実施する日常的な取り組みについて、「制御系 SIRT が担当している事業者」の内、85.7%（7 社中 6 社）が「管理対象の制御システムに関する資産管理」「管理対象の制御システムに関するセキュリティポリシーや対策方針、インシデント対応を含む各種関連ルール作り」「制御システムに係る社内関係者向けセキュリティ教育、普及啓発活動」を実施している。

「制御系 SIRT を中心とした組織体制を検討中の事業者」の内、85.7%（7 社中 6 社）が「管理対象の制御システムに関するセキュリティポリシーや対策方針、インシデント対応を含む各種関連ルール作り」「制御システムに係る社内関係者向けセキュリティ教育、普及啓発活動」を実施している。また、57.1%（7 社中 4 社）が「管理対象の制御システムに関する資産管理」を実施している。

「CSIRT が担当している事業者/CSIRT を中心とした組織体制を検討中の事業者」の内、77.8%（18 社中 14 社）が「管理対象の制御システムに関するセキュリティポリシーや対策方針、インシデント対応を含む各種関連ルール作り」を実施しており、次点で 66.7%（18 社中 12 社）が、「制御システムに係る

社内関係者向けセキュリティ教育、普及啓発活動」「制御システムに係る脆弱性情報等の収集」を実施している。61.1%（18 社中 11 社）が「管理対象の制御システムに関する資産管理」を実施している。
「情報システム部門が担当している事業者/情報システム部門を中心とした組織体制を検討中の事業者」の内、63.2%（38 社中 24 社）が「管理対象の制御システムに関する資産管理」を実施している。
「製造システム部門が担当している事業者/製造システム部門を中心とした組織体制を検討中の事業者」の内、60.7%（28 社中 17 社）が「管理対象の制御システムに関する資産管理」を実施しており、次点で 50.0%（28 社中 14 社）が「管理対象の制御システムに関するセキュリティポリシーや対策方針、インシデント対応を含む各種関連ルール作り」「制御システムに係る社内関係者向けセキュリティ教育、普及啓発活動」を実施している。また、46.4%（28 社中 14 社）が「制御システムに係る脆弱性情報等の収集」を実施しており、この内半数は「収集した制御システムに係る脆弱性情報等の影響評価」「影響評価結果にもとづく社内への対応依頼・指示等」まで実施している。
クロス集計対象の事業者においては、「管理対象の制御システムに関する資産管理」「管理対象の制御システムに関するセキュリティポリシーや対策方針、インシデント対応を含む各種関連ルール作り」「制御システムに係る社内関係者向けセキュリティ教育、普及啓発活動」に関する取り組みを進める事業者が一部見られる。
「管理対象の制御システムに関する資産管理」については、「制御系 SIRT が担当している事業者」が取り組んでいる割合が最も多い。アンケートの結果のみではどの資産を対象に必要な資産管理の実施がどの程度できているか確認することは難しいものの、制御系システムを対象とした資産管理の実施においては社内外問わず幅広い連携が求められることから、社内外における連携が進んでいる制御系 SIRT がある事業者においては、他の組織体制に比較し、資産管理の取り組みが進んでいる可能性が推定される。
「制御システムに係る脆弱性情報等の収集」について、「CSIRT が担当している事業者/CSIRT を中心とした組織体制を検討中の事業者」が取り組んでいる割合が最も多い。制御系 SIRT がある事業者の内、専任者を確保している事業者は 1 社だけであることから、情報収集は CSIRT を中心に行われている可能性が示唆される一方で、情報収集後の取り組みが限定的であることから、収集した脆弱性情報の利用については CSIRT の組織体制では課題があることが推定される。CSIRT 体制における製造システム部門との連携が望まれるが、現状 7 割程度が製造システム部門と連携していることから、脆弱性情報の収集、影響評価、評価結果に基づく対応を行う上では、連携の内容や方法に関する今後の課題が示唆される。

4.2.3 制御システムインシデント対応体制の課題

(1) 制御システムインシデント対応体制の組織的課題

設問番号	4-4-2
設問	貴社における制御システムインシデント対応体制の取組に関して、組織的課題や改善が必要な点についてお答えください。
回答形態	複数回答

- 単純集計結果

本設問への回答結果（単純集計）を図 16 に示す。制御システムインシデント対応体制の組織的課題について、「兼任者が多く、取組の機動性が担保できない。」と回答した事業者が 49.0%と最も多く、次点で「社内に専門人材が少なく、ベンダ等の支援を得ているが、それにも限界がある。」と回答した事業者が 48.0%であった。

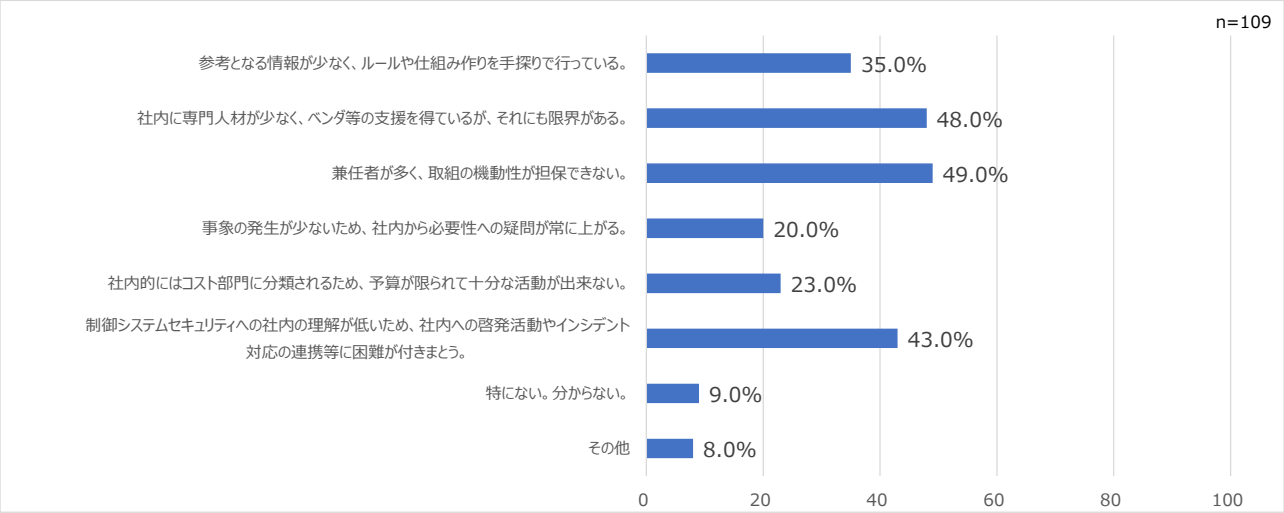


図 16 制御システムインシデント対応体制の組織的課題

● クロス集計結果

本設問への回答結果（クロス集計）を図 17 に示す。

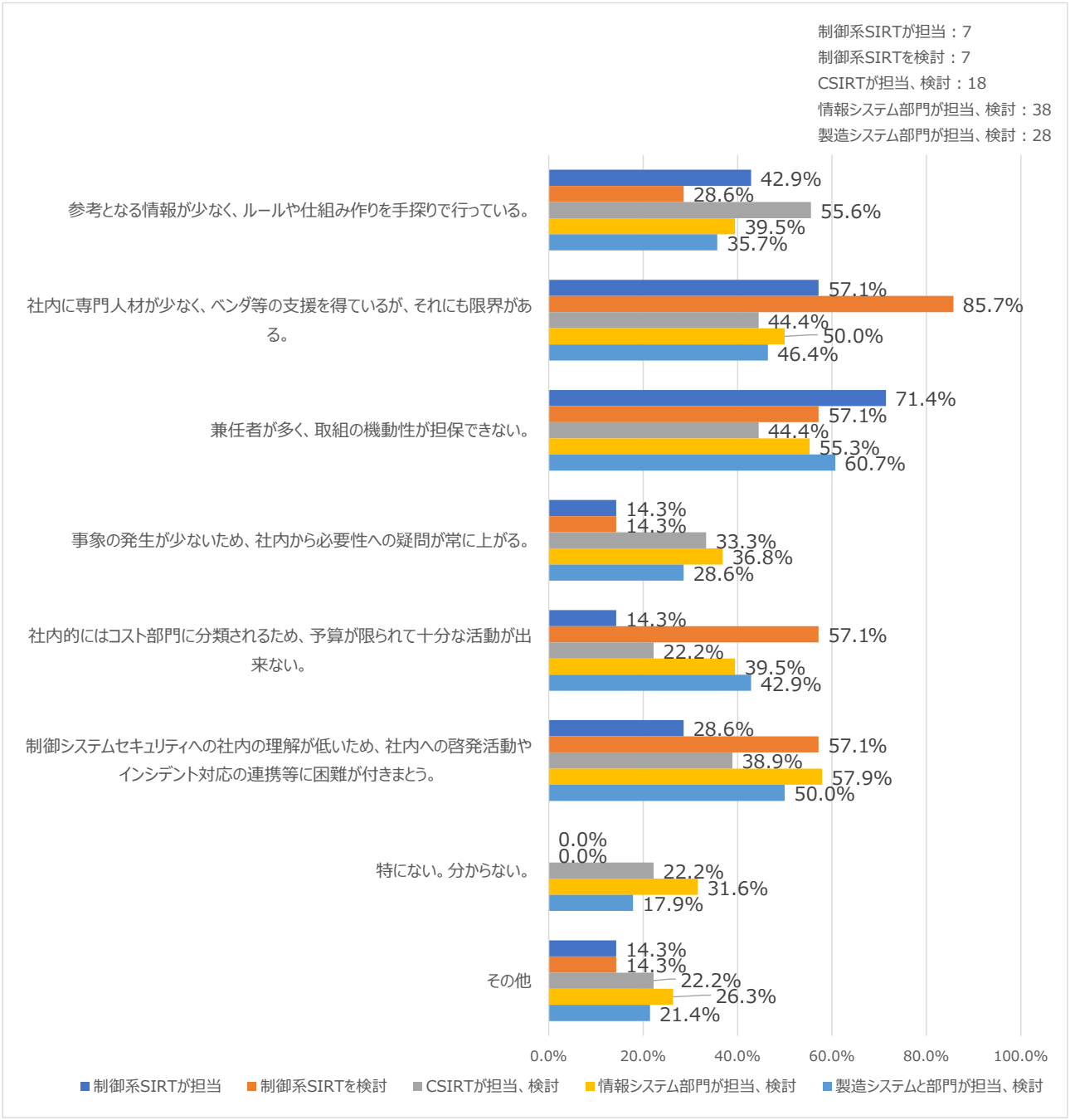


図 17 制御システムインシデント対応体制の組織的課題（クロス集計）

図 17 をもとに、制御システムインシデント対応体制の組織的課題に関する各組織の特徴について以下に示す。

制御システムインシデント対応体制の組織的課題について、「制御系 SIRT が担当している事業者」の内、71.4%（7 社中 5 社）が「兼任者が多く、取組の機動性が担保できない。」を課題として挙げている。次点で 57.1%（7 社中 4 社）が「社内に専門人材が少なく、ベンダ等の支援を得ているが、それにも限

界がある。」、42.9%（7 社中 3 社）が「参考となる情報が少なく、ルールや仕組み作りを手探りで行っている。」を課題として挙げている。

「制御系 SIRT を中心とした組織体制を検討中の事業者」の内、85.7%（7 社中 6 社）が「社内に専門人材が少なく、ベンダ等の支援を得ているが、それにも限界がある。」を課題として挙げている。次点で 57.1%（7 社中 4 社）が「兼任者が多く、取組の機動性が担保できない。」「社内的にはコスト部門に分類されるため、予算が限られて十分な活動が出来ない。」「制御システムセキュリティへの社内の理解が低いため、社内への啓発活動やインシデント対応の連携等に困難が付きまとう。」を課題として挙げている。

「CSIRT が担当している事業者/CSIRT を中心とした組織体制を検討中の事業者」の内、55.6%（18 社中 10 社）が「参考となる情報が少なく、ルールや仕組み作りを手探りで行っている。」を課題として挙げている。

「情報システム部門が担当している事業者/情報システム部門を中心とした組織体制を検討中の事業者」の内、57.9%（38 社中 22 社）が「制御システムセキュリティへの社内の理解が低いため、社内への啓発活動やインシデント対応の連携等に困難が付きまとう。」を課題として挙げている。次点で 55.3%（38 社中 21 社）が「兼任者が多く、取組の機動性が担保できない。」を課題として挙げている。

「製造システム部門が担当している事業者/製造システム部門を中心とした組織体制を検討中の事業者」の内、60.7%（28 社中 17 社）が「兼任者が多く、取組の機動性が担保できない。」を課題として挙げている。次点で 50.0%（28 社中 14 社）が「制御システムセキュリティへの社内の理解が低いため、社内への啓発活動やインシデント対応の連携等に困難が付きまとう。」を課題として挙げている。

クロス集計対象の事業者においては、「制御系 SIRT が担当している事業者」「CSIRT が担当している事業者/CSIRT を中心とした組織体制を検討中の事業者」においては、「制御システムセキュリティへの社内の理解が低いため、社内への啓発活動やインシデント対応の連携等に困難が付きまとう。」を挙げている事業者が 4 割以下である一方で、「制御系 SIRT を中心とした組織体制を検討中の事業者」「情報システム部門が担当している事業者/情報システム部門を中心とした組織体制を検討中の事業者」「製造システム部門が担当している事業者/製造システム部門を中心とした組織体制を検討中の事業者」においては、半数以上が課題として認識している。「制御系 SIRT を検討している事業者」においては、約 8 割 5 分が社内の関係者向けにセキュリティ教育・普及啓発活動を実施していることから実施内容や対象を見直す必要性が示唆される。

また、「制御系 SIRT が担当している事業者」においては「兼任者が多く、取組の機動性が担保できない。」が課題として挙げられている一方で、「制御系 SIRT を検討している事業者」においては「社内に専門人材が少なく、ベンダ等の支援を得ているが、それにも限界がある。」に対する課題を抱えている事業者が最も多く、次点で「兼任者が多く、取組の機動性が担保できない。」「社内的にはコスト部門に分類されるため、予算が限られて十分な活動が出来ない。」「制御システムセキュリティへの社内の理解が低いため、社内への啓発活動やインシデント対応の連携等に困難が付きまとう。」を課題として挙げており、組織化に至るまでの課題と、組織化に至ってからの課題に差異があることが示唆される。

(2) 制御システムインシデント対応体制の技術的課題

設問番号	4-4-3
設問	貴社における制御システムインシデント対応体制の取組に関して、技術的課題や改善が必要な点についてお答えください。
回答形態	複数回答

● 単純集計結果

本設問への回答結果（単純集計）を図 18 に示す。制御システムインシデント対応体制の技術的課題について、「制御システムインシデントの経験が無いまたは限られるため、実際の事象にあって必要な技術的対応が取れる保証がない。 」が 59.6%と最も多かった。

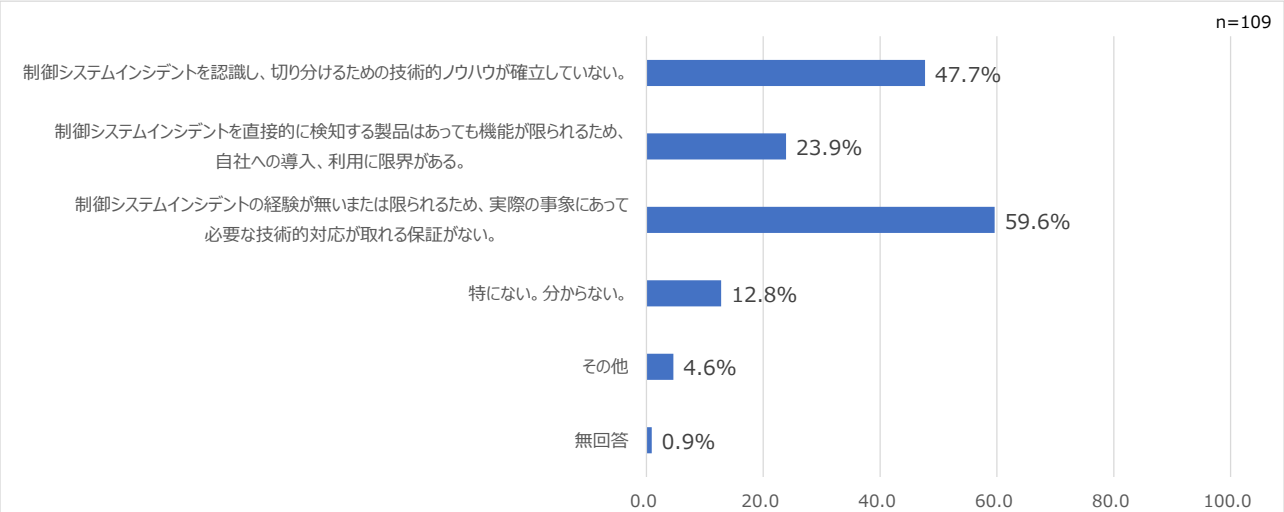


図 18 制御システムインシデント対応体制の技術的課題

● クロス集計結果

本設問への回答結果（クロス集計）を図 19 に示す。

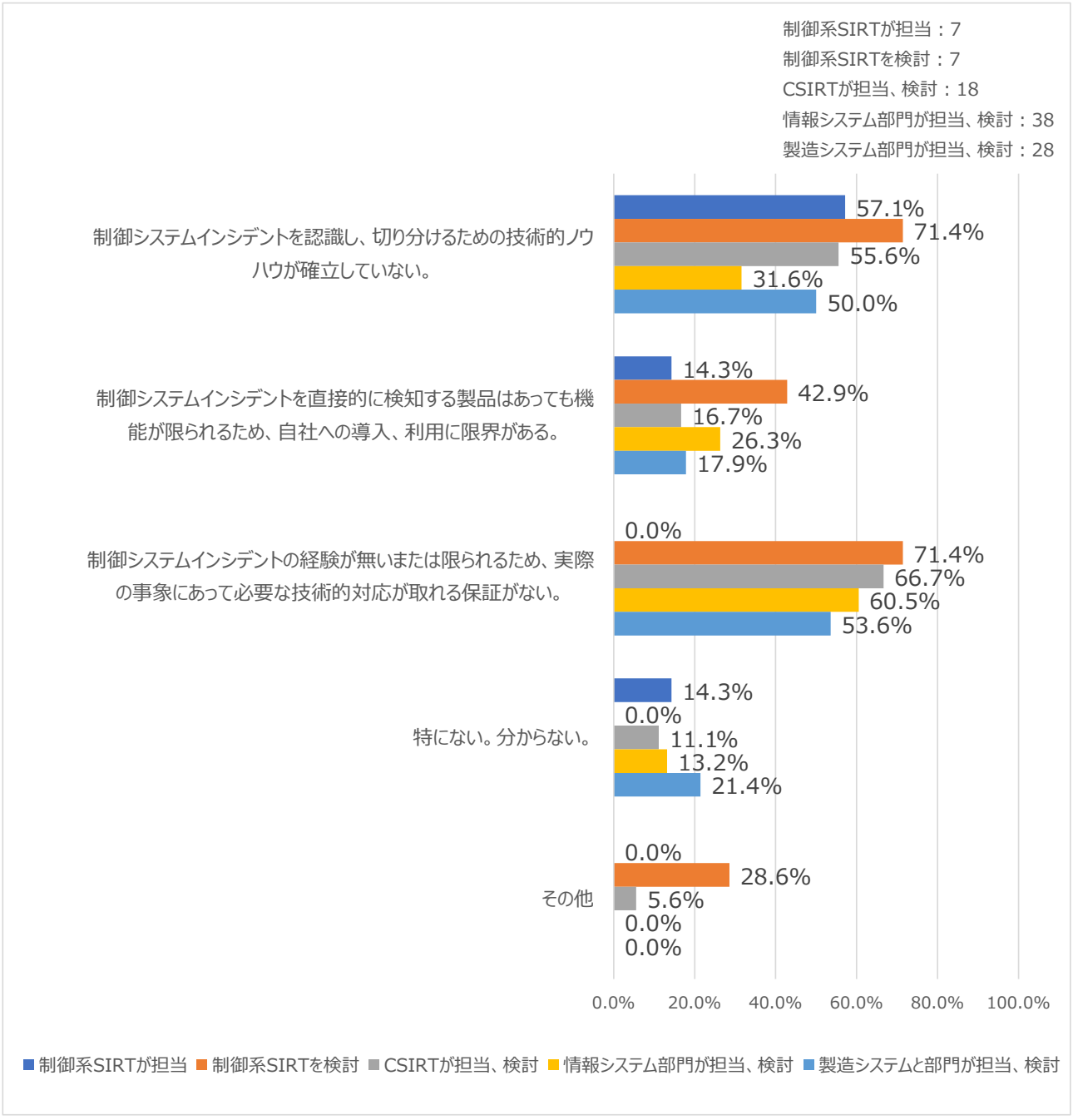


図 19 制御システムインシデント対応体制の技術的課題（クロス集計）

図 19 をもとに、制御システムインシデント対応体制の技術的課題に関する各組織の特徴について以下に示す。

制御システムインシデント対応体制の組織的課題について、「制御系 SIRT が担当している事業者」の内、「制御システムインシデントを認識し、切り分けるための技術的ノウハウが確立していない。」に対して課題を抱えている事業者が 57.1%（7 社中 4 社）であり、最も多い。他の組織体制と比較し、技術

的な課題を取り上げている事業者が少ない。

「制御系 SIRT を中心とした組織体制を検討中の事業者」においては、「制御システムインシデントを認識し、切り分けるための技術的ノウハウが確立していない。」「制御システムインシデントの経験が無いまたは限られるため、実際の事象にあって必要な技術的対応が取れる保証がない。」に対して課題を抱えている事業者が 71.4%（7 社中 5 社）であり、最も多く、次点で「制御システムインシデントを直接的に検知する製品はあっても機能が限られるため、自社への導入、利用に限界がある。」に対し課題を抱えている事業者が 42.9%（7 社中 3 社）である。

「CSIRT が担当している事業者/CSIRT を中心とした組織体制を検討中の事業者」において、「制御システムインシデントの経験が無いまたは限られるため、実際の事象にあって必要な技術的対応が取れる保証がない。」に対して課題を抱えている事業者が 66.7%（18 社中 12 社）であり、次点で「制御システムインシデントを認識し、切り分けるための技術的ノウハウが確立していない。」 に対し課題を抱えている事業者が 55.6%（18 社中 10 社）である。

「情報システム部門が担当している事業者/情報システム部門を中心とした組織体制を検討中の事業者」においては、「制御システムインシデントの経験が無いまたは限られるため、実際の事象にあって必要な技術的対応が取れる保証がない。」に対して課題を抱えている事業者が 60.5%（38 社中 23 社）であり、次点で「制御システムインシデントを認識し、切り分けるための技術的ノウハウが確立していない。」に対して課題を抱えている事業者が 31.6%（38 社中 12 社）であった。

「製造システム部門が担当している事業者/製造システム部門を中心とした組織体制を検討中の事業者」では、「制御システムインシデントの経験が無いまたは限られるため、実際の事象にあって必要な技術的対応が取れる保証がない。」に対して課題を抱えている事業者が 53.6%（28 社中 15 社）であり、次点で「制御システムインシデントを認識し、切り分けるための技術的ノウハウが確立していない。」に対して課題を抱えている事業者が 50.0%（28 社中 14 社）であった。

「制御系 SIRT が担当している事業者」と「制御系 SIRT を中心とした組織体制を検討中の事業者」を比較すると、「制御系 SIRT が担当している事業者」では技術的課題を挙げている事業者が限定的である一方で、「制御系 SIRT を中心とした組織体制を検討中の事業者」においては複数の技術的課題を抱えている事業者が多く、制御系 SIRT の組織化が技術的課題の解決に影響を与える可能性が示唆される。また、「制御システムインシデントの経験が無いまたは限られるため、実際の事象にあって必要な技術的対応が取れる保証がない。」に対して、「制御系 SIRT が担当している事業者」は課題を抱えていると回答した事業者が全くなかったが、その他の組織体制では 5 割以上が課題を抱えていると回答していることから、制御系 SIRT がある事業者では一定の制御システムインシデントの経験を有しており、有事の際の技術的対応に対して一定の取り組みを実施できることが示唆される。

5. 課題解決策や今後の取り組みの検討と提言

アンケートの単純集計およびクロス集計で得られた情報をもとに、制御系 SIRT が必要とされる理由、構築に当たって実施すべきことや解決するべき課題等を整理し、そのために取り組むことが求められることを提言としてまとめた。

5.1 制御系 SIRT の構築に向けた課題の整理

以下のような流れで、制御系 SIRT が必要とされる理由、構築に当たって実施すべきことや解決すべき課題を図 20 のフローで整理した。さらに、構築後に留意すべきことや将来的な姿を整理した。

- 制御システムインシデント対応体制が抱える課題を、アンケートおよび詳細ヒアリングの結果から以下のとおりに整理を行った。
- その中でも、アンケートおよび詳細ヒアリングの結果から共通的に確認できた 3 つの課題について、制御システムユーザーにおいて推奨される活動を詳細ヒアリングの内容をもとに提言する。

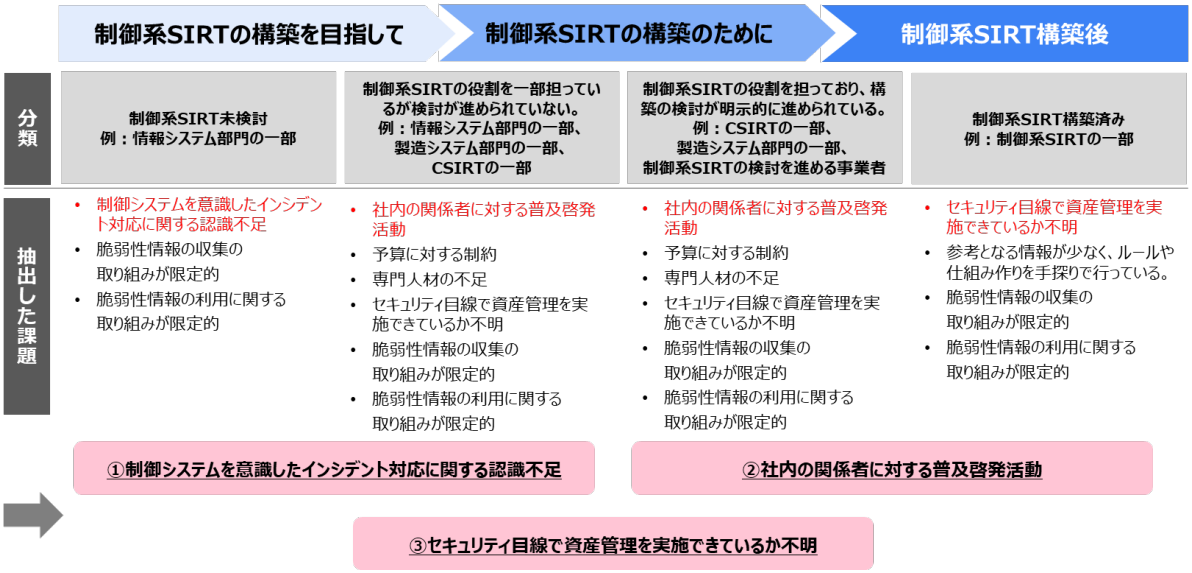


図 20 制御系 SIRT 構築に向けた整理のフロー

5.2　提言：3 つの課題に対して制御システムユーザーに求められる取り組み

上記の流れで整理した 3 つの課題に対して、制御システムユーザーが目指すべき体制とそのために取り組むことが求められることを提言としてまとめた。

5.2.1　提言①：制御システムを意識したインシデント対応に関する認識不足の改善

1 つ目の課題である「制御システムを意識したインシデント対応に関する認識不足」の改善のため、次の点を提言する。

- IT システムと比較して制御システムインシデントの対応では特徴的な点があるため、**制御システムを意識したインシデント対応の必要性を訴える**ことが重要である。図 21 はそのアプローチを示したものである。
- ヒアリングでは、他社のインシデントやガイドライン・規格がきっかけとなり、制御システムを意識したインシデント対応の検討が進められた事例が多く、**必要性を訴える上で、業界における制御セキュリティに関する情報を取りまとめる**ことが重要だと考えられる。
- 制御システムを意識したインシデント対応においては、IT／OT 連携が重要であり、ヒアリングで確認できたとおり、インシデント時の連携ルールの構築や仮想的な組織の構築でも十分な対応となる。制御システムを意識したインシデント対応を行う上で、**専門組織の構築が必ずしも必要ではなく、各社の状況に応じてコストが少なく最適な体制を整備する**ところから始めることが重要である。

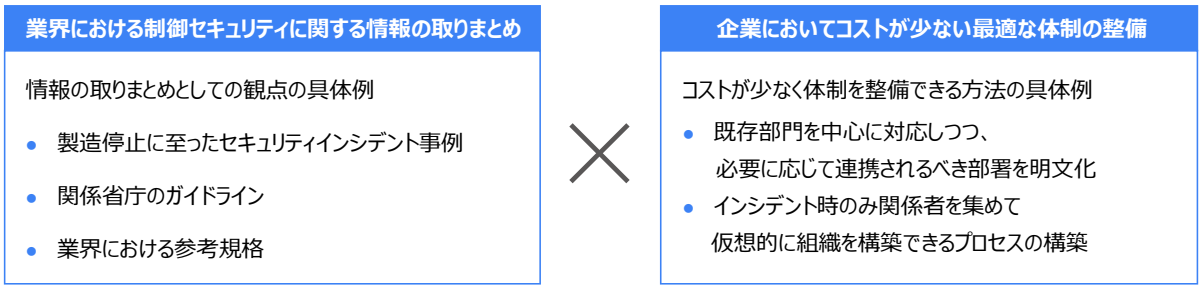


図 21 制御システムを意識したインシデント対応へのアプローチ

5.2.2　提言②：社内の関係者に対する制御システムセキュリティの普及促進

次に、2 つ目の課題である「社内の関係者に対する普及啓発活動」の促進のため、次の点を提言する。

- 社内の関係者に対する普及啓発活動も制御システムのインシデント対応を検討・運用する上で重要である。図 22 はその施策例を示したものである。

- 特に制御系インシデントを予防・対応できる体制を構築する上では、**工場現場の従業員に対するサイバーセキュリティの考え方の浸透が不可欠である。**
- 考え方を浸透させる上で、**工場現場に対するセキュリティ教育が重要な施策**である。また、セキュリティ教育だけでなく、**人事制度の一部としてセキュリティに関する業務の重要性を向上させることも効果的な施策**である。

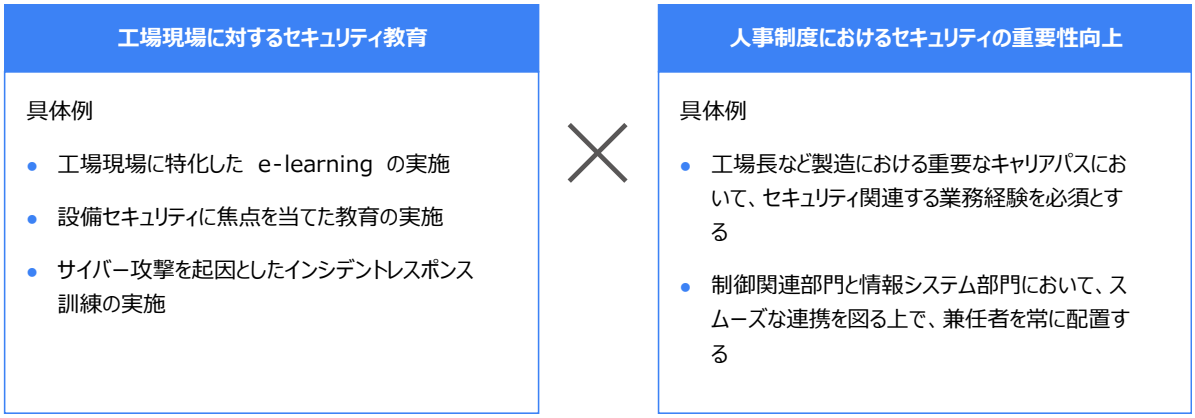


図 22 社内関係者への制御システムにおけるセキュリティの普及施策例

5.2.3 提言③：セキュリティ対応を考慮した資産管理の実施

3 つ目の課題である「セキュリティ目線で資産管理を実施できているか不明」の改善のため、次の点を提言する。

- 資産管理は、平時においては脆弱性が含まれている機器の特定など、有事においては制御システムインシデントの原因特定など、さまざまなタイミングで活用され、より強固な制御システムインシデント体制を構築する上で、重要な活動である。
- 図 23 に示すように、セキュリティ対応を考慮した資産管理を行う上で、目的と対象範囲が重要な観点となる。管理すべき項目に関しては、IT と OT とで大きな変わりはないが、OT では資産管理の対象範囲を拡大する際に必要なコストが大幅に増加すると考えられる。

目的と最低限管理すべき項目の一例

目的	最低限管理すべき項目
制御システムインシデントの原因特定	機器名・IPアドレス
脆弱性特定	機器名・バージョン情報
サプライチェーン管理	機器名・機器ベンダ・購入先
SBOM生成	機器名・ソフトウェア・バージョン情報

資産管理の対象範囲の整理の一例

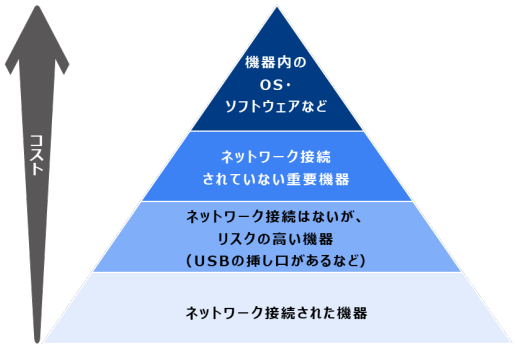
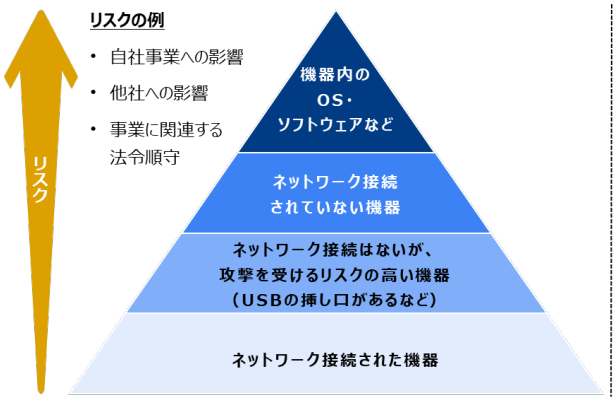


図 23 OT 資産管理における管理対象範囲とコストとの関係

- 対象範囲を広げるとコストが上がるため、企業のセキュリティの目的に応じて、所定のコストの範囲で対象を指定する必要がある。そのためには、**リスクベースで重要な機器などに限定した上で、対象を明確にすることが重要**である。
- また、資産管理を行う上で、**新規設備に対して導入する際に登録を行うような仕組みを構築することも重要**である。すべての新規設備ではなく、ネットワーク接続される機器や USB の挿し口がある機器などに限定することも考えられる。

リスクベースの資産管理について



資産管理に向けた機器登録の仕組み

具体例

- ITネットワークに接続される機器に関して情報システム部門に登録する
- IPアドレスが与えられる機器に関して帳簿登録する
- USBの挿し口がある機器について資産帳簿に登録する

図 24 リスクベースの資産管理の考え方の例および機器登録の仕組みの例

6. まとめ

本実態調査は制御システムに関するセキュリティの取り組み、特にサイバーインシデントに関して、一般製造業者がどのように対応しようとしているのか、体制やルール等の整備状況、インシデントに備えた各種の準備状況、そして実際にインシデントに際しての対応等の状況を広く実態調査したものである。これまでは断片的にしか把握できていなかったこれらの状況をある程度整理することができたとともに、制御系 SIRT（必ずしも専用の物理的組織とは限らず、バーチャルに必要な機能を持ち寄った組織なども含む）にまつわる現状の課題や、課題解決のためにそのような組織が必要である理由、備えるべき機能、整備に向けて取り組むべきこと等の提言とあわせて取りまとめている。

今後は今回の調査結果や提言内容を踏まえて、一般製造業者において制御系 SIRT に類する活動や取り組みがより盛んになり、制御システムインシデントの予防や発生時の効果的な対応に結び付くことを期待している。

なお、本実態調査を通して作成した提言については、調査において参考とされたインシデント事例もまだ限られたものであることから、今後さらに読者各位の実践の場で活用され、そのフィードバックを得ることで、より効果的な取り組みを支援するための JPCERT/CC による各種施策の立案につなげていきたいと考えている。

JPCERT CC®

Appendix1：図表

JPCERT CC®

Appendix2：表