経済産業省

資料5

# 令和４年度に行った調査結果及び今後の取組について

経済産業省

サイバーセキュリティ課

産業機械課

# 目次

# 目次

# 工場セキュリティガイドラインの普及啓発について

第４回工場SWG資料

- 様々な組織において工場システムにおけるセキュリティ推進のための取組が行われている。また、工場システムのセキュリティ関連サービスも続々と国内展開されており、一部については工場セキュリティガイドラインの活用・参照がなされている。
- 今後、アンケート調査により把握する業界・企業等の課題や要望も踏まえ、必要な業界や個社に対して、工場セキュリティガイドラインの普及啓発を進めていく予定である。
- ガイドラインの普及啓発や今後の取組について、以下のような論点を元に御意見をいただきたい。

## 工場セキュリティガイドラインの普及啓発に関する論点

- 特に本ガイドラインを普及させるべき業界はどこか。
- いかなる者を巻き込めば、効果的な本ガイドラインの普及啓発がなされると考えられるか。
  （例：業界団体、コンサル、セキュリティベンダ　等）
- その他、本ガイドライン普及に寄与する取組はあるか。
  （例：ガイドライン実践のためのセミナー・研修、SC3との協力等のコミュニティ形成論）
- 例えば、スマートファクトリに特化したガイドライン等、本ガイドラインのほか、取り組んでいくべき課題はあるか。
- その他

# 目次

# 「工場システムのサイバーセキュリティ対策のアンケート調査」概要

- 経済産業省所管の業界団体を中心に、工場システムのセキュリティに関する対策・課題・要望等を把握することを目的にアンケート調査を実施した。

## 目的

工場システムを中心としたセキュリティに関する対策・課題・要望等の把握

工場セキュリティガイドラインの普及策の検討

**業界団体向けアンケート調査概要**

| | |
|---|---|
| 調査対象 | 経済産業省所管の業界団体<br>配布対象：<br>パルプ・紙・紙加工品製造業<br>業務用機械器具製造業<br>石油製品・石炭製品製造業<br>情報通信機械器具製造業<br>鉄鋼業<br>生産用機械器具製造業<br>電子部品・デバイス・電子回路製造業<br>電気機械器具製造業<br>窯業・土石製品製造業<br>非鉄金属製造業<br>印刷・同関連業<br>化学工業<br>プラスチック製品製造業<br>輸送用機械器具製造業 |
| 依頼数 | 25件 |
| 有効回答数 | 31件※ |
| 調査項目数 | 26項目 |
| 調査項目 | A. 団体の属性情報<br>B. セキュリティ活動状況<br>C. セキュリティ課題<br>D. ガイドライン作成<br>E. ガイドライン認知状況 |
| 調査手法 | Webアンケート調査（任意回答） |
| 調査期間 | 2022年9月～2022年10月 |

※ 依頼した業界団体が複数の業界団体から構成される団体等については、1件の依頼に対して複数の業界団体の回答が得られた場合があり、依頼数と比較して有効回答数が多くなっている。

# 「工場システムのサイバーセキュリティ対策のヒアリング調査」概要

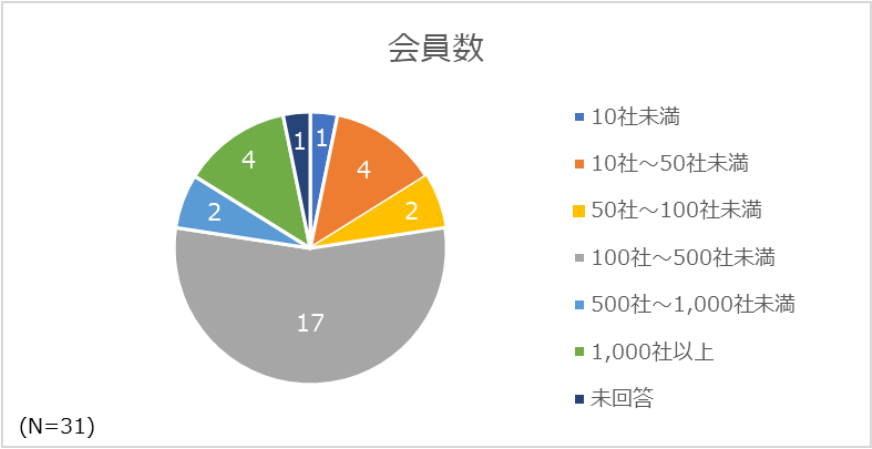
- アンケートに回答いただいた業界団体のうち、セキュリティ活動状況や会員企業のセキュリティ対策状況を考慮し、10団体に対してヒアリングを実施した。
- 業界団体のセキュリティ活動状況、会員企業のセキュリティ対策状況、工場ガイドラインに対する意見、工場ガイドラインの普及活動等について、より具体的な内容を調査した。

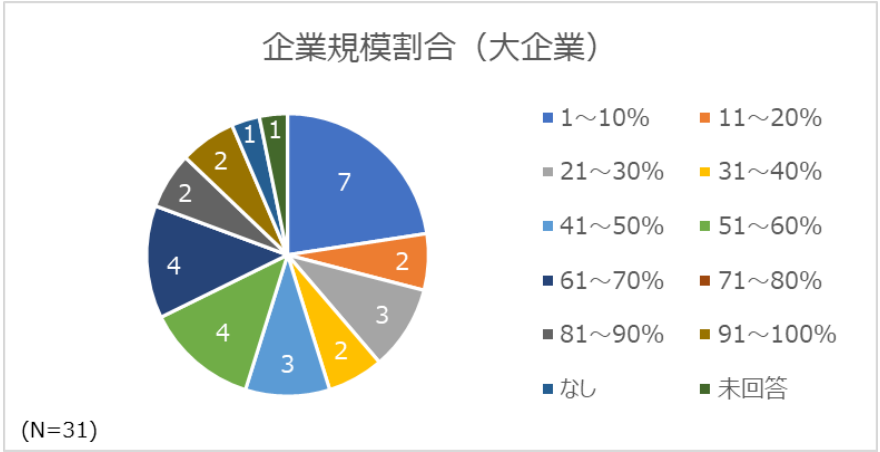
**業界団体向けヒアリング調査概要**

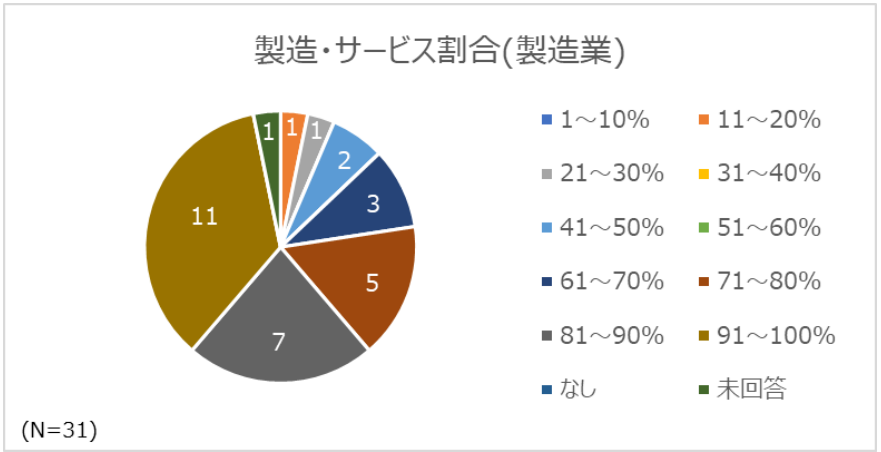
| | |
|---|---|
| 調査対象 | 経済産業省所管の業界団体 |
| ヒアリング件数 | 10件 |
| 調査項目数 | 13項目 |
| 調査項目 | A. 業界団体のサイバーセキュリティ活動状況・展望<br>（サイバーセキュリティ活動内容・活動経緯・課題・影響など）<br>B. 会員企業におけるサイバーセキュリティ対策状況・展望<br>（サイバーセキュリティ対策状況・対策の実施理由など）<br>C. 工場セキュリティガイドラインについて<br>（工場セキュリティガイドラインの難易度・活用可能性など）<br>D. 工場セキュリティガイドラインの普及に向けた活動について<br>（工場セキュリティガイドラインの周知や支援策への協力など） |
| 調査期間 | 2022年12月～2023年2月 |

# （参考）団体の属性情報

- 会員数は、「100社～500社未満」が17団体と最も多かった。
- 企業規模割合（大企業）は「1～10%」が7団体と最も多かった。
- 製造業の割合は、「91%～100%」が11団体と最も多かった。



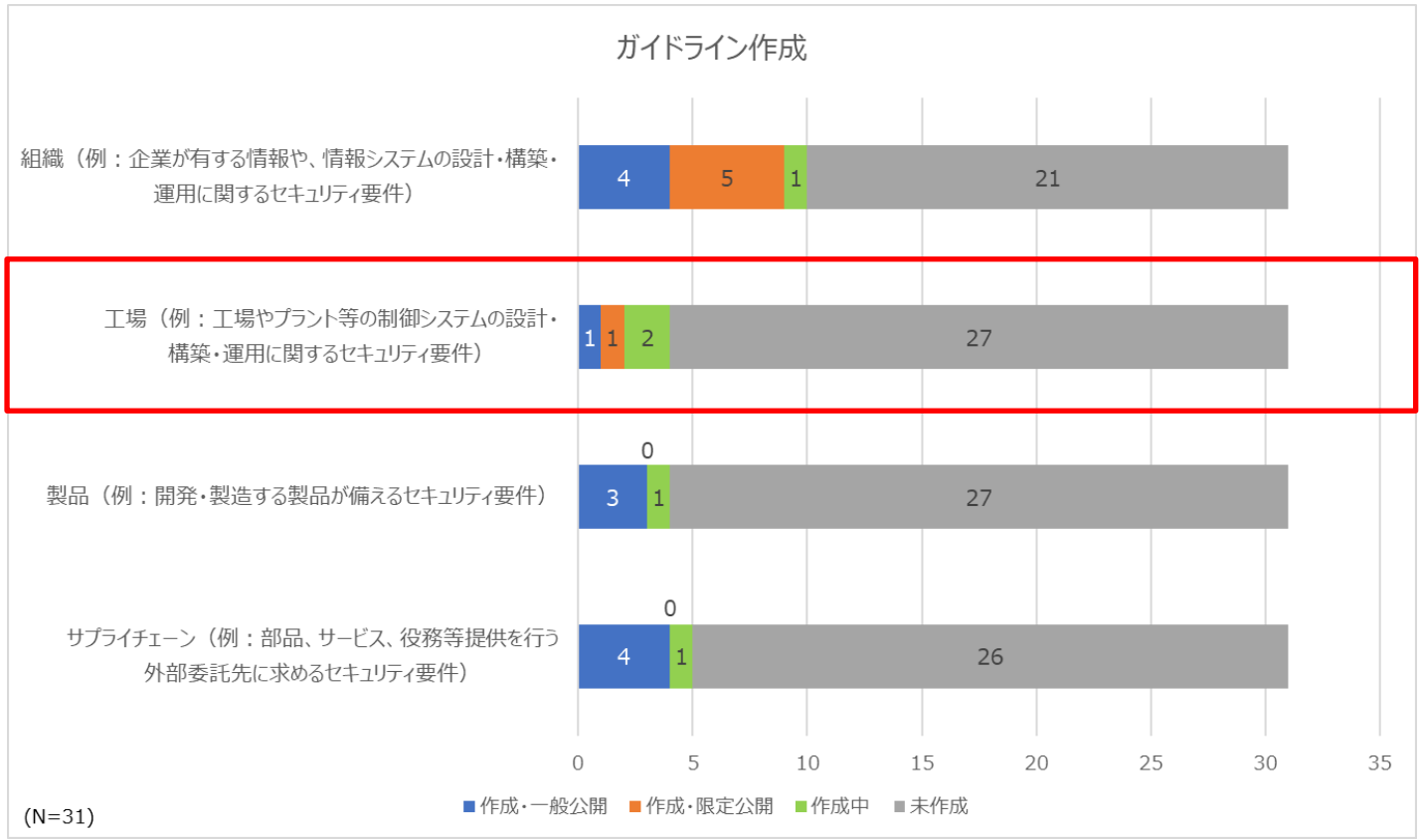



団体向け

# 業界団体におけるセキュリティガイドライン作成状況

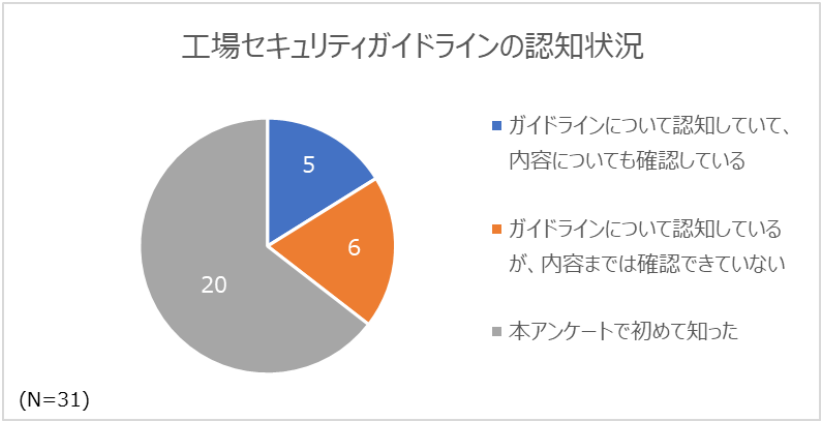
- 「①組織」に関するセキュリティガイドラインについて、「作成・一般公開」、「作成・限定公開」、「作成中」と回答した業界団体は約3割。一方で、「②工場」、「③製品」、「④サプライチェーン」に関するセキュリティガイドラインについて、「作成・一般公開」、「作成・限定公開」、「作成中」と回答した業界団体は約1割。
- 「②工場」は特に作成率が低い。

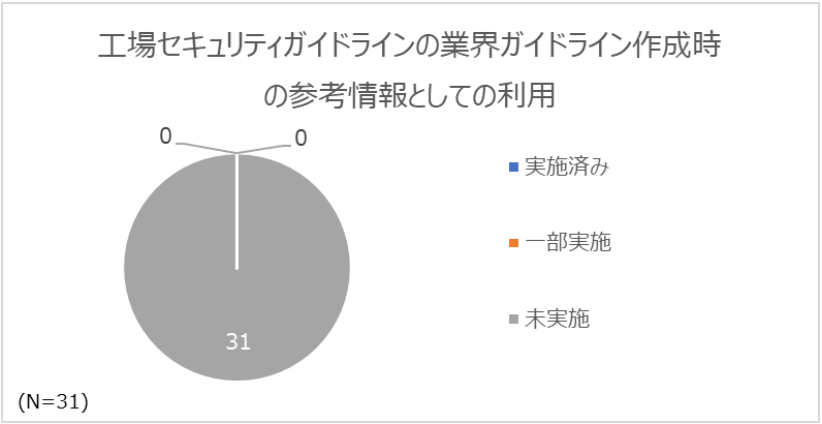


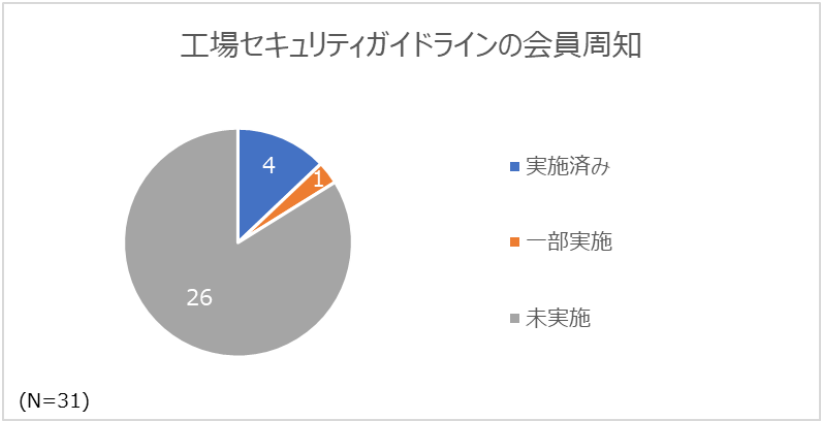
# 工場セキュリティガイドラインの活用状況

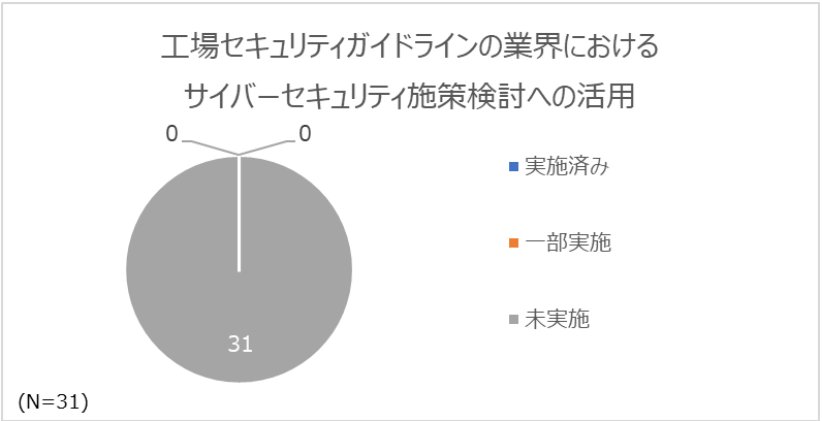
団体向け

- 工場セキュリティガイドラインの認知状況について、「本アンケートで初めて知った」が20団体と最も多かった。
- 工場セキュリティガイドラインの会員周知について、「未実施」が26団体であった。
- 工場セキュリティガイドラインの業界ガイドライン作成時の参考情報としての利用や、業界におけるサイバーセキュリティ施策検討への活用については、「未実施」と全ての団体が回答した。




- 会員周知を「実施済み」と回答した団体が、具体的にどのような方法で周知を実施しているか等を把握する設問は、本アンケートに含まれていない。

# 目次

# 会員企業へのアンケート調査概要

- アンケート調査対象とした業界団体に依頼を行い、業界団体から会員企業に対し、工場システムのセキュリティに関する対策・課題・要望等を把握することを目的にアンケート調査を送付し、任意で回答いただいた。

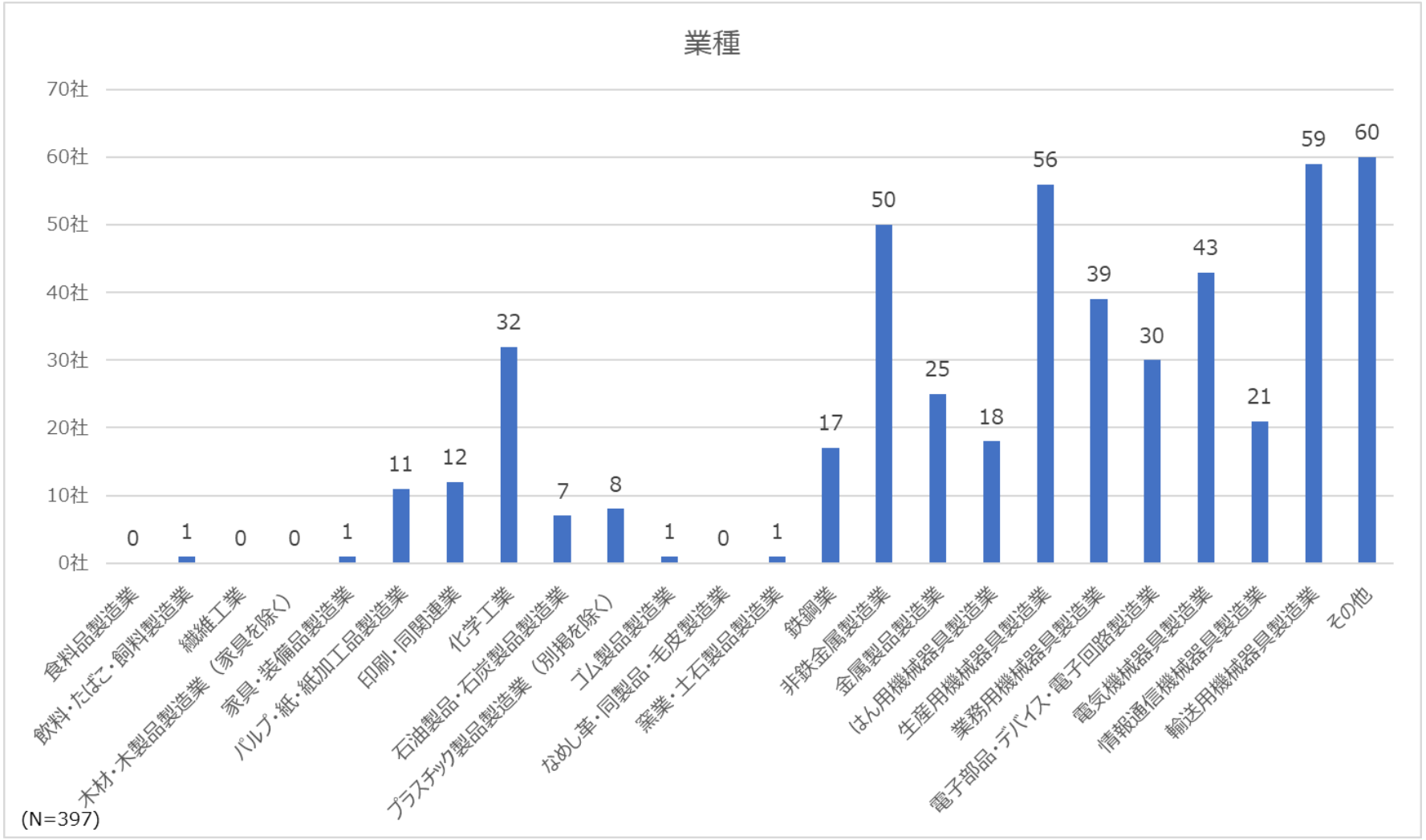
| | |
|---|---|
| 調査対象 | 経済産業省所管の業界団体の会員企業 |
| 有効回答数 | 397件※ |
| 調査項目数 | 71項目 |
| 調査項目 | A. 回答者の属性情報<br>B. 基本セキュリティ対策<br>C. セキュリティインシデント<br>D. 工場におけるデータ分析<br>E. 工場におけるリスク分析<br>F. 工場におけるセキュリティ体制<br>G. 工場における外部委託状況<br>H. 工場における具体のサイバーセキュリティ対策<br>I. サイバーセキュリティ全般における課題や要望について<br>J. 工場セキュリティにおける課題や要望について<br>K. OSSの対策 |
| 調査手法 | Webアンケート調査（任意回答） |
| 調査期間 | 2022年9月～2022年10月 |

※　業界団体経由のため、企業への正確な依頼数は把握できないが、回答のあった企業が所属する業界団体（25団体）の会員企業数を合計すると約2,700件であり、これが概ねの調査送付数と想定される。

個社向け

# （参考）企業回答者の属性情報（1/2）

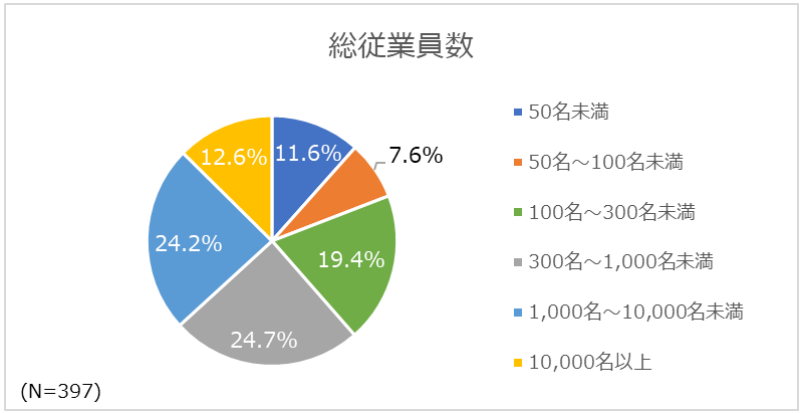
- 業種について、「その他」（60社）が最も多いが、それ以外では「輸送用機械器具製造業」（59社）、「生産用機械器具製造業」（56社）、「非鉄金蔵製造業」（50社）が多い。

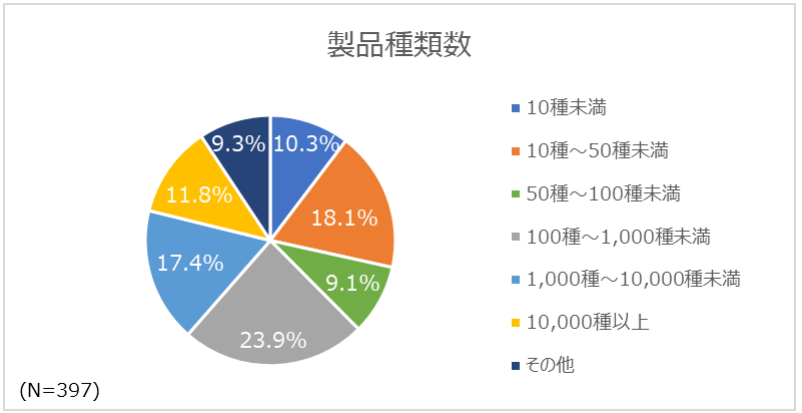


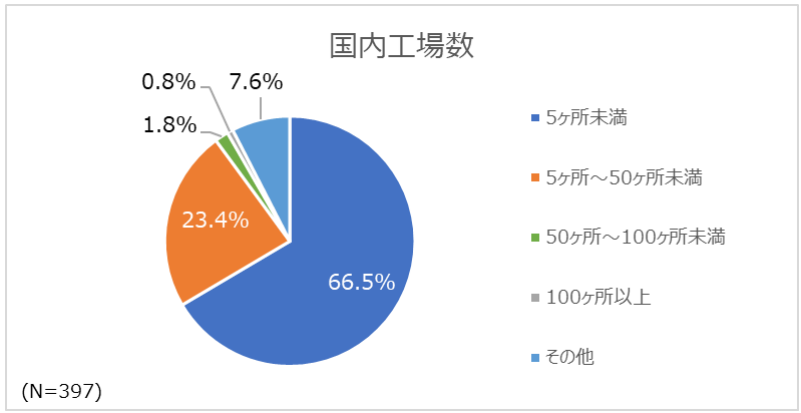
個社向け

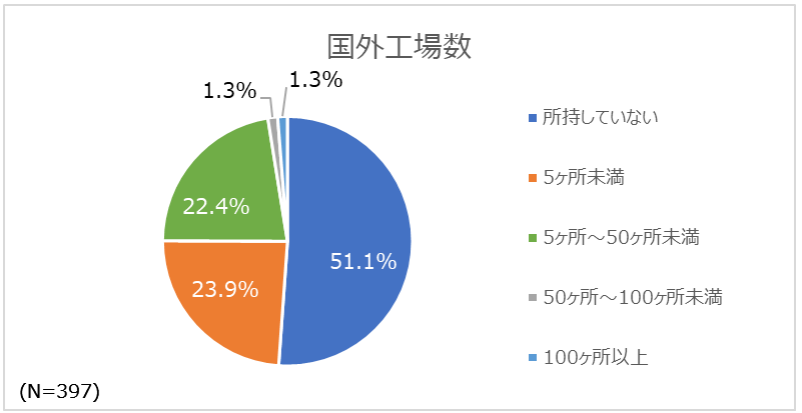
# （参考）企業回答者の属性情報（2/2）

- 総従業員数が300名未満と回答した企業は38.6%であった。
  ※中小企業基本法では、「製造業、建設業、運輸業、その他の業種」における中小企業の範囲としては、常時使用する従業員の数が300人以下、と定義されている。
- 取り扱っている製品種類数は、100種未満が37.4%であった。
- 国内工場数について、「5ヶ所未満」が66.5%と最も多かった。
- 国外工場数について、「所持していない」が51.1%と最も多かった。



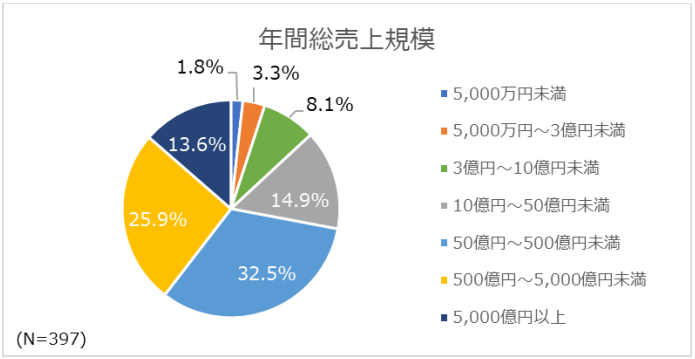



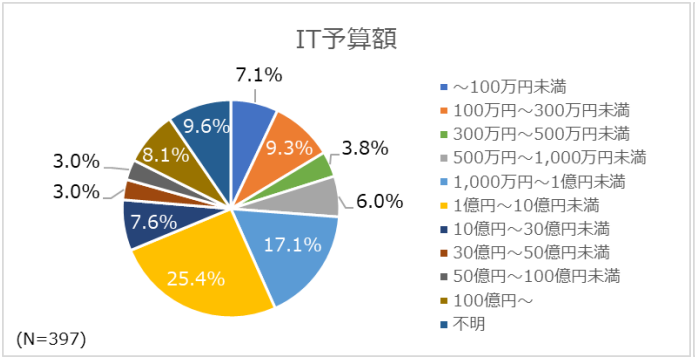



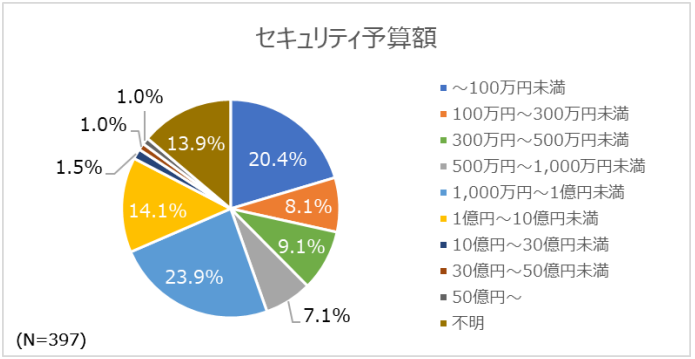
個社向け

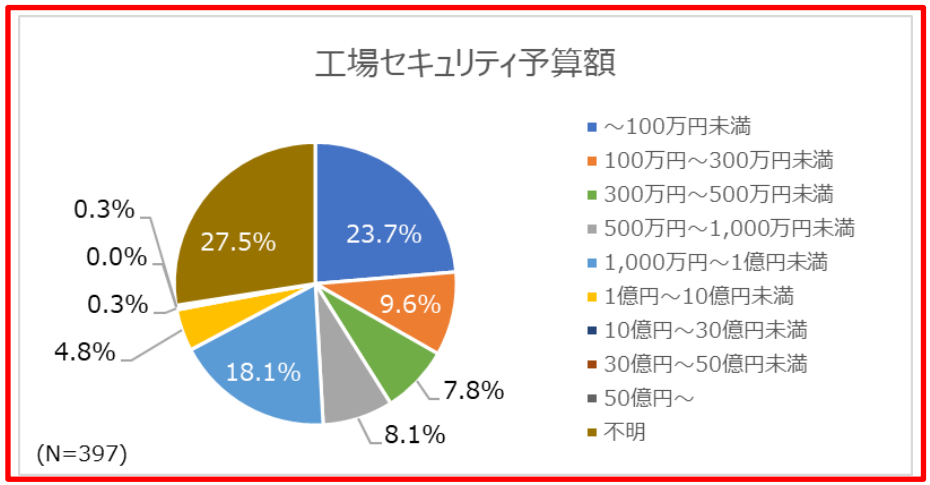
# 売上規模及び各予算額

- 年間総売上規模が10億円未満と回答した企業は13.2%であった。
- IT予算額は、「1億円～10億円未満」が25.4%と最も多かった。
- セキュリティ予算額は、「1,000万円～１億円未満」が23.9%と最も多く、次いで100万円未満が20.4%であった。
- 工場のセキュリティ予算額は、100万円未満が23.7%と最も多かった。また、不明が27.5%であった。



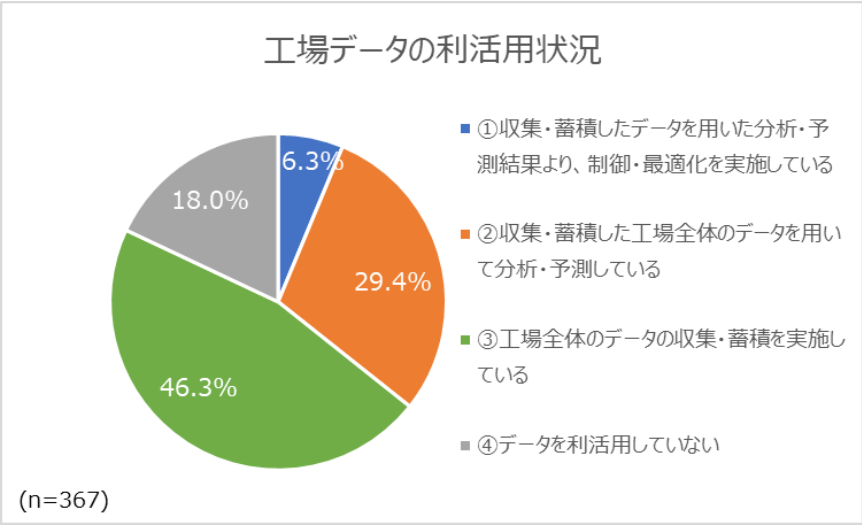



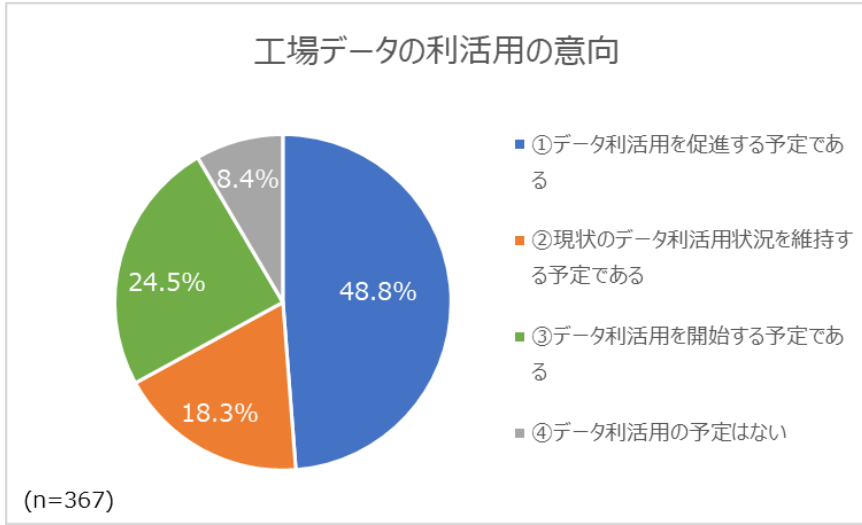

- 工場セキュリティ予算額が「～100万円未満」の企業のうち、**47.9%**の企業が、「工場システムのサイバーセキュリティ予算額が少ない」ことを工場セキュリティの課題に挙げていた。
- これらの企業が具体的にどのような課題認識を持っているかの設問は、本アンケートに含まれていない。
- 「不明」と回答した理由の可能性としては、工場におけるセキュリティ予算額が切り出されていない、本社側で工場側の予算を把握していない、アンケート調査の回答者が企業のITを中心に担当する者であったため把握できていない、等が推察される。

個社向け

# 工場におけるデータ分析

- 工場データの利活用状況について、「工場全体のデータの収集・蓄積を実施している」と答えた企業46.3%と最も多かった。 一方で、「データを利活用していない」と答えた企業は18.0%であった。
- 工場データの利活用の意向について、「データ利活用を促進する予定である」が48.8%と最も多かった。



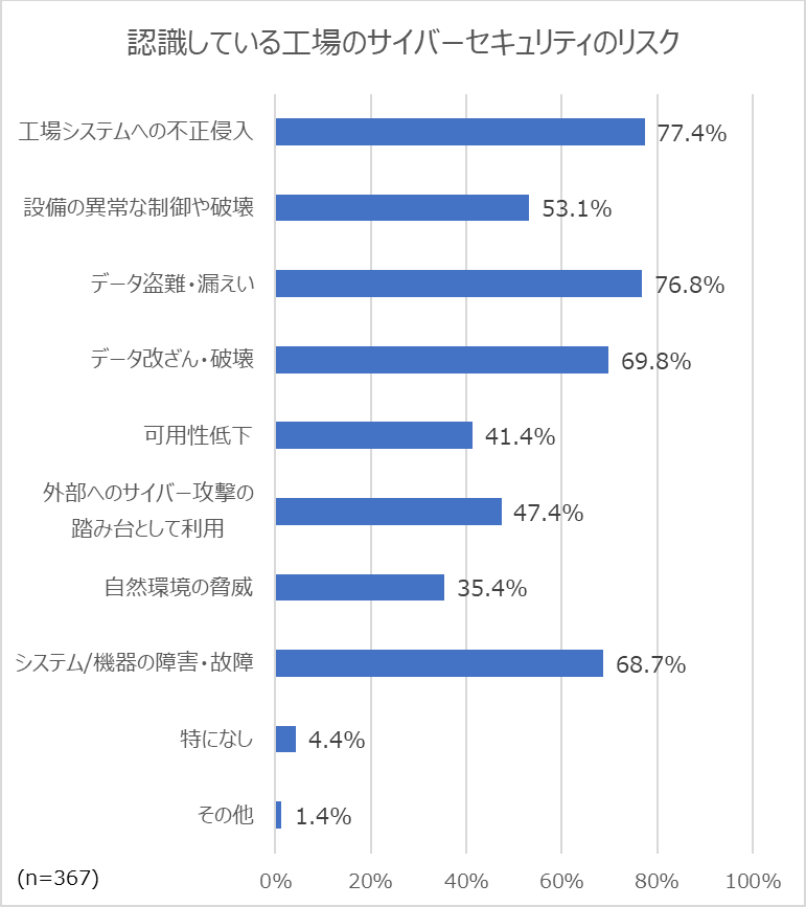

- 各選択肢の例は以下のように示している。
  ① 工場全体のデータを連携できるようデータベース等に保存している
  ② 蓄積しているデータを分析・予測し、生産計画変更や故障予測などに利用している
  ③ 分析・予測結果を基に、工場の各機器をリアルタイムに自動操作などしている
- 回答企業が具体的にどのようなことを実施しているか等を把握する設問は、本アンケートに含まれていない。

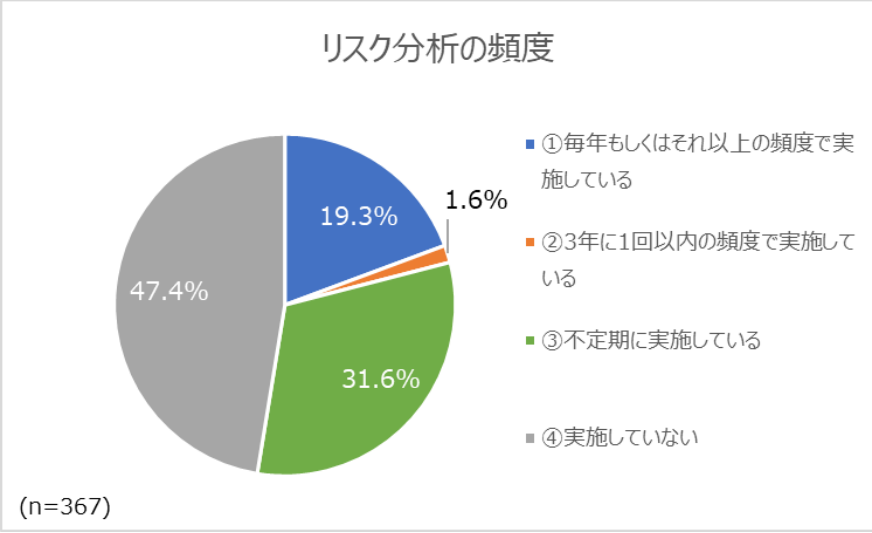
- 回答企業が具体的にどのようなデータ利活用を想定しているか等を把握する設問は、本アンケートに含まれていない。

個社向け

# 工場におけるリスク分析

- 認識している工場のサイバーセキュリティのリスクについて、「工場システムへの不正侵入」が77.4%と最も多く、「データ盗難・漏えい」（76.8%）、「データ改ざん・破壊」（69.8%）「システム/機器の障害・故障」（68.7%）と続いた。
- リスク分析の頻度について、「実施していない」が47.4%と最も多かった。



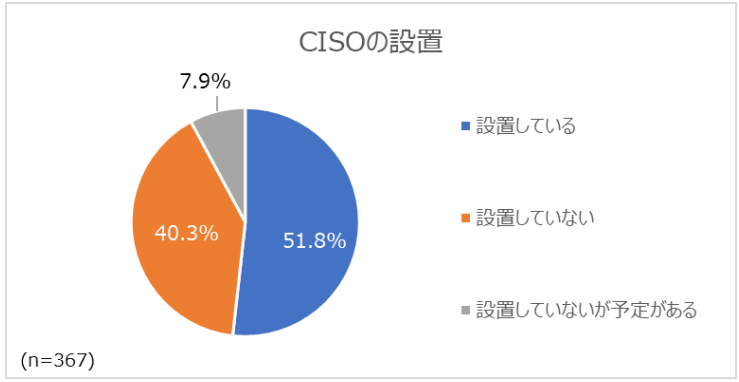



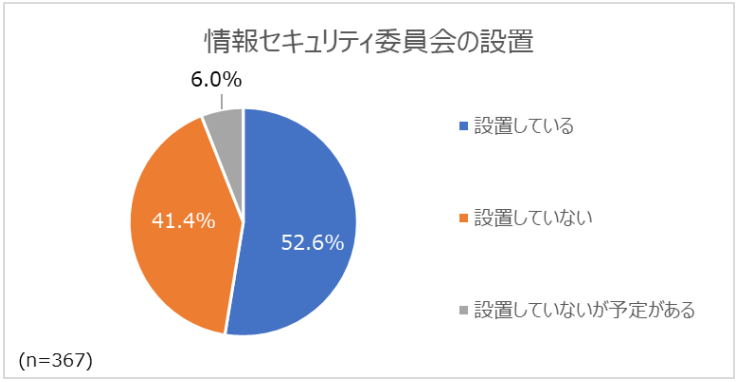

- リスク分析の例として、「リスクが顕在化した場合の事業被害に関する分析」を示している。
- リスク分析の参考資料としてIPAの「制御システムのセキュリティリスク分析ガイド 第2版 ～セキュリティ対策におけるリスクアセスメントの実施と活用～」を示している。
- 回答企業が具体的にどのようなリスク分析を実施しているか等を把握する設問は、本アンケートに含まれていない。

個社向け

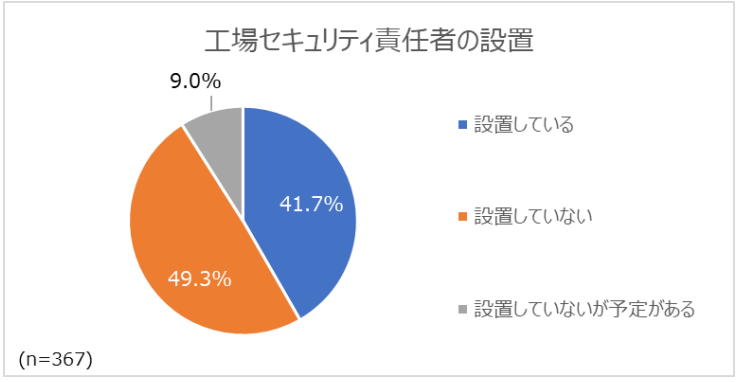
# 工場におけるセキュリティ体制

- CISOの設置について、「設置している」が51.8%と半数程度だが、工場セキュリティ責任者の設置については、「設置している」が41.7%とCISO設置率より低かった。
- 情報セキュリティ委員会の設置について、「設置している」が52.6%と半数程度であった。




- 回答企業が、情報セキュリティ委員会で具体的にどのような議論を実施しているかや、どのような頻度で議論しているか等を把握する設問は、本アンケートに含まれていない。

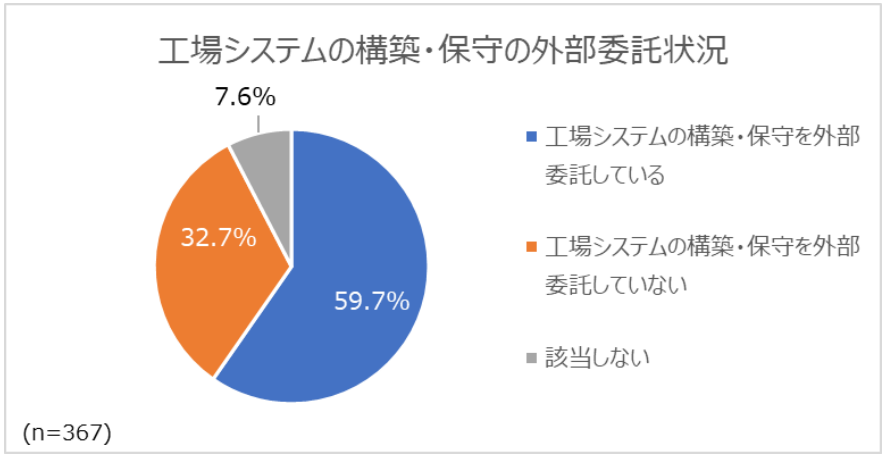



- 回答企業が、工場セキュリティ責任者に具体的にどのような役割を求めているか等を把握する設問は、本アンケートに含まれていない。

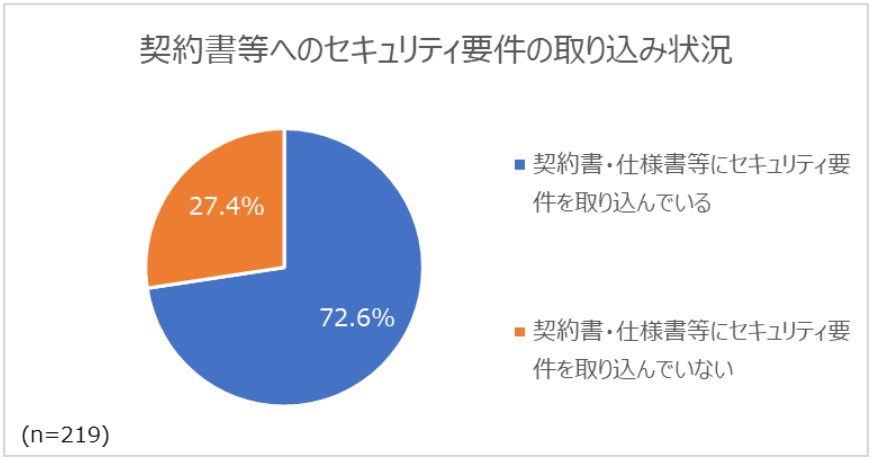
個社向け

# 工場における外部委託状況

- 工場システムの構築・保守の外部委託状況について、「工場システムの構築・保守を外部委託している」が59.7%と約6割は外部委託があった。
- 外部委託のある企業における契約書等へのセキュリティ要件の取り込み状況について、「契約書・仕様書等にセキュリティ要件を取り込んでいる」が72.6%であり、7割以上でセキュリティが考慮されていた。




- 外部委託の定義は示していないため、例えば、企業グループ内の外部委託等の場合、「外部委託していない」と回答している可能性がある。

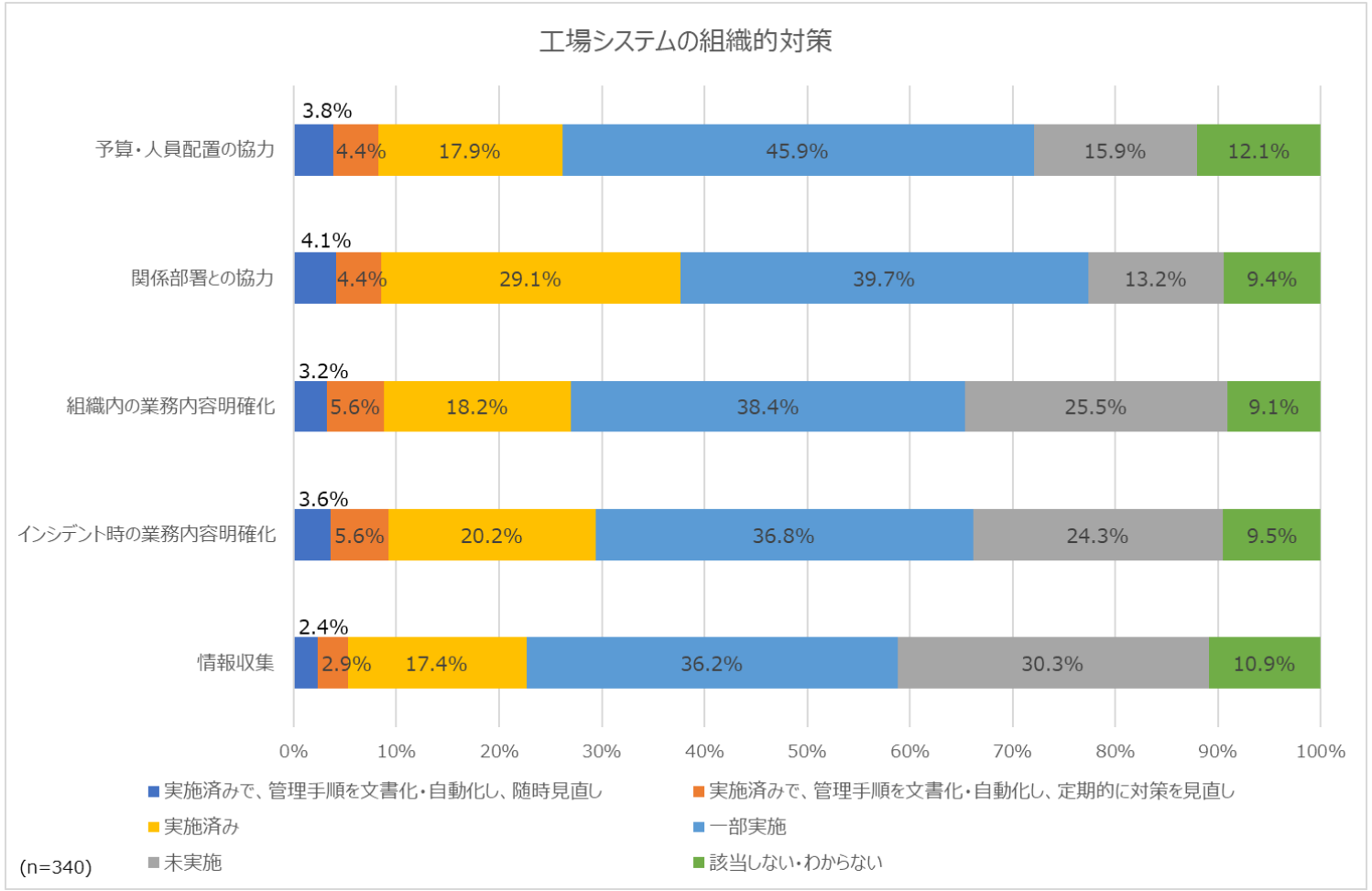



- 具体的にどのような事項を契約書等へ記載したか等を把握する設問は、本アンケートに含まれていない。

個社向け

# 工場ガイドチェックリストの実施状況（1.工場システムの組織的対策）

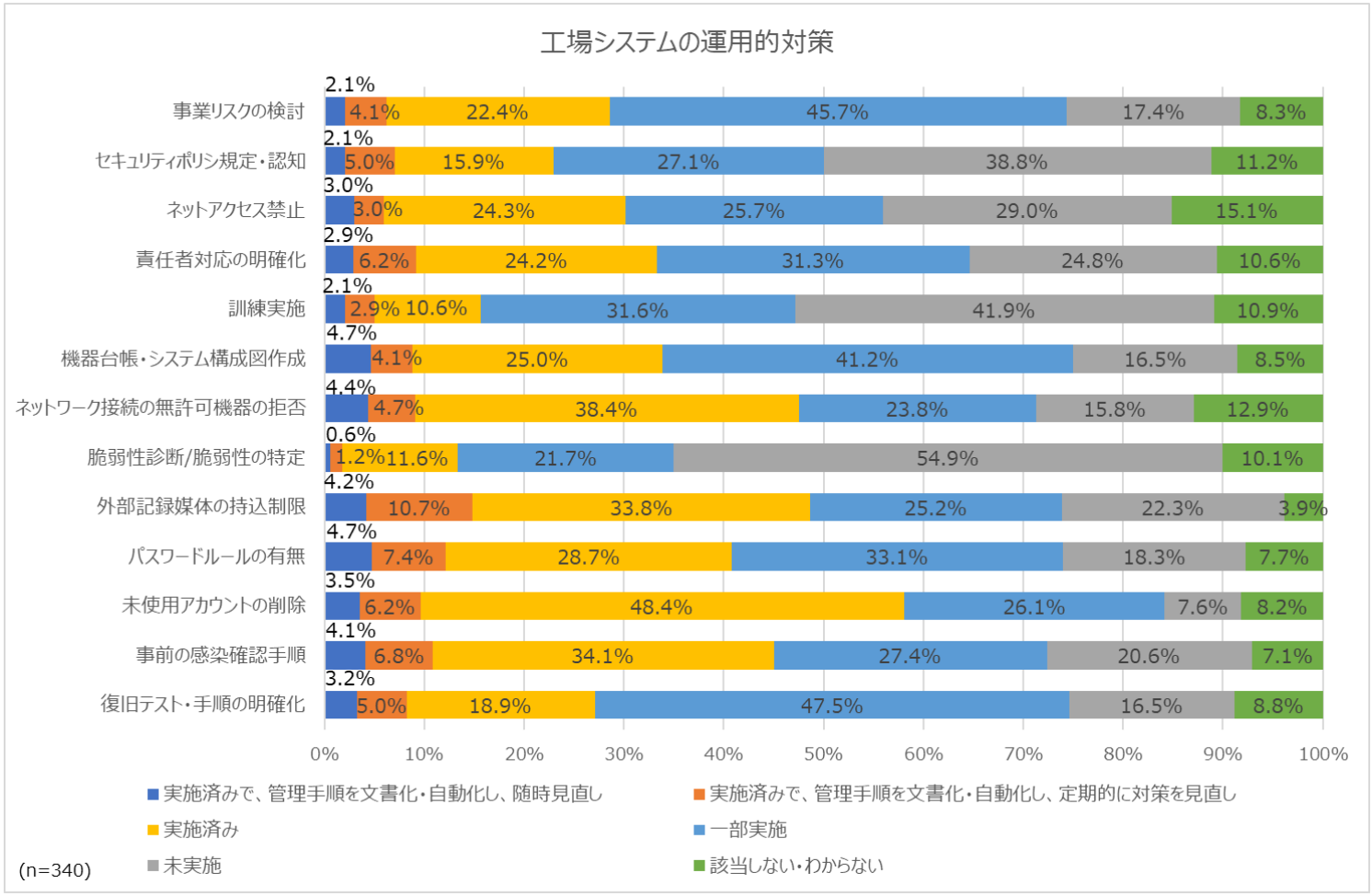
- 工場システムの組織的対策のうち、「情報収集」について「未実施」または「該当しない・わからない」が41.0%と他の対策と比較して、最も多かった。



個社向け

# 工場ガイドチェックリストの実施状況（2.工場システムの運用的対策）

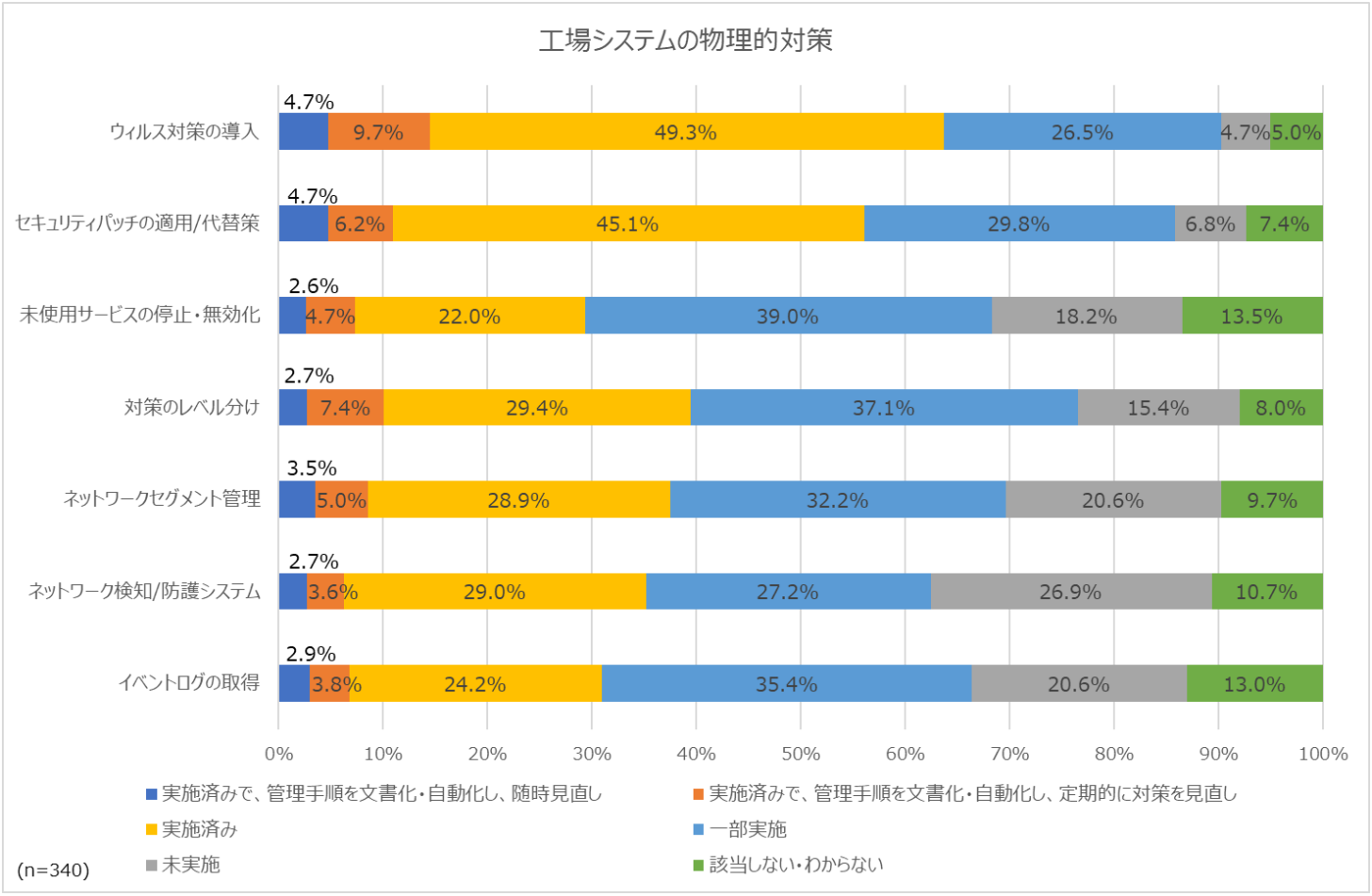
- 工場システムの運用的対策のうち、「脆弱性判断・脆弱性の特定」について「未実施」または「該当しない・わからない」が65.0%と他の対策と比較して、最も多かった。



個社向け

# 工場ガイドチェックリストの実施状況（3.工場システムの物理的対策）

- 工場システムの物理的対策のうち、「ウイルス対策の導入」「セキュリティパッチの適用/代替策」について実施済み※であるのがそれぞれ63.7%、55.3%と他の対策と比較して多かった。

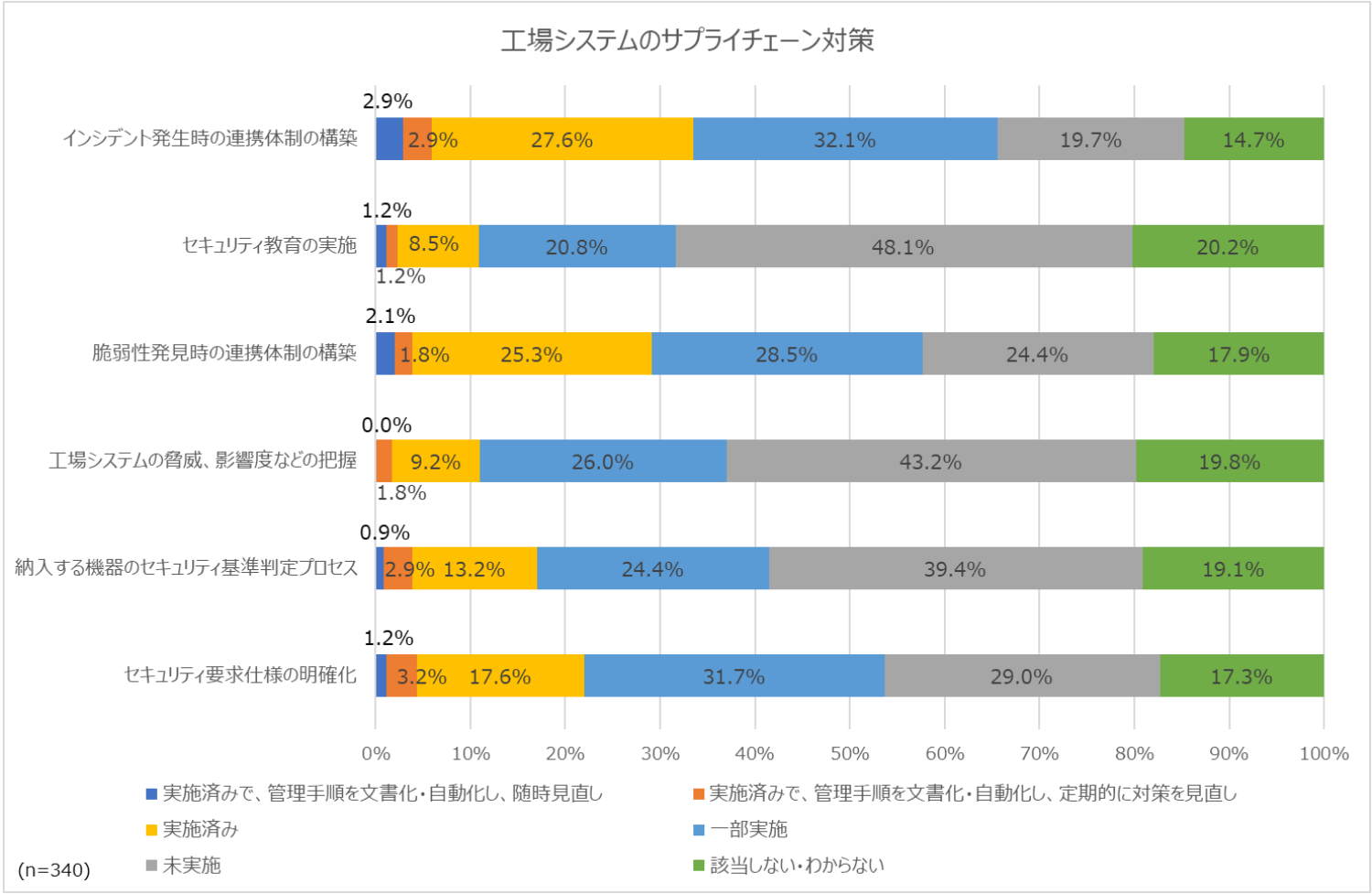



※「実施済みで、管理手順を文書化・自動化し、随時見直し」「実施済で、管理手順を文書化・自動化し、定期的に対策を見直し」「実施済み」の合計

個社向け

# 工場ガイドチェックリストの実施状況（4.工場システムのサプライチェーン対策）

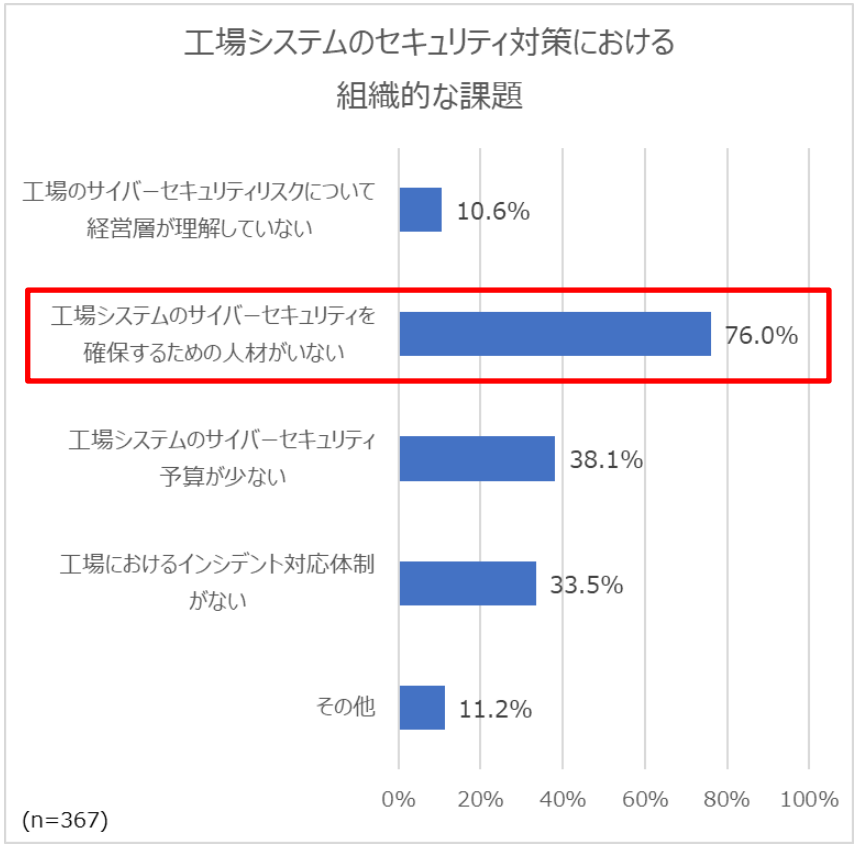
- 工場システムのサプライチェーン対策のうち、「セキュリティ教育の実施」について「未実施」または「該当しない・わからない」が68.3%と他の対策と比較して、最も多かった。

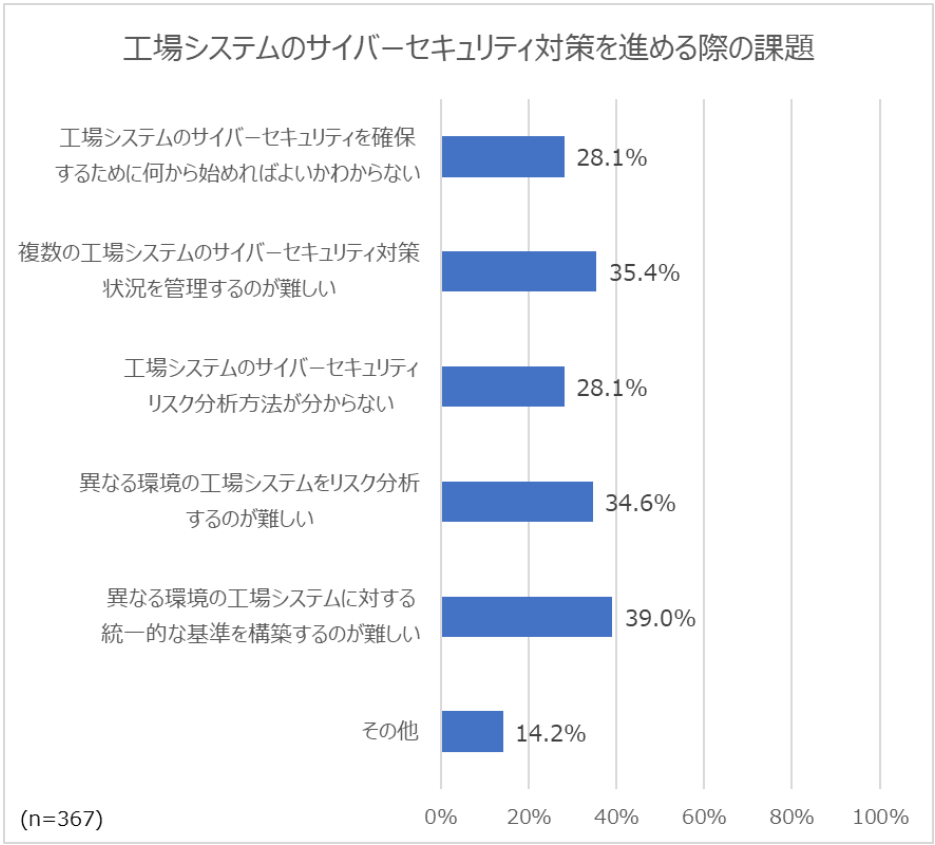


個社向け

# 工場セキュリティにおける課題や要望について（1/3）

- 工場システムのセキュリティ対策における組織的な課題について、「工場システムのサイバーセキュリティを確保するための人材がいない」が76.0%と最も多かった。
- 工場システムのサイバーセキュリティ対策を進める際の課題について、統一的な基準構築やリスク分析、対策状況の管理の難しさ等、いずれの項目についても3～4割の企業が課題としていた。

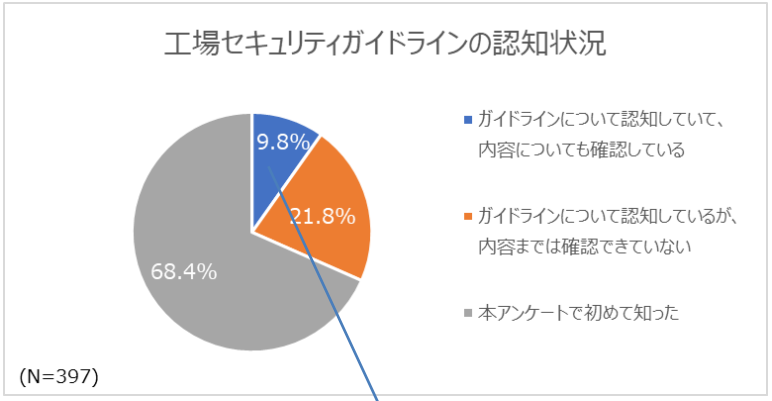


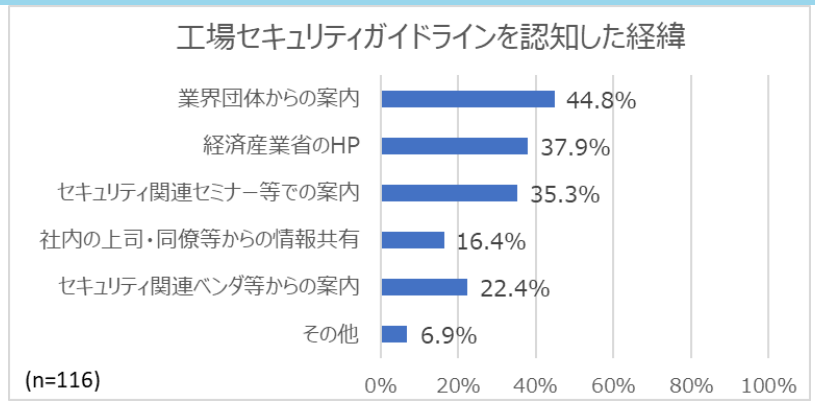



個社向け

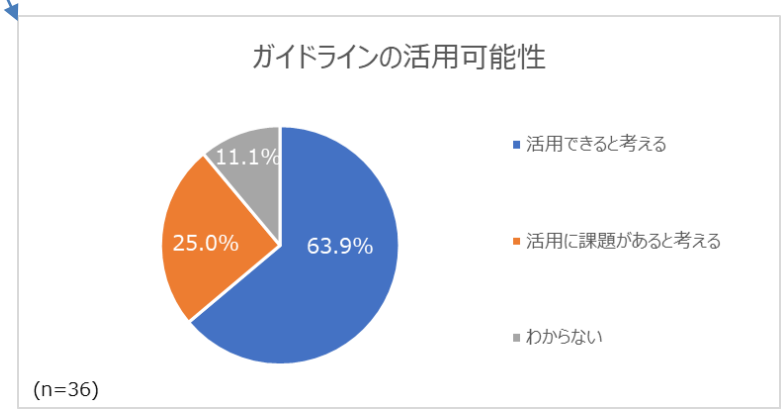
# 工場セキュリティにおける課題や要望について（2/3）

- 工場セキュリティガイドラインの認知状況について、「本アンケートで初めて知った」が68.4%と最も多く、「ガイドラインについて認知していて、内容についても確認している」のは9.8%であった。
- 工場セキュリティガイドラインを認知した経緯について、「業界団体からの案内」が44.8%と最も多く、「経済産業省のHP」（37.9%）、「セキュリティ関連セミナー等での案内」（35.3%）が続いた。
- ガイドラインの活用可能性について、「活用できると考える」が63.9%と最も多かった。



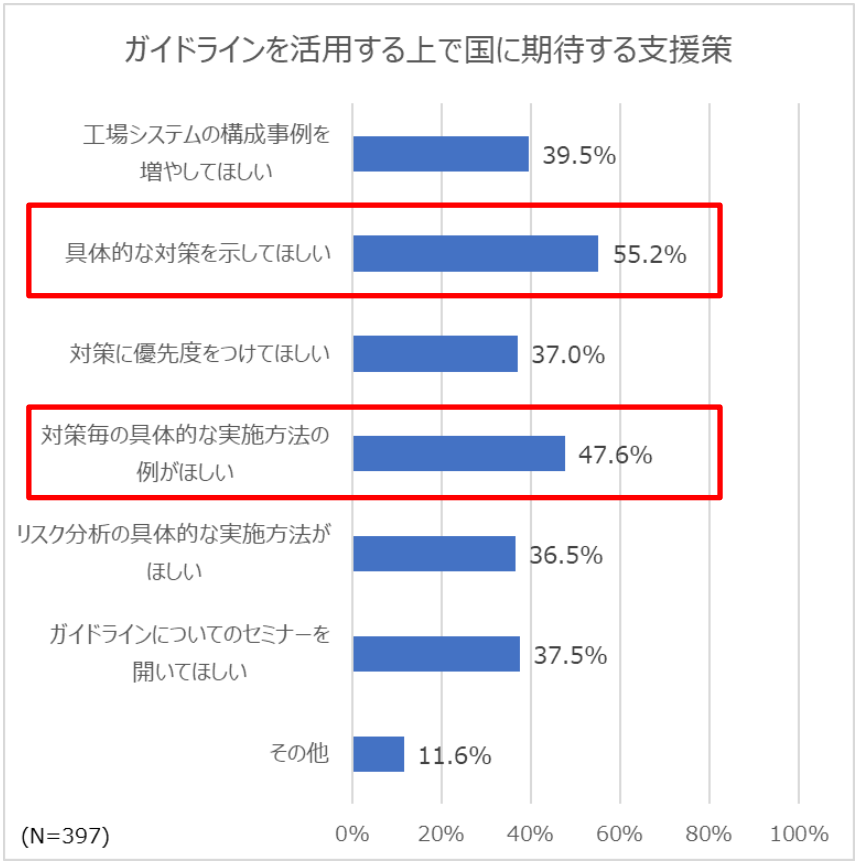

※ 「工場セキュリティガイドラインの認知状況」の設問において、「ガイドラインについて認知していて、内容についても確認している」との回答者が対象

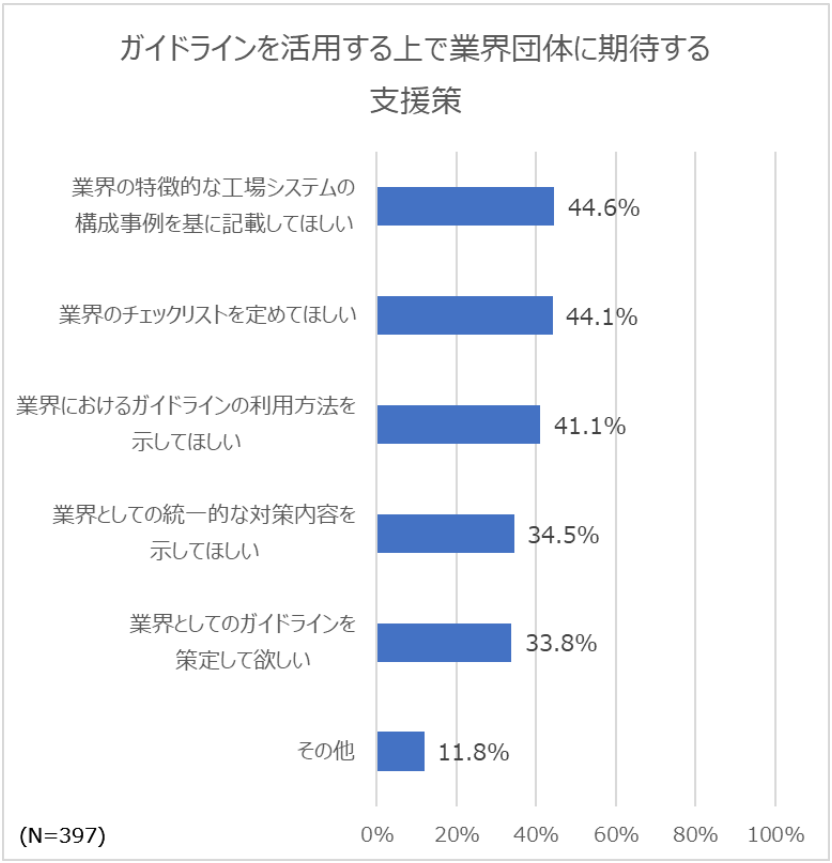


個社向け

# 工場セキュリティにおける課題や要望について（3/3）

- ガイドラインを活用する上で国に期待する支援策について、「具体的な対策を示してほしい」が55.2%と最も多く、「対策毎の具体的な実施方法の例がほしい」が47.6%と続いた。
- 業界団体に期待する支援策について、業界における構成事例やチェックリスト、ガイドラインの利用方法、統一的な対策内容等、いずれの支援策についても3～4割強の企業が期待していた。



# 目次

# 取組の方向性

## 工場セキュリティガイドラインの普及啓発に関する論点（第４回SWG提示）

- 特に本ガイドラインを普及させるべき業界はどこか。
- いかなる者を巻き込めば、効果的な本ガイドラインの普及啓発がなされると考えられるか。
  （例：業界団体、コンサル、セキュリティベンダ　等）
- その他、本ガイドライン普及に寄与する取組はあるか。
  （例：ガイドライン実践のためのセミナー・研修、SC3との協力等のコミュニティ形成論）

## 調査結果を踏まえた取組の方向性

- 工場ガイドの認知率・普及率は業界・企業共に低かったことから、まずは普及の底上げを図ることが必要であることを確認。
  - ✓ SC３の活動と連携し工場ガイドを業界団体に対して周知
  - ✓ セキュリティベンダやIPAなど各者が実施するセミナー等を活用した周知
  - ✓ 関係省庁（デジ庁デジタル臨調等）や業所管部局との連携、継続的なフォローアップ

- 工場セキュリティにおける企業の課題としては人材不足が最も多かった。また、企業は工場現場のデータの利活用を行う意向がある割に、リスク分析はできていない。さらに、国に対しては、工場ガイドの具体的な対策や事例を示してほしいという声が多い。
  - ✓ 情報処理安全確保支援士等の更なる活用といった支援層の拡大
  - ✓ 関係機関（IPA等）とも連携した工場ガイドの深掘り・具体化した文書（詳細ガイド、実施例）の作成・ブラッシュアップ
  - ✓ 業界団体、セキュリティベンダ等によるサポート

# 目次

# 工場セキュリティガイドラインの普及啓発について

第４回工場SWG資料

- 様々な組織において工場システムにおけるセキュリティ推進のための取組が行われている。また、工場システムのセキュリティ関連サービスも続々と国内展開されており、一部については工場セキュリティガイドラインの活用・参照がなされている。
- 今後、アンケート調査により把握する業界・企業等の課題や要望も踏まえ、必要な業界や個社に対して、工場セキュリティガイドラインの普及啓発を進めていく予定である。
- ガイドラインの普及啓発や今後の取組について、以下のような論点を元に御意見をいただきたい。

## 工場セキュリティガイドラインの普及啓発に関する論点

- 特に本ガイドラインを普及させるべき業界はどこか。
- いかなる者を巻き込めば、効果的な本ガイドラインの普及啓発がなされると考えられるか。
  （例：業界団体、コンサル、セキュリティベンダ　等）
- その他、本ガイドライン普及に寄与する取組はあるか。
  （例：ガイドライン実践のためのセミナー・研修、SC3との協力等のコミュニティ形成論）
- 例えば、スマートファクトリに特化したガイドライン等、本ガイドラインのほか、取り組んでいくべき課題はあるか。
- その他

# スマートファクトリーにおけるセキュリティ検討の必要性

- 現行の「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」については、各業界・業種が自ら工場のセキュリティ対策を立案・実行することで、産業界全体、とりわけ工場システムのセキュリティの底上げを図ることを目的として作成。

・現行のFAシステムを例に、制御システムに対するセキュリティ施策を検討するプロセスおよび勘所を提示

・既存の制御システムを前提に、境界防御型のセキュリティを想定。

**ステップ 1**

**内外要件（経営層の取組や法令等）や業務、保護対象等の整理**

- **ステップ1-1**
- **ステップ1-2** 業務の整理
- **ステップ1-3** 業務の重要度の設定
- **ステップ1-4** 保護対象の整理
- **ステップ1-5** 保護対象の重要度の設定
- **ステップ1-6** ゾーンの整理とゾーンと業務、保護対象の結びつけ
- **ステップ1-7** ゾーンと、セキュリティ脅威の影響の整理

**ステップ 2**

**セキュリティ対策の立案**

- **ステップ2-1** セキュリティ対策方針の策定
- **ステップ2-2**
  想定脅威に対するセキュリティ対策の対応づけ
  (1)システム構成面での対策
  (2)物理面での対策

**ステップ 3**

**セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）**

- **ライフサイクルでの対策**
  **サプライチェーンを考慮した対策**
  (1)ライフサイクルでの対策
  (2) サプライチェーン対策

**事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す**

**・スマートファクトリーに向けた制御システムにおけるシステムアーキテクチャの変化**

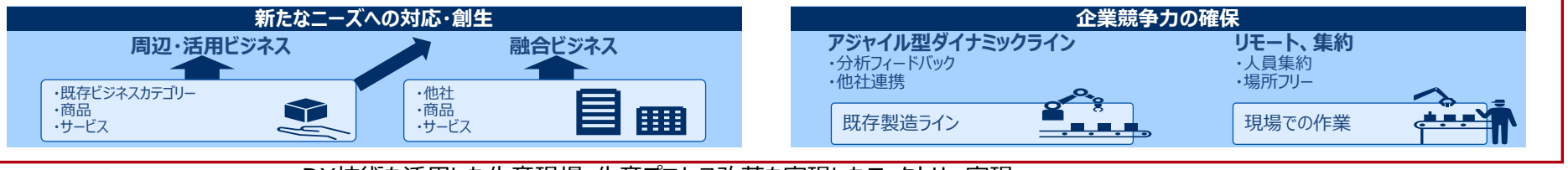
**・サプライチェーンによる脅威の増加**

**工場がクラウドやデジタルツインといったサイバー空間に密接に繋がっていく世界における**
**セキュリティのあり方を検討することが必要。**

# スマートファクトリーの目的

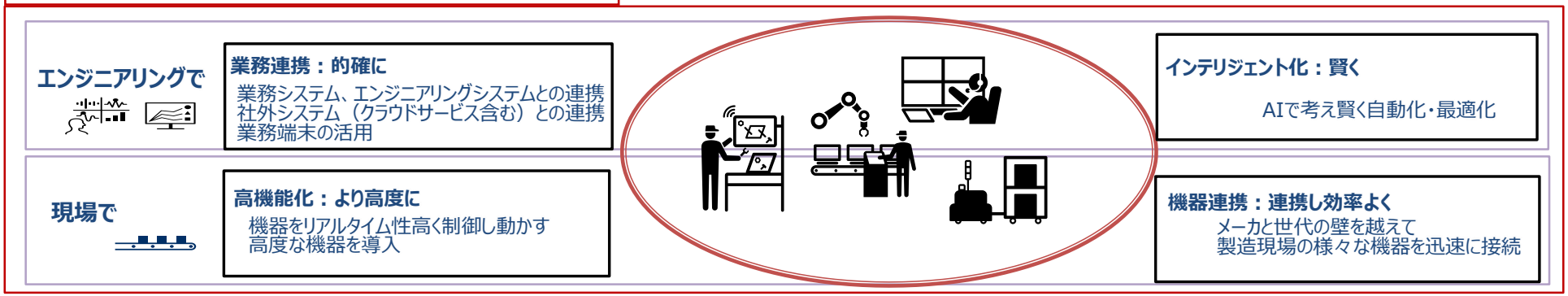
- スマートファクトリーは、新たなニーズへ対応した商品やサービスの迅速な提供を実現できるなど、 製造業のビジネス競争力を強化する源泉。
- 工場のスマート化を達成していくためには、汎用品の活用、クラウドとの連携やデジタルツインといったサイバー空間との密接な繋がりが進んでいくと想定される。

**DXによるビジネス競争力の強化**



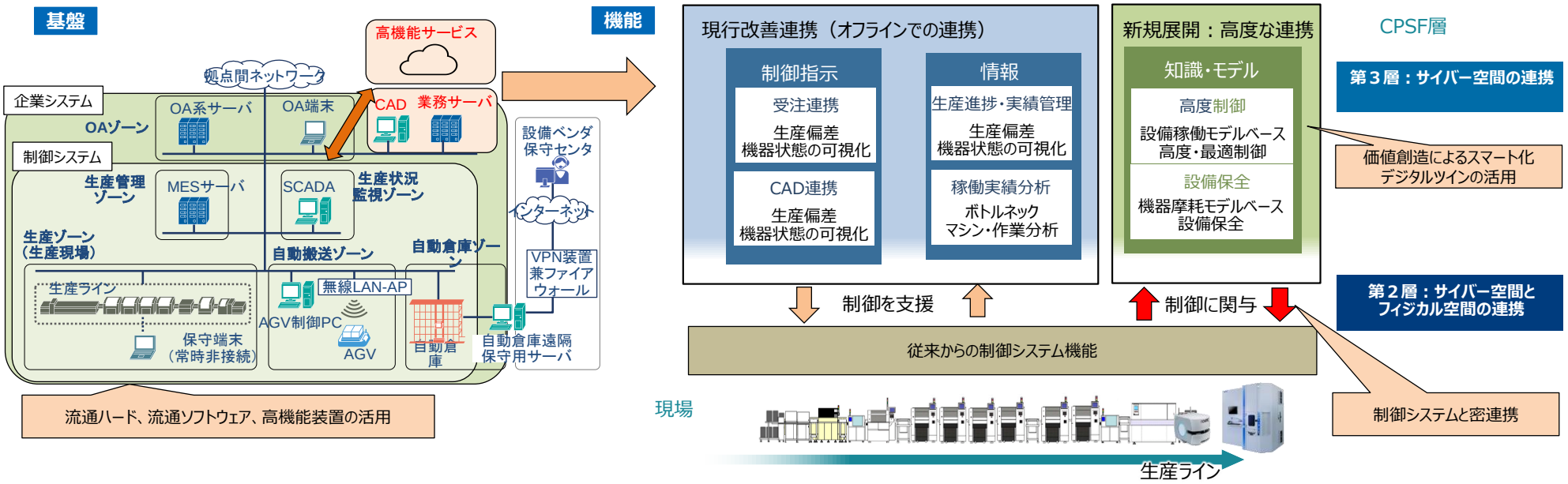

DX技術を活用した生産現場・生産プロセス改革を実現したファクトリー実現

広くつながり＋スマートなファクトリーの実現




| | 分類 | システムへの要求 | システムの変化 |
|---|---|---|---|
| 現場で | 基盤 | 市場、ビジネス変化による製品やサービスのライフサイクル短期化と同期した、生産ラインや制御システムの短期間での構築 | 流通ハードウェア、流通ソフトウェア（市販パッケージ、OSS）、高機能装置の活用 |
| エンジニアリングで | 機能（現行改善） | 高効率を目指し、社内外のデータ、機能の活用（受注、CAD、データ解析、リモート保守など） | クラウドサービスを含む社内外の業務関連システムと連携（受注、CAD、データ解析、リモート保守など） |
| | 機能（新規展開） | より高度な制御やサービスを目指し、Society5.0（CPSF）での新たな業務機能構築 | サイバー空間レベルでの価値創造によるスマート化（高機能、品質） |

# （参考）スマートファクトリーにおける連携イメージ



# 工場のスマート化に伴うリスクを管理していくための考え方の仮説

- 工場のスマート化を進めていくためには、付随するリスクを管理するための考え方や対応のあり方を検討する必要性が生じていると考えられる。
- 具体的には、汎用品活用への対応、外部連携対応、新たな制御モデルへの対応について検討が必要であるとともに、スマートファクトリーに対応できる人材のあり方について、検討を進めていくことが必要と考えられる。
- また、汎用品の活用や連携の増加に伴い、サプライチェーンで考慮しなければいけない事項も変化・増加し得ることから、スマートファクトリー特有のサプライチェーン対応についても、検討を進めていくことが必要と考えられる。
- 加えて、戦略的イノベーション創造プログラム（SIP）においてもスマート工場のセキュリティに資する技術開発がなされていることから、こうした技術との連携も模索していくことが効果的と考えられる。

| 分類 | 従来のセキュリティ施策の考え方 | スマートシステム化に伴うセキュリティ施策へのインパクト |
|---|---|---|
| 基盤 | ・ホワイトボックスの考え方で構築<br>・制御システムをシェル化<br>（シェルの核ほどホワイトボックス）し、シェルの境界でシステム、運用にてセキュリティ施策を実施。 | 流通品の活用によりシェル内の各所でブラックボックスの汎用品を活用するため、既存の考え方（シェルの界面でガード）でのセキュリティ施策が有効でなくなる。<br>→・シェル内のブラックボックスの汎用品からインシデントが発生 |
| 機能（現行改善） | ・制御システム機能と連携システムの機能と直接の連携はない（停止しても制御への直接影響しない）<br>・連携するデータは独自形式<br>・制御システム機能のセキュリティは各機能が独自に実施。 | 制御機能の一部として社内外システムの機能を利用<br>社外システムとのデータ交換も中心に標準データ形式を利用<br>→・外部システムでのセキュリティインシデントによる不正データが制御に影響<br>・標準的なプロトコルを利用するマルウェアの影響を受けるためインシデント発生可能性が拡大 |
| 機能（新規展開） | ・確立された制御ロジックをベースに制御システムの機能を実現。このためロジックが正しく実装されているかを検証する構築段階での施策によりセキュリティを実現。 | サイバー空間にフィジカルの世界をモデル化し高度な制御システムの機能を実現するという新たな制御モデルの誕生。<br>→新しい考え方のためセキュリティリスク分析およびセキュリティ施策が不明<br>・誤ったモデル実装によるインシデント発生<br>・モデルの誤った利用によるインシデント発生モデルの改ざんを含む） |

**システム/運用/マネージメント**

**汎用品活用（ゼロトラスト範囲拡大）への対応**
- ハードウェア　・ソフトウェア
- 機能　・サービス

**外部連携対応**
- 標準データ活用時のセキュリティ施策
- 不正データに対応するセキュリティ施策（CPSF2層の対応）

**新たな制御モデルへの対応**
- 装置、機能動作モデル化時のセキュリティ施策
- モデル利用時におけるセキュリティ施策（CPSF3層の対応）

**人材**

**スマートファクトリー対応スキル向上**
- 変化に対応できる知識
- 多様なインシデントの経験

**サプライチェーン**

**外部連携に係る契約先との留意事項**

**OSS等の開発プロセスでの留意事項**

**クラウド等の調達・契約の留意事項**

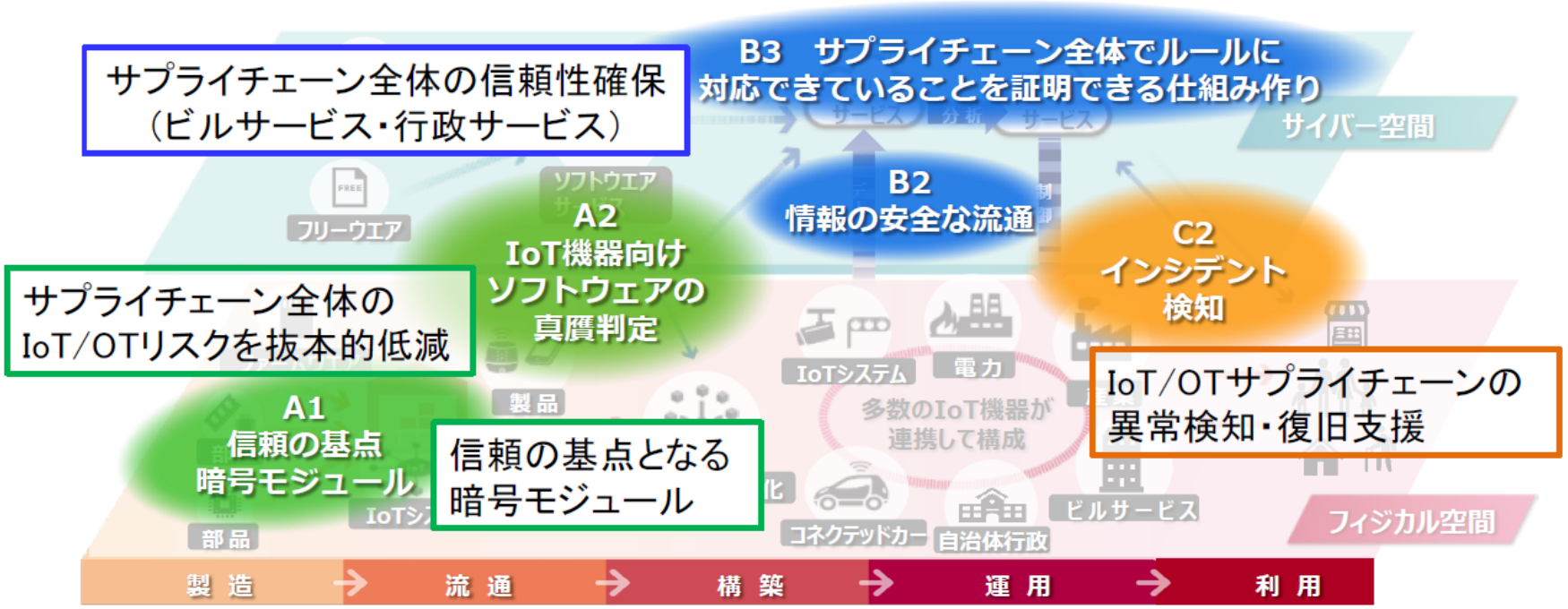
**スマートファクトリーガイドを通じ、先進的な事業者が臆することなく工場のスマート化を進め、「稼げる工場化」を促進することを後押ししていく。**

# （参考）SIP（2017年度～2022年度）におけるサイバー・フィジカル・セキュリティの研究開発事項

## 『サイバー・フィジカル・セキュリティ対策基盤』構築に向けた研究開発項目

IoT機器やサプライチェーンの各構成要素について，セキュリティの確保（**信頼の創出**）とその確認（**信頼の証明**）を繰り返し行い，**信頼のチェーンを構築・維持**することで，IoTシステム・サービス及びサプライチェーン全体の**セキュリティ**を確保

サイバー空間とフィジカル空間の双方に跨るIoT社会でのサプライチェーン



# 検討の進め方のイメージ

- 令和５年度中に、工場SWGの委員のうち、関心の高い委員を中心に、更なる課題の深堀や具体的な対策の検討を進め、適宜工場SWGに付議・報告する形で進めていくことを想定。
- まずは、スマート化を進める業界・企業におけるニーズを調査し、P33で記述したような仮説の検証を行うことで、いかなる成果物の形がよいかの精査や、必要な対策のブラッシュアップを行っていく。

**工場ガイドラインのパブコメにおいては、インターネット接続やクラウド利用、サプライチェーンにおけるセキュリティ確保に関する御意見が複数者から挙げられたことからも関心は一定数存在するものと認識。**

パブコメでの主な御意見

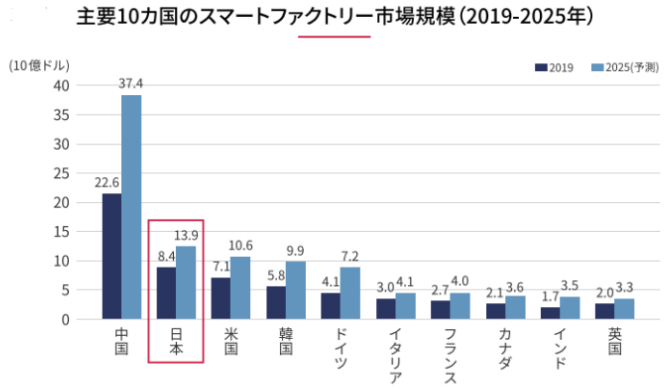
インターネット接続やクラウド利用、工場間の接続に関する御意見

- 制御ゾーンや生産管理ゾーンから**直接インターネットへ接続する経路**を記載してはどうか。【セキュリティ会社】
- 制御ゾーンの機器をリモートでメンテナンスしたり、生産性分析業務を外部クラウドで行うことも増えている。**外部ネットワークとの接続も想定**すべきではないか。【印刷】
- 想定工場のシステムで**クラウドに関する指針**を示してほしい。【個人】
- 自動倉庫の遠隔保守以外は拠点内に閉じているため、**インターネット接続やクラウド技術の使用も想定に加える必要**はないか。【工作機器】
- **拠点間の脅威や被害拡大・対策の意識を強め**てもよい。【製造】

サプライチェーンに関する御意見

- Society5.0では、柔軟で動的なサプライチェーンの構成が可能だが、**サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という新たなリスクへの対応が必要**となっている。【セキュリティ会社】
- 工場DXの推進により、**ソフトウェアやクラウドが導入されていく製造環境、サプライラーと連携した製造環境に必要なセキュリティ対策の必要性を追加**することが望ましい。【セキュリティ会社】

**国内のスマートファクトリー市場は主要10カ国で見ても大きく、様々な分野の製造業においてスマート化やDX化の事例も見られる。**




出所）「INVEST JAPAN 製造業」（JETRO）において BIS Research のデータを元に作成

製造業DX取組事例

| | |
|---|---|
| 株式会社今野製作所（油圧機器） | 株式会社ダイセル（化学） |
| 沖電気工業株式会社（通信機器） | 三菱電機株式会社（総合電機） |
| 富士通株式会社（総合ITベンダー） | ヤマハ発動機株式会社（輸送用機器） |
| オークマ株式会社（工作機器） | ビジネスエンジニアリング株式会社（システムベンダー） |
| トヨタ自動車株式会社（自動車） | 川崎重工業株式会社（重工業） |
| 三和工機株式会社（工作機器） | オムロン株式会社（産業機器） |
| 株式会社アイデン（制御盤） | ダイキン工業株式会社（空調機） |
| 株式会社IHI（重工業） | |

出所）「製造業DX取組事例集」（経済産業省）

# （参考）成果物のイメージ

- 現時点での成果物のイメージとしては、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」の別冊として整備していくことを想定。
- 成果物については、スマートファクトリーを持つ主要な業界・企業に対して普及に向け積極的な働きかけを行っていくことを想定。

## 成果物のイメージ

**スマートファクトリー化**

- **ブラックボックス活用（ゼロトラスト範囲拡大）への対応**
- **外部連携データへの対応**
- **モデルベース高度制御への対応**
- **スマートファクトリー対応スキル向上**

**サプライチェーン**

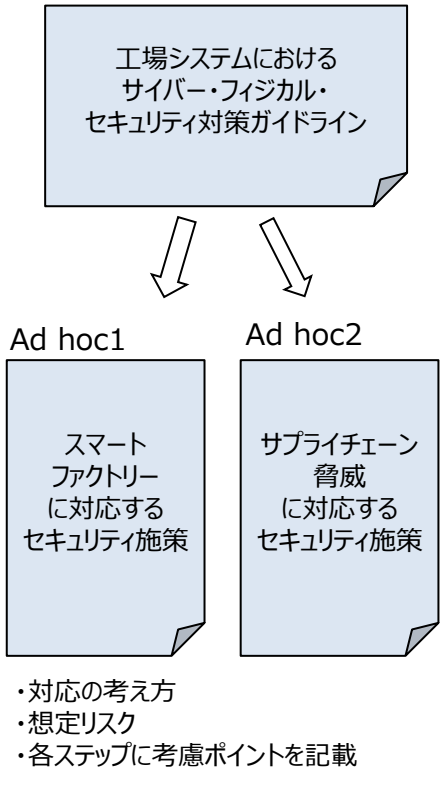
- **外部連携に係る契約先との留意事項**
- **OSS等の開発プロセスでの留意事項**
- **クラウド等の調達・契約の留意事項**

**推進方法：ガイドライン整備活動の内で推進**

目次案

Ad hoc1：スマートファクトリに対応するセキュリティ施策
- ・全体の考え方
- ・想定リスク
- ・下記のカテゴリごとに各ステップ（ステップ１～３）でのガイド
  - ・ブラックボックス活用への対応
  - ・外部連携データへの対応（CPSF2層）
  - ・モデルベース高度制御への対応（CPSF3層）
  - ＋
- ・ステップ３の横断内容として
  - スマートファクトリー対応スキル向上

Ad hoc2：サプライチェーン脅威に対応するセキュリティ施策
- ・全体の考え方
- ・想定リスク
- ・下記のカテゴリごとに各ステップ（ステップ１～３）でのガイド
  - ・システム・運用での感染・業務影響防止策
  - ・開発委託、OSS活用時の対応
  - ・SolarWinds的な事象防止
  - ＋
- ・横断的内容として
  - ・調達（部品、サービス）、契約
  - ・xBoM管理




- ・対応の考え方
- ・想定リスク
- ・各ステップに考慮ポイントを記載

# 目次

# ３．ご議論いただきたいこと

１．「工場システムのサイバーセキュリティ対策のアンケート・ヒアリング調査」概要、結果を踏まえた取組の方向性

- 「工場システムのサイバーセキュリティ対策のアンケート・ヒアリング調査」の結果について、着目すべき点。
- P27の取組の方向性について

２．工場のスマート化に向けた対応（仮説）

- スマートファクトリのためのガイドラインのニーズ
- P33に記載した仮説
- P35に記載した進め方

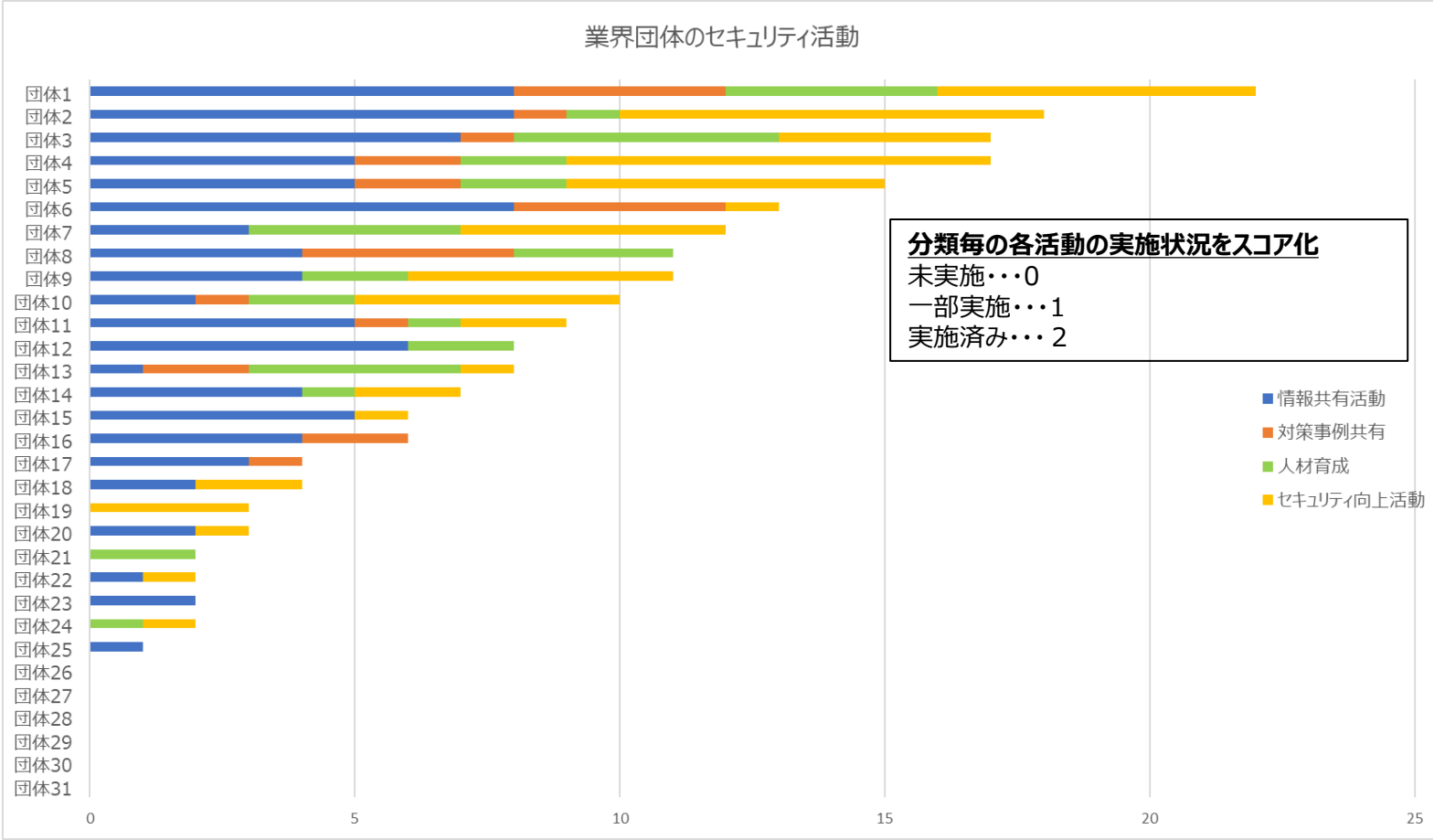
# 参考資料

## 団体及び企業のセキュリティ活動一般に関する調査結果

団体向け

# 業界団体におけるセキュリティ活動状況

- 8団体が「情報共有活動」「対策事例共有」「人材育成」「セキュリティ向上活動」の全てを実施していた。一方で、6団体がセキュリティ活動をいずれも実施していない。



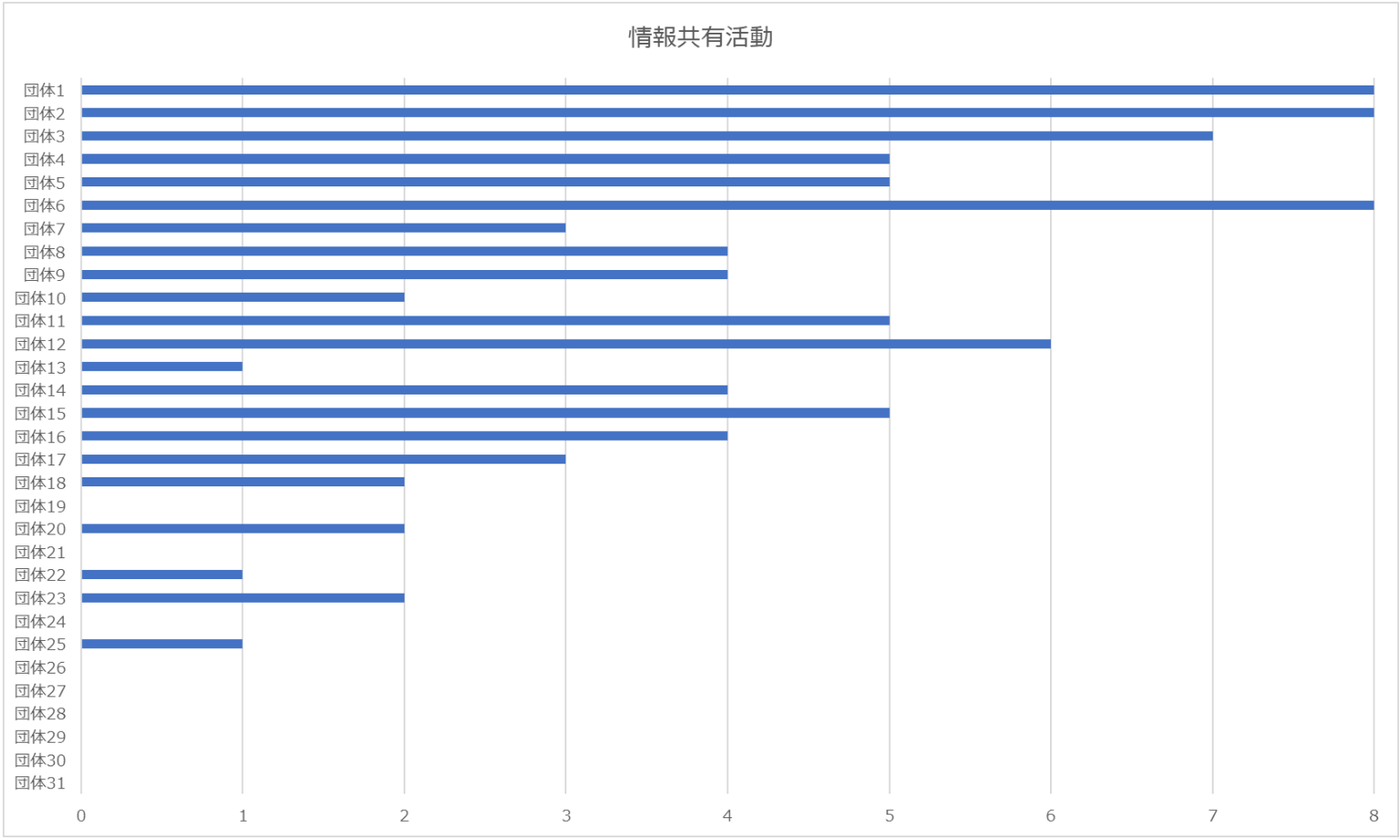
団体向け

# 業界団体におけるセキュリティ活動状況（1.情報共有活動）

- 情報共有活動については、22団体（約7割）が何らかの活動を実施していた。

情報共有活動における活動例
①国や関係機関等組織からの脅威・インシデント情報等の会員への提供
②業界団体が収集した脅威・インシデント情報等の会員への提供
③会員間の情報共有の仕組みの構築・運営
④会員のインシデントに関する情報を元にした注意喚起や関連情報の提供

各活動例の実施状況を加算し、スコア化
未実施・・・0
一部実施・・・1
実施済み・・・2



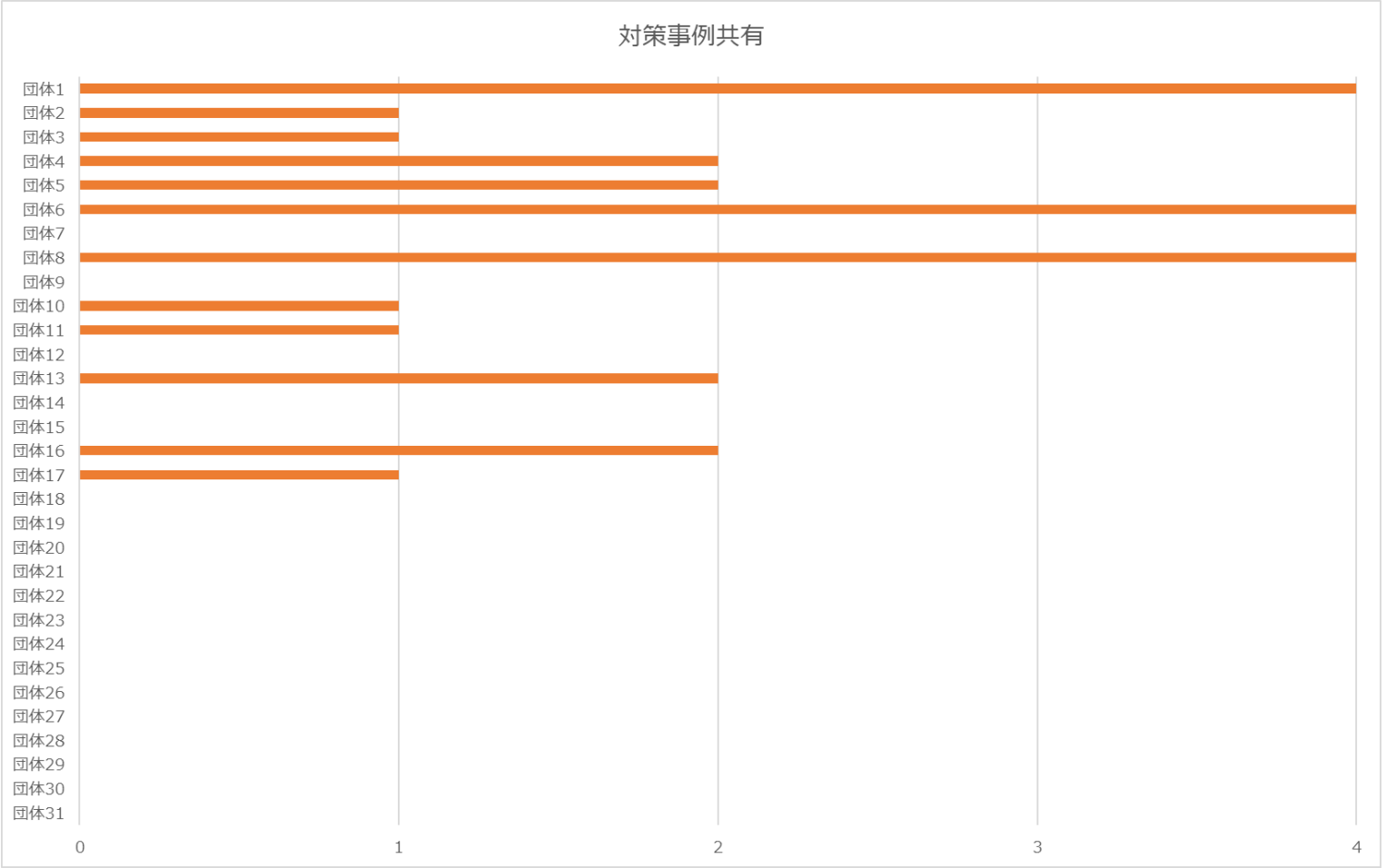
団体向け

# 業界団体におけるセキュリティ活動状況（2. 対策事例共有）

- 対策事例共有については、12団体（約4割）が何らかの活動を実施していた。

対策事例共有活動における活動例
①会員のサイバーセキュリティ対策事例に関する情報共有
②サイバーセキュリティ関連製品・ソリューション等の情報提供
③インシデント対応に関するマニュアル等作成・提供

各活動例の実施状況を加算し、スコア化
未実施・・・0
一部実施・・・1
実施済み・・・2



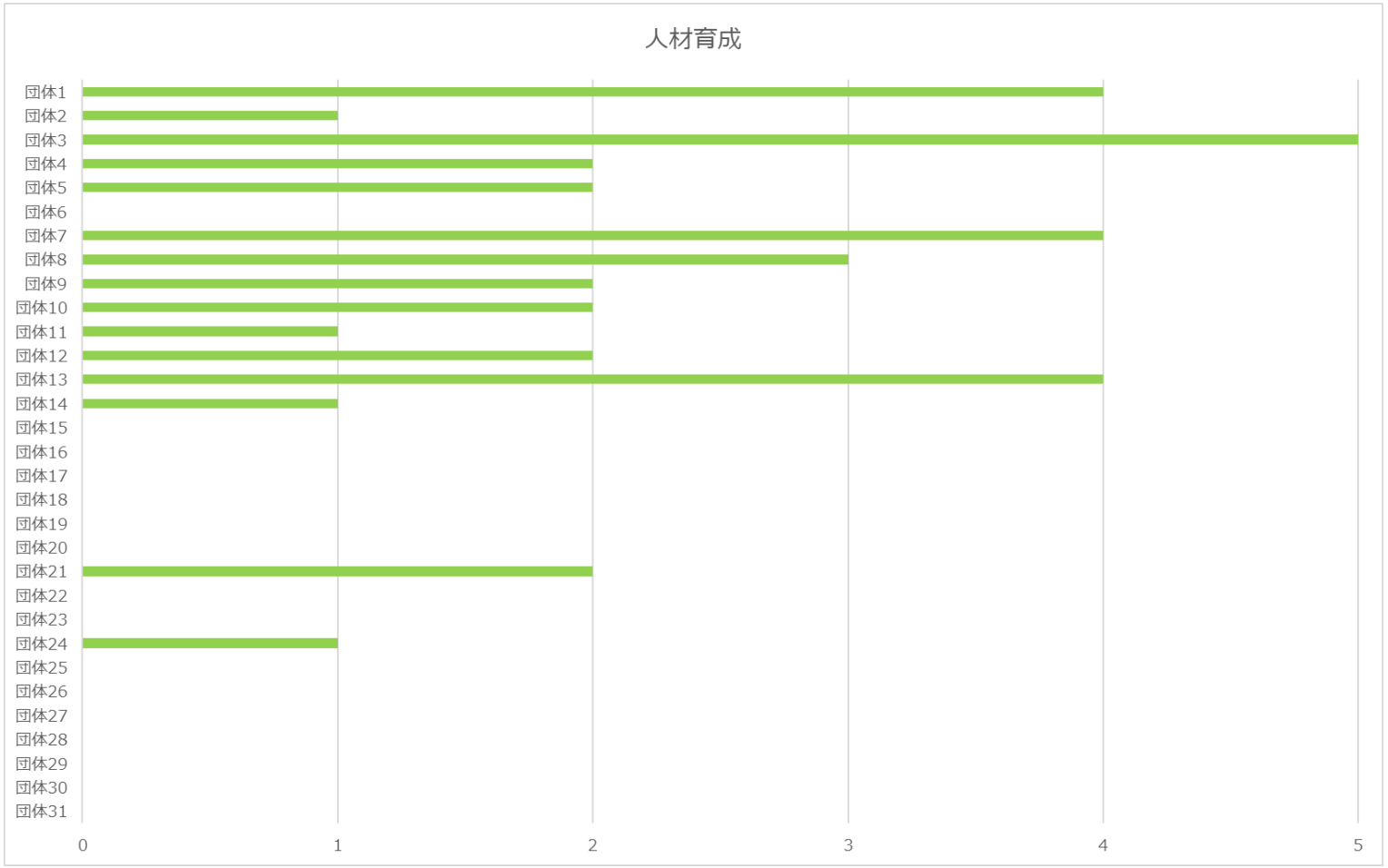
団体向け

# 業界団体におけるセキュリティ活動状況（3. 人材育成）

- 人材育成活動については、15団体（約5割）が何らかの活動を実施していた。

対策事例共有活動における活動例
①セキュリティに関する教育・研修、セミナー等の実施
②サイバーセキュリティ教育コンテンツの作成・提供
③外部事業者のサイバーセキュリティ演習の提供
④業界独自のサイバーセキュリティ演習の企画・実施
⑤各社サイバーセキュリティ演習実施方法に関するマニュアル等作成・提供
⑥国等が実施するサイバーセキュリティ演習への参加

各活動例の実施状況を加算し、スコア化
未実施・・・0
一部実施・・・1
実施済み・・・2



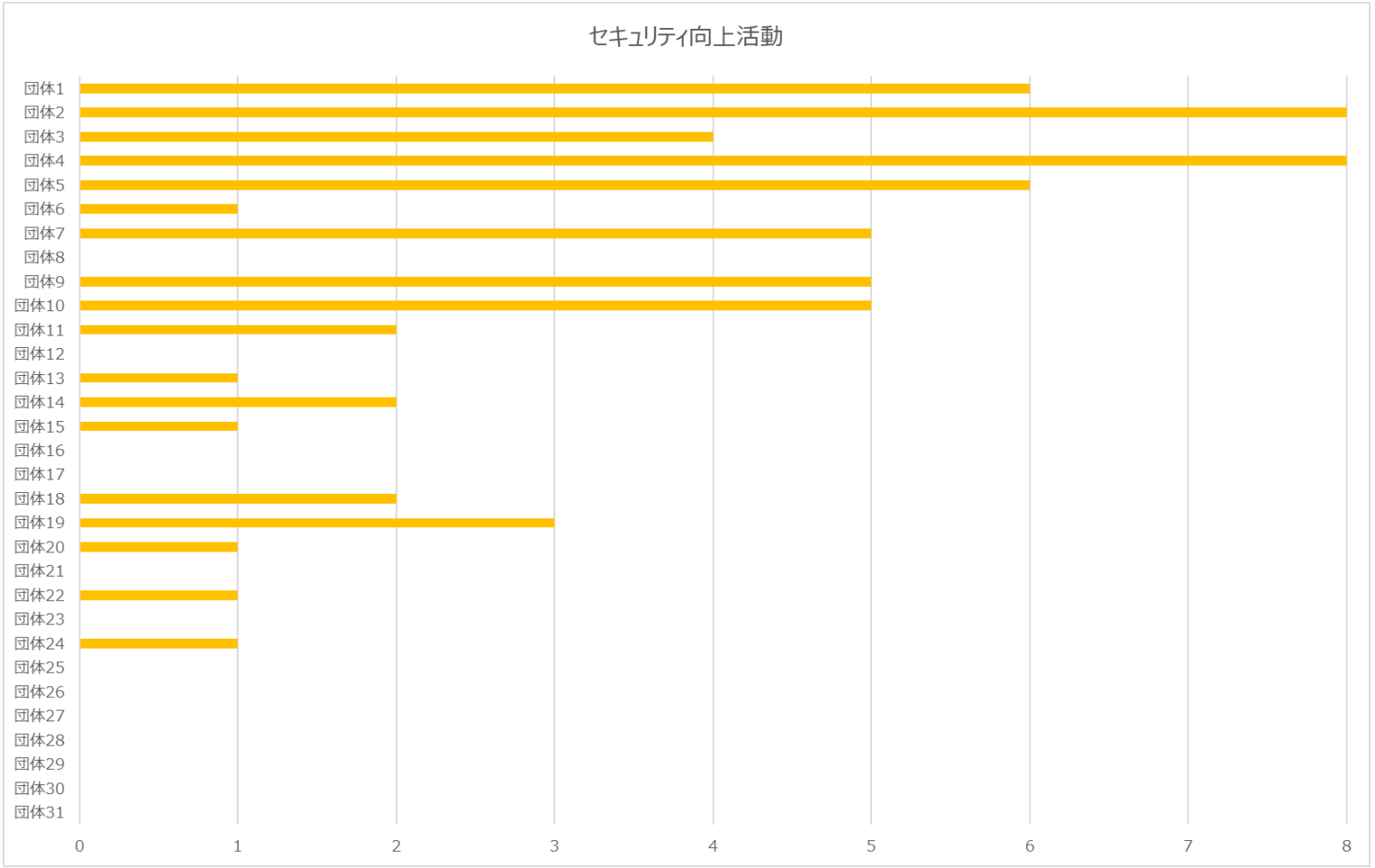
# 業界団体におけるセキュリティ活動状況（4. セキュリティ向上活動）

団体向け

- セキュリティ向上活動については、 18団体（約6割）が何らかの活動を実施していた。

セキュリティ向上活動における活動例
①会員が情報共有を行うための会議体の設置・運用
②業界としてのセキュリティ方針・対策を検討する会議体の設置・運用
③インシデント発生時のサポート（助言、対応支援）
④会員のサイバーセキュリティに関する意識や対策状況等の把握・実態調査
⑤他の業界団体やISAC等とのサイバーセキュリティに関する連携

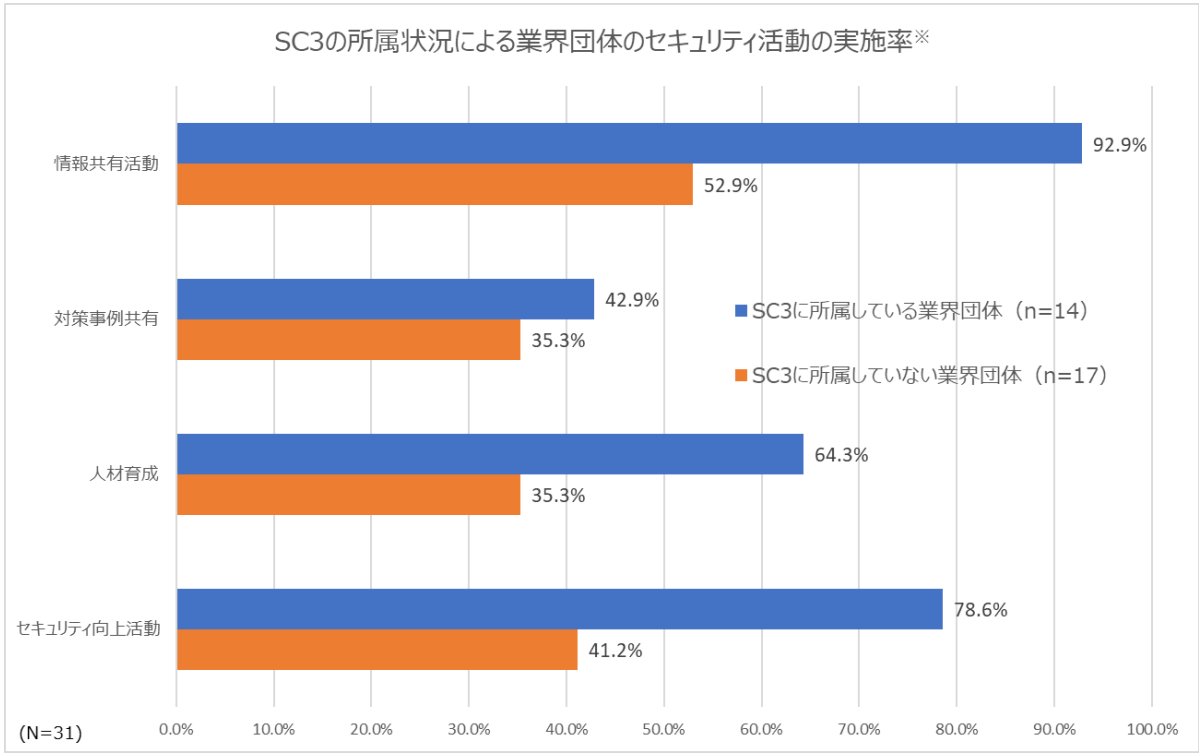
各活動例の実施状況を加算し、スコア化
未実施・・・0
一部実施・・・1
実施済み・・・2



団体向け

# SC3の所属状況による業界団体のセキュリティ活動の差異

- サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）に所属している業界団体と所属していない業界団体における、セキュリティ活動の差異を見ると、**全てのセキュリティ活動において、SC3に所属している業界団体の実施率が高い**。特に、「情報共有活動」や「セキュリティ向上活動」はSC3に所属している業界団体の7割5分以上が実施している。
- したがって、SC3に所属している業界団体はセキュリティ活動を活発に実施している傾向にある。SC3では、中小企業を含む日本のサプライチェーン全体でのセキュリティ対策に関する情報提供・共有を実施していることから、このような情報が業界団体のセキュリティ活動に寄与している可能性があると考えられる。
- 以上から、**業界団体に対して、SC3等のセキュリティに関する情報共有や対策強化に向けた取組を行う組織体への参加を促進し、業界団体のセキュリティ活動に活用可能な情報入手の機会を増やしていくことが望ましい**と考えられる。



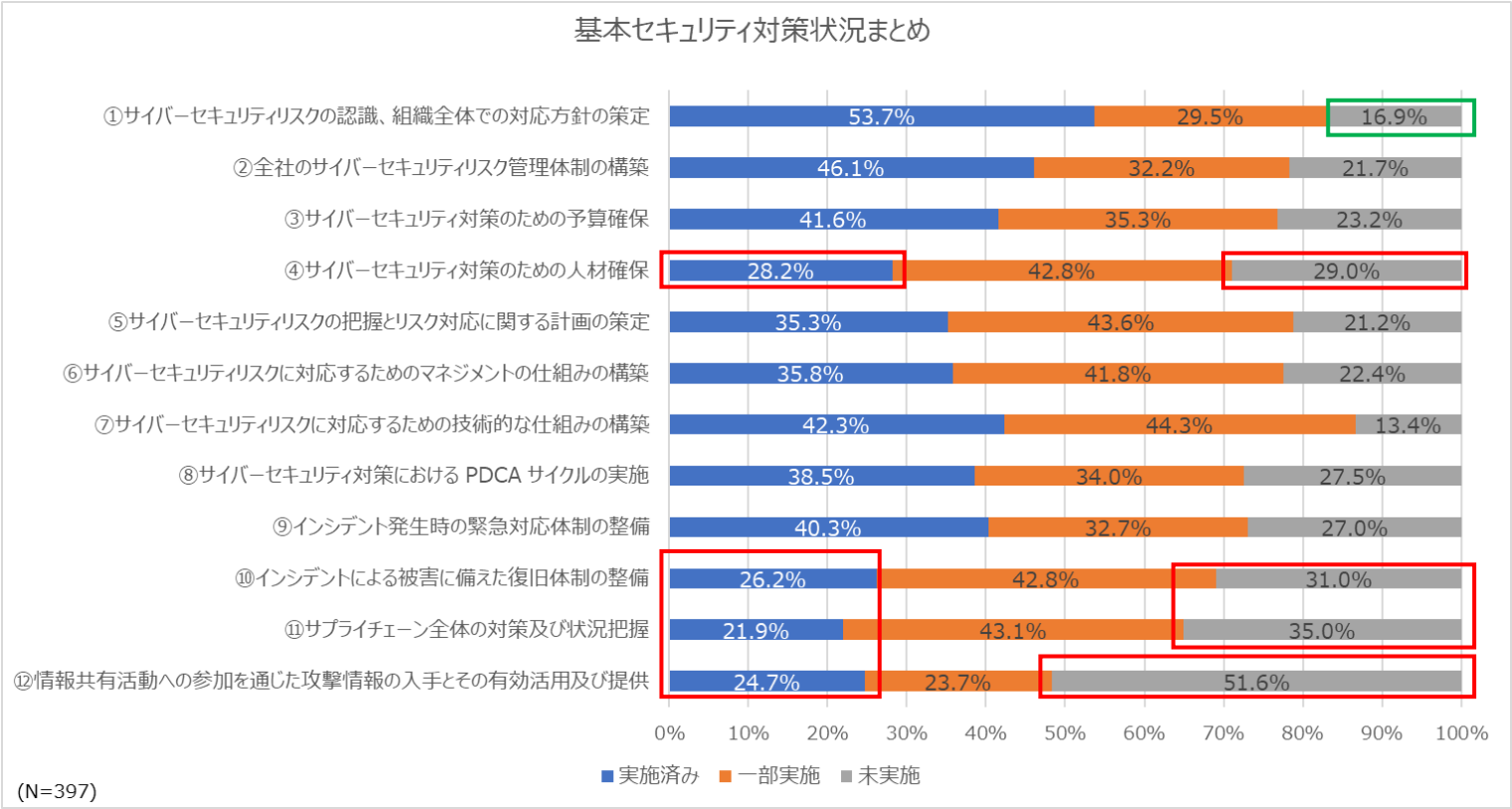

※実施率は、各セキュリティ活動の分類において何らかの活動を実施している業界団体の割合

個社向け

# 会員企業の基本セキュリティ対策状況

**サイバーセキュリティ経営ガイドラインVer 2.0の項目を基に各社の基本セキュリティ対策を確認**

- 「①サイバーセキュリティリスクの認識、組織全体での対応方針の策定」の実施率は高い一方、「**④サイバーセキュリティ対策のための人材確保**」、「**⑩インシデントによる被害に備えた復旧体制の整備**」、「**⑪サプライチェーン全体の対策及び状況把握**」、「**⑫情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供**」においては、**「実施済み」の回答率が低く、「未実施」の回答率が高い**。
- したがって、企業においてはセキュリティリスクを認識できている一方、**人材確保、復旧体制の整備、サプライチェーン対策、情報共有活動に関する対策を実施できていない傾向**にある。



個社向け

# 会員企業の基本セキュリティ対策状況と課題（ヒアリング結果）

- 実施率が低いセキュリティ対策について、その取組が困難な理由を自由記述を基に分析した。
- 人材確保については、**専門人材の育成が困難、専任不在・人員不足による多忙、規模が大きくない企業において担当者を抱えられない等**が課題。
- 復旧体制の整備については、**組織の事業継続の一環としてサイバーセキュリティが考慮されていない**点が課題。
- サプライチェーン対策については、**取引先に求める要求事項や実態の確認方法がわからない、確認のためのリソース不足**が課題。
- 情報共有活動については、**共有する脅威情報等が収集できていない、社外含め情報共有のための体制・手順が未整備**が課題。

| 人材確保 | 復旧体制の整備 | サプライチェーン対策 | 情報共有活動 |
|---|---|---|---|
| • 体系的な人材育成体制の構築ができない<br>• 社内の情報管理を1人で実施している<br>• 専属の担当者がいない<br>• 中堅企業にセキュリティ担当者を抱えるのは難しい | • IT-BCPの取組はあるが、サイバーセキュリティに特化していない<br>• サイバー攻撃を想定したBCPは策定できていない<br>• 都度対応であり、明文化できていない | • 経営資源が不足している<br>• 各取引先の状況に依存している<br>• 社外のセキュリティ対策を確認できない<br>• 取引先のサイバーセキュリティ対策の把握・展開ができていない | • 情報共有すべきインシデント・脅威情報がない<br>• 情報共有するための体制が構築できていない<br>• 社内共有のみで、社外へ共有していない |
| **人材の育成・教育体制が未整備、専任担当者を抱えられない** | **サイバー攻撃を想定したBCP/IT-BCPが未策定** | **取引先に求める要求事項、確認方法が不明確、リソース不足** | **共有する脅威情報等が収集できていない、社外含め情報共有のための体制・手順が未整備** |