業界セキュリティガイドライン等の策定支援業務

業界セキュリティガイドライン等の策定状況

調査報告書

2024年3月29日

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目次

1. 背景・目的

1.1 背景

近年、機密情報を狙ったサイバー攻撃は日々発生し、その被害が確認されている。情報セキュリティ対策が強固とはいえない中小企業を対象としたサイバー攻撃や、それに起因する大企業等の被害も顕在化してきており、大企業のみならずサプライチェーンを構成する中小企業においても、サイバー攻撃の脅威にさらされている実情が明らかになっている。

このような背景のもと、独立行政法人情報処理推進機構（以下「IPA」という。）が事務局を務める「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）」内の「中小企業対策強化 WG」では、2021 年度において「中小企業を含むサプライチェーンにおける情報セキュリティ対策状況等の調査」として、11 分野の業界団体や ISAC 等の団体にヒアリング調査を実施して問題意識を整理し、2022 年度において「業界セキュリティガイドライン等の共通項抽出業務」として、業界団体等が策定しているセキュリティ対策に関するガイドライン（以下「業界セキュリティガイドライン等」という。）」を収集し、複数の業界で共通の基準や要求事項を抽出して共通項をとりまとめ、IPA「中小企業の情報セキュリティ対策ガイドライン」の改訂においても反映した。

2023 年度においては、改訂を行った「中小企業の情報セキュリティガイドライン（第 3.1 版）」をもとに、モデルケース実証として業界セキュリティガイドラインの策定支援、及び加盟企業に対する策定した業界セキュリティガイドライン適用のマネジメント指導を行う「業界セキュリティガイドライン等の策定支援業務」を実施する。モデルケース実証の結果は、業界セキュリティガイドライン展開の導入手引き等の支援ツールとして作成することで、SC3 団体会員（業界団体）での「中小企業の情報セキュリティガイドライン」の活用促進に供することとしている。

1.2 目的

本調査は、業界セキュリティガイドライン等の策定支援を実施するにあたり、SC3 団体会員（業界団体）が行うセキュリティ対策として、業界セキュリティガイドライン等の策定有無、未策定の場合はその理由、策定支援に関する関心度等を調査し、その結果を調査結果として取りまとめることを目的とする。

2. 業界セキュリティガイドライン等の策定状況調査

2.1 調査方針

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）の加盟団体の内、業種別団体57団体に対して、IPA から調査協力依頼のメールを配信し、Web アンケート調査方式（記名式）で 48 件の有効回答を得た。

表 2-1 アンケート調査概要

調査名称	業界セキュリティガイドラインに関するアンケート
調査対象	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）の加盟団体の内、業種別 57 団体
有効回答数	48 件
調査項目数	29項目
調査項目	・業界団体におけるサイバーセキュリティ活動の実施状況 ・「中小企業のセキュリティ対策ガイドライン（3.1 版）」の認知および活用状況 ・業界セキュリティガイドライン等の作成または改訂の意向
調査手法	Web アンケート調査
調査期間	2023 年 10 月 19 日～2023 年 12 月 15 日
発送数	57 件

＜本調査結果で示す図の注意事項＞

- 各設問の回答方法には、単数回答と複数回答の 2 種類がある。
- 図表中の「n」は、集計した回答者数を表している。
- 図や表中の比率は、小数第 2 位を四捨五入しているため、合計が 100%にならないことがある。また、複数回答の設問の比率の合計は、100%を超える場合もある。
- 本文やグラフ・数表上の選択肢表記は場合によっては語句を簡略化してある。

2.2 調査結果

2.2.1 回答者属性

(1) 会員数(設問1-3)

回答者の会員数(正会員以外の会員も含む)は、「100 社～500 社未満」(50.0%)が最も多く、以下「10 社～50 社未満」(25.0%)、「50 社～100 社未満」(16.7%)の順となっている。

表 2-2 会員数(設問 1-3)

会員会社数	件数
10 社未満	1
10 社～50 社未満	12
50 社～100 社未満	8
100 社～500 社未満	24
500 社～1,000 社未満	0
1000 社以上	2
無回答	1
総計	48

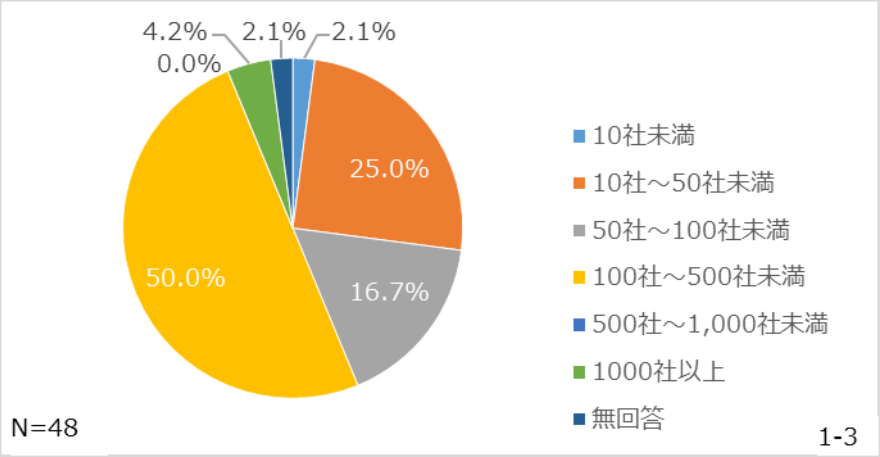

図 2-1 会員数(設問 1-3)

(2) 会員における業種(設問 1-6)

回答者の会員における業種は、「製造業」(52.1%)がもっと多く、以下「その他」(16.7%)、「卸売業,小売業」(8.3%)の順となっている。

表 2-3 会員における業種(設問 1-6)

業種	件数
製造業	25
電気・ガス・熱供給・水道業	2
情報通信業	1
卸売業, 小売業	4
金融業, 保険業	2
生活関連サービス業, 娯楽業	1
医療, 福祉	3
その他	8
無回答	2
総計	48

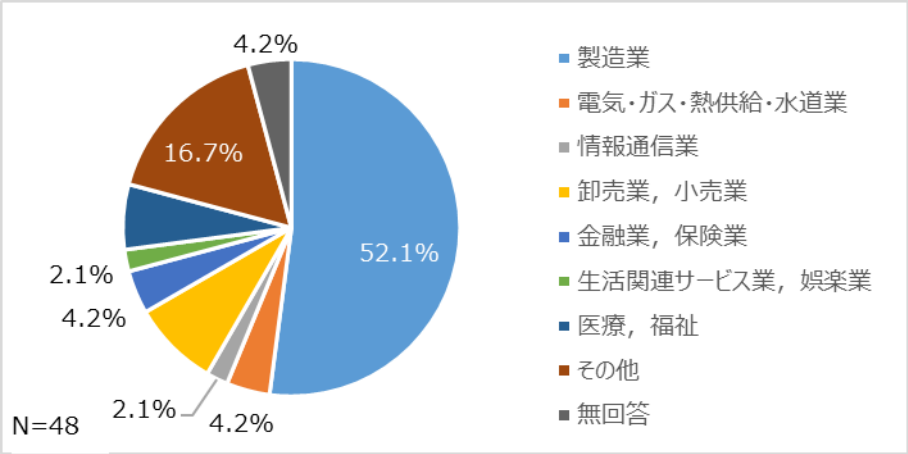

図 2-2 会員におおける業種(設問 1-6)

(3) 会員における企業規模の割合(設問 1-4)および製造業とサービス業の割合(設問 1-5)

回答者ごとに、会員の企業規模の割合(大企業、中小企業、その他の合計が 100%)、および製造業(工場を持つ企業)とサービス業の割合(製造業、サービス業、その他の合計が 100%)を調査した。調査結果を、回答団体の業種及び会員数で整理した。

表 2-4　企業規模の割合（設問 1-4）および製造業とサービス業の割合（設問 1-5）

業界団体		企業規模の割合			製造業とサービス業の割合		
業種	会員数	大企業	中小企業	その他	製造業	サービス業	その他
電気・ガス・熱供給・水道業（2）	100～500 未満	20%	80%	0%	0%	0%	100%
	10～50 未満	100%	0%	0%	0%	0%	100%
製造業（25） ※無回答 2 件	100～500 未満	85%	15%	0%	91%	9%	0%
		78%	20%	2%	50%	45%	5%
		70%	25%	5%	50%	50%	0%
		60%	30%	10%	60%	30%	10%
		42%	21%	37%	90%	0%	10%
		42%	58%	0%	83%	17%	0%
		30%	70%	0%	100%	0%	0%
		20%	80%	0%	10%	90%	0%
		10%	90%	0%	80%	20%	0%
		5%	95%	0%	100%	0%	0%
		5%	95%	0%	100%	0%	0%
	50～100 未満	100%	0%	0%	90%	10%	0%
		50%	50%	0%	90%	10%	0%
		50%	30%	20%	50%	30%	20%
		20%	80%	0%	80%	10%	10%
		14.5%	85.5%	0%	80%	20%	0%
		10%	80%	10%	60%	40%	0%
		0%	90%	10%	100%	0%	0%
	10～50 未満	100%	0%	0%	100%	0%	0%
		100%	0%	0%	100%	0%	0%
		54%	46%	0%	100%	0%	0%
		0%	100%	0%	100%	0%	0%
	10 未満	100%	0%	0%	100%	0%	0%
生活関連サービス業，娯楽業（1）	10～50 未満	43%	30	27%	18%	55%	27%
金融業，保険業（2） ※無回答 1 件	10～50 未満	95%	0%	5%	0%	100%	0%
卸売業，小売業（4） ※無回答 1 件	1000 以上	30%	70%	0%	0%	100%	0%
		2%	98%	0%	0%	0%	100%
	100～500 未満	65%	30%	5%	25%	70%	5%
医療，福祉（3） ※無回答 1 件	100～500 未満	20%	75%	5%	20%	75%	5%
		5%	95%	0%	5%	95%	0%
	10～50 未満	20%	80%	0%	25%	0%	75%
情報通信業（1）	50～100 未満	（無回答）			0%	0%	100%
その他（8） ※無回答 1 件	100～500 未満	70%	10%	20%	60%	20%	20%
		30%	70%	0%	90%	10%	0%
		0%	10%	90%	0%	100%	0%
		80%	7%	13%	60%	30%	10%
	10～50 未満	0%	0%	100%	0%	0%	100%
		0%	100%	0%	60%	40%	0%
	（無回答）	51%	41%	8%	28%	43%	29%

※業種の記載で、丸かっこ内の数字は会員企業の数（表 2-3 を参照）

2.2.2 業界団体におけるサイバーセキュリティ活動の実施状況

(1) 脅威・インシデント等の情報共有に関する実施状況(設問 2-1)

業界団体における脅威・インシデント等の情報共有に関する実施状況を質問したところ、実施済みと回答した活動としては「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」(45.8%)が最も多く、一部実施(50.0%)を含めると 10 割近くが実施していた。次いで「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」(25.0%)で、一部実施(39.6%)を含めると 6 割以上が実施していた。これらのことから、脅威・インシデント等の会員への情報提供はある程度実施されていることが伺える。

一方、未実施と回答した活動としては「会員間の情報共有の仕組みの構築・運営」(52.1%)が最も多く、次いで「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」(43.8%)が実施されていないという回答だった。会員間の情報共有の仕組みや、会員のインシデント情報を元にした注意喚起は 5 割程度しか進んでいない様子が伺える。

表 2-5 脅威・インシデント等の情報共有に関する実施状況(設問 2-1)

	未実施	一部実施	実施済み	無回答	全体
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	4.2%	50.0%	45.8%	0.0%	100.0%
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	35.4%	39.6%	25.0%	0.0%	100.0%
会員間の情報共有の仕組みの構築・運営	52.1%	29.2%	14.6%	4.2%	100.0%
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	43.8%	35.4%	14.6%	6.3%	100.0%
その他	50.0%	6.3%	8.3%	35.4%	100.0%

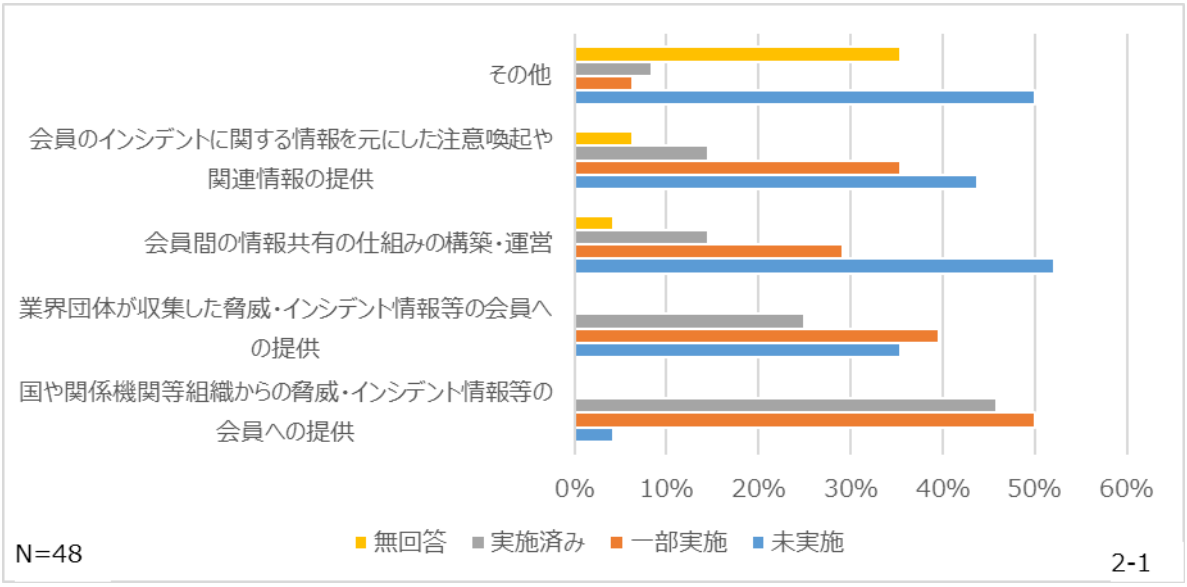

図 2-3 脅威・インシデント等の情報共有に関する実施状況(設問 2-1)

（2）脅威・インシデント等の情報共有に関する具体的な内容（設問 2-2）

（設問 2-1）の脅威・インシデント等の情報共有に関する具体的な取り組み内容について、自由記述で得られた主な回答内容を以下に示す。

表 2-6 脅威・インシデント等の情報共有に関する具体的な内容（設問 2-2）

化学工業分野で J-CSIP に参加している企業間で定期的に情報共有のための会合、講演会を開催している。また、毎月セキュリティに関するニュースを発行している。
月一回の委員会にてサイバーセキュリティ技術動向などを会員企業と共有。年二回の講演にて、協会外の企業とも共有。
会員企業は同業種がほとんどだが、夫々の会社によりセキュリティ対策の相違がある。ISMS 認証を受けている会社が10社以上、プライバシーマーク取得会社が20社程度あるが、その他の会社については個々セキュリティ対策レベルは分からない。今後アンケートによる個別調査を行い、対策実施状況を把握したい。
サイバーセキュリティ活動は電力 ISAC として実施。
協会内で発生したインシデントに関して、注意喚起の発信を行った。
SC3 事務局からの注意喚起等お知らせの会員への案内
国や関係機関等組織からの脅威・インシデント情報をメールで会員へ提供
医療機関内のセキュリティ調査の声掛け、サイバーセキュリティ対策 TF の立ち上げ、情報配信サービス等
当協会ウェブサイト上の「行政・関係機関からのお知らせ」欄に、国や関係機関等から寄せらせた情報を掲載している。
経産省から発行されている「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 Ver1.0」を元にした中小製造業向けの工場セキュリティ構築のためのガイドライン発行。
会員向けに一斉通知やメルマガ配信、事例説明会を通じて情報提供を実施。
IPA の J-CSIP 鉄鋼 SIG に参画
技術情報管理認証制度の認証取得を奨励
IPA からもらった情報の転送
案件ごとに会員 HP に掲載。範囲が狭いものは、技術委員会や広報委員会で展開。
ホームページ等で会員に開示
セミナーの開催
IPA からの SC3 提供情報を会員へ提供
「通信ネットワーク機器セキュリティ・ユーザーガイドライン」（機器ユーザ向け）の策定・公表、およびその他「通信ネットワークセキュリティ関連情報」の公表
IPA/SC3、政府省庁から受領したセキュリティ関連情報の会員展開（メール）
会員のインシデントに関する情報は、規制上のルール（不具合報告）による。
会員限定のメールマガジン「事務局便り」により、必要に応じて情報を提供する。
セキュリティセミナーの開催
ダイレクトメールによる情報共有や勉強会の実施。

(3) サイバーセキュリティ対策事例の共有に関する実施状況(設問 2-3)

業界団体におけるサイバーセキュリティ対策事例の共有に関する実施状況を質問したところ、実施済みと回答した活動としては「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」(8.3%)が最も多く、一部実施(25.0%)を含めると 3 割以上が実施していた。次いで「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」(4.2%)で、一部実施(39.6%)を含めると約 4 割が実施していた。いずれも、3～4 割の実施であり、サイバーセキュリティ対策事例の共有は進んでいないと言える。

一方、「インシデント対応に関するマニュアル等の作成・提供」は 77.1%が未実施で、業界団体としてのインシデント対応マニュアルの作成・提供活動はあまり行われていないことが伺える。

表 2-7 サイバーセキュリティ対策事例の共有に関する実施状況(設問 2-3)

	未実施	一部実施	実施済み	無回答	全体
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	60.4%	25.0%	8.3%	6.3%	100.0%
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	54.2%	35.4%	4.2%	6.3%	100.0%
インシデント対応に関するマニュアル等の作成・提供	77.1%	16.7%	2.1%	4.2%	100.0%
その他	52.1%	6.3%	2.1%	39.6%	100.0%

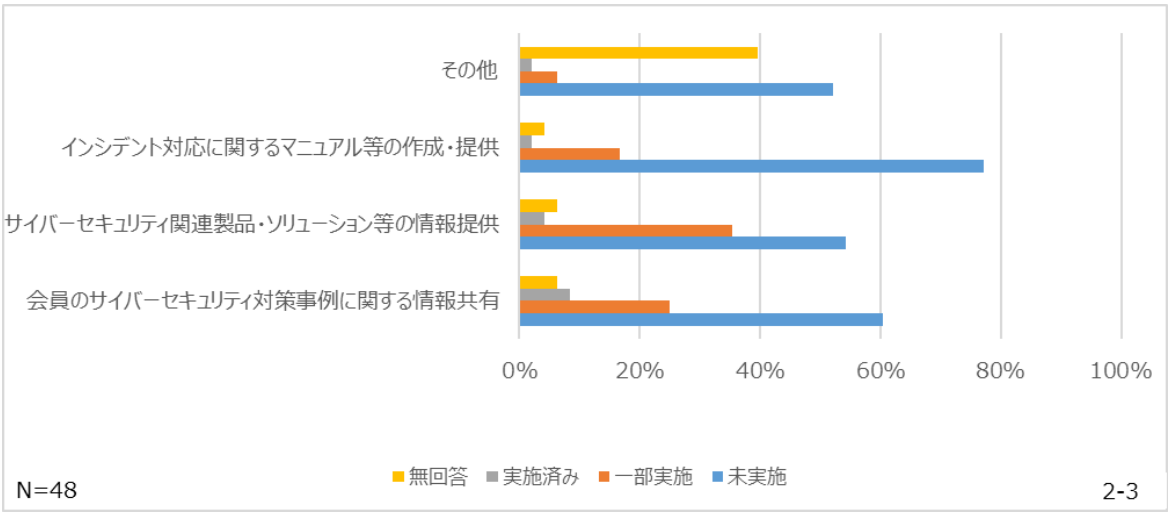

図 2-4 サイバーセキュリティ対策事例の共有に関する実施状況(設問 2-3)

（4）サイバーセキュリティ対策事例の共有に関する具体的な取り組み内容（設問 2-4）

（設問 2-3）のサイバーセキュリティ対策事例の共有に関する具体的な取り組み内容について、自由記述で得られた主な回答内容を以下に示す。

表 2-8 サイバーセキュリティ対策事例の共有に関する具体的な取り組み内容（設問 2-4）

IPA、SC3、経済産業省、警察庁などからの注意喚起の配信など
他団体とのコラボレーションにて、インシデント対応における留意点などを会員企業と共有
IPA から発信される情報は、その都度会員向けに発信している。
業界標準類としてのガイドラインの作成
事例説明会にて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を実施。
サイバーセキュリティ―関連のセミナーの情報などを適宜展開。
協会においては ISMS を取得し、協会内の啓発に努めている。
業界関連団体と協業してガイドラインの作成、自己評価の依頼、困りごと相談会の開催
「通信ネットワーク機器セキュリティ・ユーザーガイドライン」（機器ユーザ向け）の策定・公表
NISC 医療セプター及び IPA 発行文書に関する情報は共有している。
マルウェア、スパイウェア/グレーウェア、挙動不審接続監視、ポリシー違反ログ等に関する情報を恒常的にウォッチし、職員に提供する。

（5）サイバーセキュリティ人材育成に関する実施状況（設問 2-5）

業界団体におけるサイバーセキュリティ人材育成に関する実施状況を質問したところ、実施済みと回答した活動としては「セキュリティに関する教育・研修、セミナー等の実施」（16.7%）が最も多く、一部実施（33.3%）を含めると約 5 割が実施していた。

一方、未実施と回答した活動としては、「サイバーセキュリティ教育コンテンツの作成・提供」（81.3%）、「外部事業者のサイバーセキュリティ演習の提供」（87.5%）、「業界独自のサイバーセキュリティ演習の企画・実施」（85.4%）、「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」（85.4%）が多く、業界団体としてのサイバーセキュリティ教育コンテンツの作成・提供、およびサイバーセキュリティ演習に関する取組みは進んでいないことが伺える。

表 2-9 サイバーセキュリティ人材育成に関する実施状況（設問 2-5）

	未実施	一部実施	実施済み	無回答	全体
セキュリティに関する教育・研修、セミナー等の実施	47.9%	33.3%	16.7%	2.1%	100.0%
サイバーセキュリティ教育コンテンツの作成・提供	81.3%	8.3%	6.3%	4.2%	100.0%
外部事業者のサイバーセキュリティ演習の提供	87.5%	4.2%	4.2%	4.2%	100.0%
業界独自のサイバーセキュリティ演習の企画・実施	85.4%	6.3%	4.2%	4.2%	100.0%
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	85.4%	8.3%	2.1%	4.2%	100.0%
国等が実施するサイバーセキュリティ演習への参加	64.6%	25.0%	8.3%	2.1%	100.0%
その他	57.8%	2.2%	0.0%	40.0%	100.0%

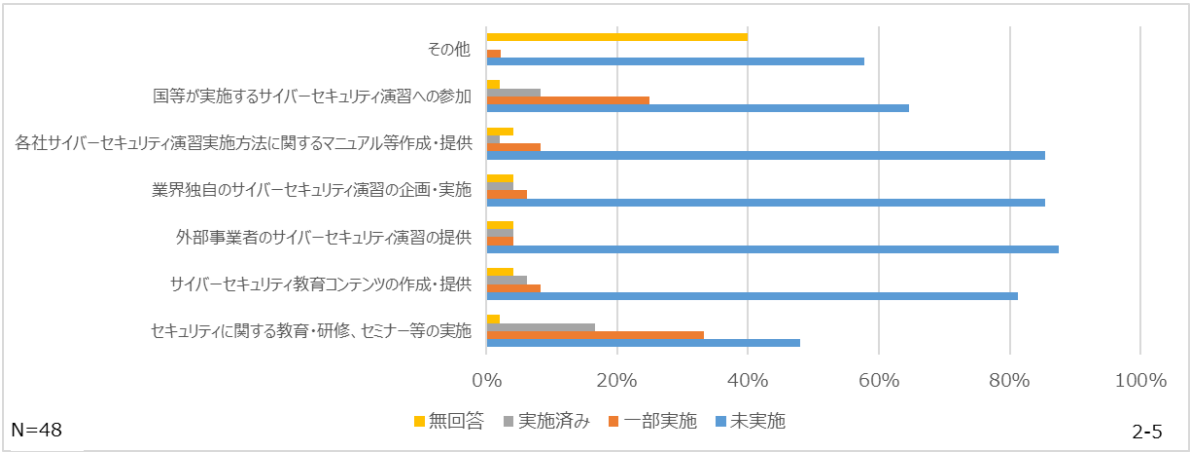

図 2-5 サイバーセキュリティ人材育成に関する実施状況(設問 2-5)

(6) サイバーセキュリティ人材育成に関する具体的な内容(設問 2-6)

(設問 2-5)のサイバーセキュリティ人材育成に関する具体的な取り組み内容について、自由記述で得られた主な回答内容を以下に示す。

表 2-10 サイバーセキュリティ人材育成に関する具体的な内容(設問 2-6)

IPA による講演会実施
協会独自にサイバーセキュリティ関連の教材コンテンツを開発し、会員企業と共有。協会外にも共有。
ISMS に関する情報提供を個別会社間で行ったという実績はあるが、各社の個別対応に任せている。
サイバーセキュリティ人材育成は電力 ISAC として実施。
情報セキュリティポリシーの作成、情報セキュリティ委員会の運営、標的型メール訓練の実施など。但し、協会会員ではなく、協会内部活動として、協会職員を対象としたもの。
独自セミナーおよび厚生労働省と連携したセミナーの開催
サイバー攻撃発生時の情報収集、報告ルールの定着を目的とした情報連絡訓練を実施。
IPA から頂く講演案内の回覧
当協会に所属する会員向け研修実施
総会において IPA の講演を実施
セミナーの開催
一部会員メンバーによる NICT「ナショナルサイバートレーニングセンター」のプログラム受講
薬機法に基づく製品サイバーセキュリティに関する教育、セミナー実施。

(7) 業界のセキュリティ向上に関する検討に関わる活動(設問 2-7)

業界団体における業界のセキュリティ向上に関する検討に関わる活動について質問したところ、実施済みと回答した活動は「会員が情報共有を行うための会議体の設置・運用」(22.9%)が最も多いが、一部実施(22.9%)を含めても 5 割を下回る。また、「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」、「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」についても、一部実施を含めても 3 割程度であった。

「インシデント発生時のサポート(助言、対策支援)」は 8 割以上が未実施で、「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」についても 7 割が未実施で、業界団体としての検討が進んでいない。

表 2-11 業界のセキュリティ向上に関する検討に関わる活動(設問 2-7)

	未実施	一部実施	実施済み	無回答	全体
会員が情報共有を行うための会議体の設置・運用	52.1%	22.9%	22.9%	2.1%	100.0%
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	64.6%	14.6%	18.8%	2.1%	100.0%
インシデント発生時のサポート(助言、対策支援)	83.3%	8.3%	4.2%	4.2%	100.0%
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	70.8%	10.4%	14.6%	4.2%	100.0%
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	66.7%	20.8%	10.4%	2.1%	100.0%
その他	58.3%	0.0%	2.1%	39.6%	100.0%

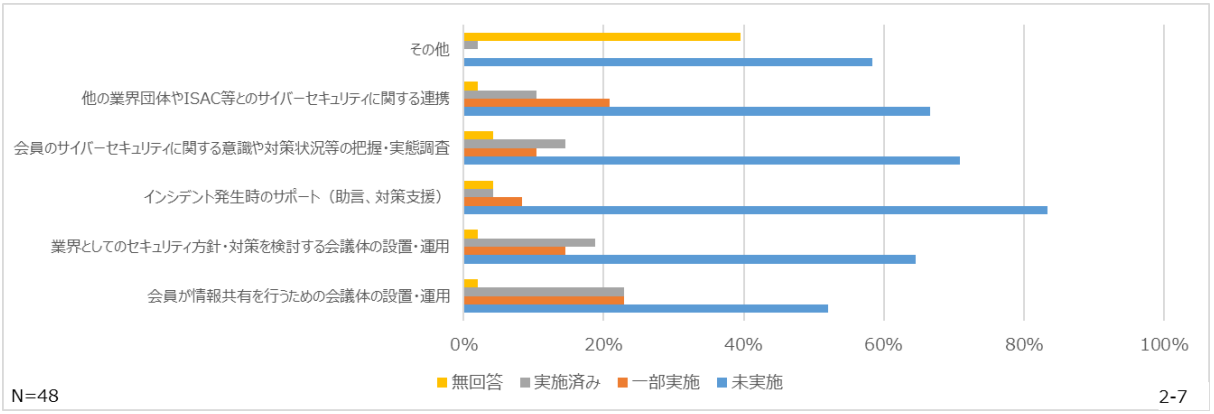

図 2-6 業界のセキュリティ向上に関する検討に関わる活動(設問 2-7)

（8）業界のセキュリティ向上に関する検討に関わる具体的な内容（設問 2-8）

（設問 2-7）の業界のセキュリティ向上に関する検討に関わる具体的な取り組み内容について、自由記述で得られた主な回答内容を以下に示す。

表 2-12 業界のセキュリティ向上に関する検討に関わる具体的な内容（設問 2-8）

制御系のサイバーセキュリティに関して、会員向けガイドラインの作成のための勉強会を実施中。
JPCERT との連絡会議を定期的に実施。
月一回の委員会にてサイバーセキュリティ技術動向などを会員企業と共有。
年二回の講演にて、協会外の企業とも共有。
インシデント発生時のサポートは電力 ISAC として実施。
電力 ISAC との連携
情報処理安全確保支援士を外部派遣として採用し、情報セキュリティ活動の向上を行っている。
サイバーセキュリティ対策 TF の立ち上げ、セキュリティ委員会の設置（従来よりあり）
セミナーにおいて、厚生労働省、IPA、ISAC 等と連携
せきゅちてぃ委員会の開催（1回/月）
工場セキュリティに関するアンケート
業界内に会員事業者と構成するセキュリティ方針・対策を検討する会議体の設置・運用。
IPA の J-CSIP 鉄鋼 SIG に参画
悪質クレーマーの情報は会員間で共有するシステムがある。大きなハッキングがあったら状況を聞いて会員に流したい。
会員にサイバーセキュリティの保険を勧めている
業界としてのセキュリティ方針・対策というよりは、業界共通のシステムのセキュリティ方針・対策の検討が主な目的となっている。
IPA による設計品質ガイドライン策定への一部会員メンバー参加、 JEITA「スマートホーム部会・サイバーセキュリティ WG」への参加、総務省・経産省によるサイバーセキュリティ関連委員会への参画
正会員対象のシステム部会

（9）業界団体におけるセキュリティ課題（設問 2-9）

業界団体におけるセキュリティ課題について質問したところ、「会員企業のセキュリティの実態が把握できていない」（23.4%）が最も多く、次いで「会員企業における共通のセキュリティ課題が明確にできていない」（20.4%）、の回答が多かった。

表 2-13 団体におけるセキュリティ課題（設問 2-9）

回答	件数
会員企業のセキュリティの実態が把握できていない	32
会員企業における共通のセキュリティ課題が明確にできていない	28
業界団体にセキュリティに関する活動を推進するための知識・知見が不足している	24
会員企業の実態を把握した上で、業界としてのガイドライン・指針等を策定するのが難しい	21
会員企業に対して具体的なセキュリティ対策を示せていない	22
特に無し	7
その他	3

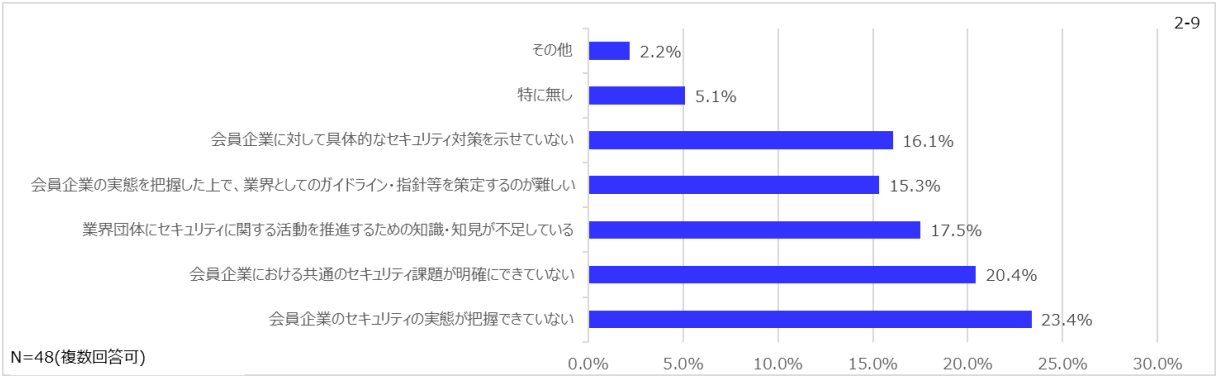

図 2-7 団体におけるセキュリティ課題(設問 2-9)

(10) セキュリティ課題の具体的な内容(設問 2-10)

(設問 2-9)の業界団体におけるセキュリティ課題について、自由記述で得られた主な回答内容を以下に示す。

表 2-14 セキュリティ課題の具体的な内容(設問 2-10)

制御系のサイバーセキュリティに関して、会員向けガイドラインの作成のための勉強会を実施中。
小規模事業者が大半を占めていること、各社により顧客対応に相違があることなどにより、一律な研修を実施することは困難。個々の会社の顧客からの要望により、それぞれが対応しているのが実情である。
現在は協会内部組織の情報セキュリティ強化を優先している段階。内部組織のセキュリティ向上をはたしたのちに、外部会員に対するセキュリティ強化を検討する
会員企業の顧客である医療機関のサイバーセキュリティに関する意識のレベルや対応体制がまちまちである。
会員企業に対しては(会員数が少ないこともあって)実態把握等できているが、業界全体・サプライチェーン全体については実態の把握は十分にはできていない。
会員企業は大企業が多く、すでに社内でセキュリティ対策を実施している。特に当会から会員へのセキュリティ対策への指導はなし。
会員が当団体に求めているのは指導まで行かず、情報提供だけである。定款にも特に書かれていない。大企業は独自に進めているし、中小企業はまだ必要性を感じていない。あまり各企業の内部まで入り込まないようにしている。
エンジン関連企業の業界団体であるが、企業規模によって対策がまちまちなので、基本各社の自助努力に任せている。
会員が医療機関から対策等求められるが、専任の担当者がいないので対応できない。一部の企業においては、情報系の担当者すらいない。(IT ベンダー任せ)
自己評価数が意外と低い
当協会は、通信機器製造事業者・通信事業者の業界団体であり、本業の製品・サービスに関するセキュリティ対策の側面と、一般的な企業としての各社情報通信システムのセキュリティ対策の側面があるが、いずれも細部については、企業秘密であるため、具体的な状況は把握できていない。
”Secure by Design”の基礎を各企業が学べるような教育・トレーニングプログラムが至急必要である。

(11) 業界セキュリティガイドライン等や文書の作成状況(設問 2-11)

業界団体における業界セキュリティガイドライン等や文書の作成状況を対象範囲毎に質問したところ、作成・公表済みと回答した文書は「組織」に関するもの(18.8%)が最も多いが、作成中(2.1%)も含めても約 2 割しか作成されていなかった。「工場」「製品」「サプライチェーン」「その他」、いずれも作成・公表済みと回答した文書は 1 割に満たないが、作成中と回答した文書は「工場」(6.3%)、「サプライチェーン」(6.3%)に関するものが多く、作成が進みつつある状況がみられる。

表 2-15 業界セキュリティガイドライン等や文書の作成状況(設問 2-11)

	未作成	作成中	作成 公表済	無回答	全体
組織 (例:企業が有する情報や、情報システムの設計・構築・運用に関するセキュリティ要件)	72.9%	2.1%	18.8%	6.3%	100.0%
工場 (例:工場やプラント等の制御システムの設計・構築・運用に関するセキュリティ要件)	79.2%	6.3%	6.3%	8.3%	100.0%
製品 (例:開発・製造する製品が備えるセキュリティ要件)	83.3%	0.0%	8.3%	8.3%	100.0%
サプライチェーン (例:部品、サービス、役務等提供を行う外部委託先に求めるセキュリティ要件)	77.1%	6.3%	8.3%	8.3%	100.0%
その他	56.3%	0.0%	8.3%	35.4%	100.0%

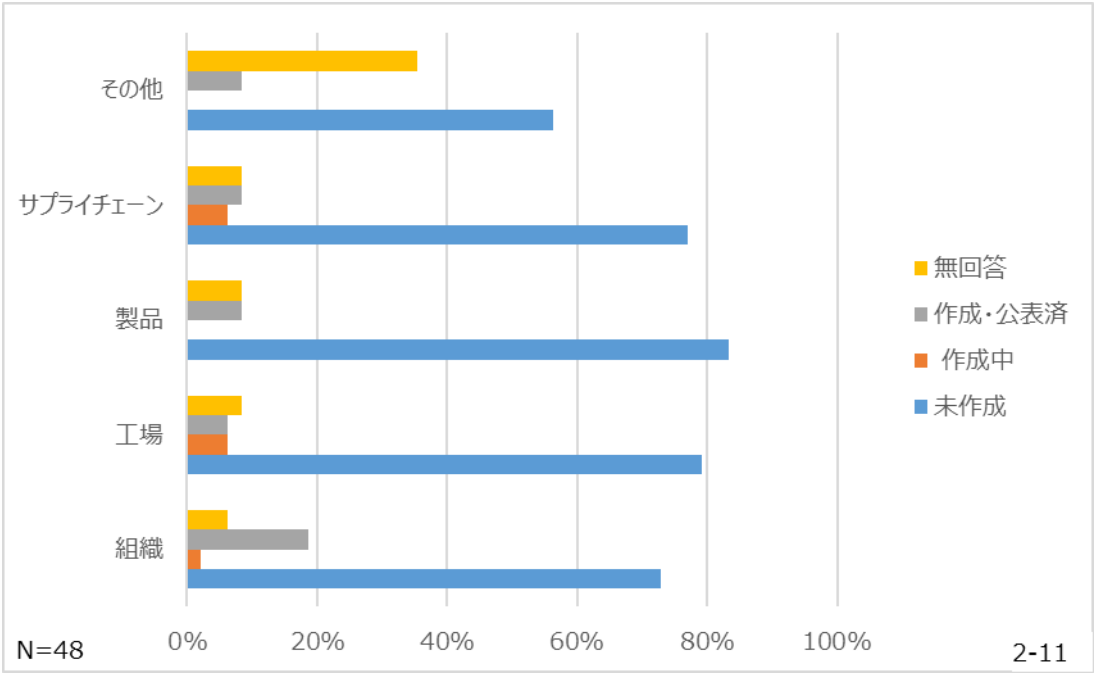

図 2-8 業界セキュリティガイドライン等や文書の作成状況(設問 2-11)

1）「その他」の詳細

（設問 2-11）で「その他」と回答された詳細について、自由記述で得られた主な回答内容を以下に示す。

表 2-16 業界セキュリティガイドライン等や文書の作成状況「その他」の詳細

現在、組織の中での対応はコアになる人選自体が難しい状況である
日本電気協会の電力制御システムセキュリティガイドライン、スマートメーターシステムセキュリティガイドラインとして公表済
JAHIS リモートサービス セキュリティガイドライン Ver.3.1a
都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領（参考例） 都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領（参考例）の解説
製造業（大手）においては作成されていると思われるが、販売業においては中小企業が多く未対応と考えられる。
製品（例：開発・製造する製品が備えるセキュリティ要件）のガイドライン策定については、国内外の基準制定状況等を鑑み、従うべき基準の乱立等を防ぐ意味から、敢えて策定しない方針。
各種のセキュリティ関連情報の調査を実施し、その内容を適宜公表（内容は多岐に渡るため具体的情報は省略）。
協会内規程「情報セキュリティ対策基準」を整備済み。

（12）「作成中」、「作成・公表済」のガイドラインや文書の名称（設問 2-12）

（設問 2-11）の「作成中」、「作成・公表済」のガイドラインや文書の名称について、自由記述で得られた主な回答内容を以下に示す。

表 2-17 「作成中」、「作成・公表済」のガイドラインや文書の名称（設問 2-12）

名称は非公表
情報セキュリティ関連規程、情報セキュリティ基本方針 ※どちらも組織内部用であり公開していない。
JAHIS「製造業者/サービス事業者による医療情報セキュリティ開示書」ガイド Ver.4.1（MDS/SDS） JAHIS シングルサインオンにおけるセキュリティガイドライン Ver.2.1 JAHIS 保存が義務付けられた診療録等の電子保存ガイドライン Ver.4 JAHIS リモートサービス セキュリティガイドライン Ver.3.1a
はじめて工場セキュリティを導入するためのガイドライン
一般社団法人日本鉄鋼協会にて作成済
自工会・部工会サイバーセキュリティガイドライン
BMSec（事務機セキュリティプログラム）
情報セキュリティ実施要領
自工会/部工会・サイバーセキュリティガイドライン
石油分野における情報セキュリティ確保に係る安全ガイドライン →ただし、公表はしていない。また、現在、改訂作業中。
「情報セキュリティ基本方針」、「情報セキュリティ関連規程」（協会事務局としてのセキュリティ基準文書であり一般公開していない）
医療機器のサイバーセキュリティ導入に関する手引書」 「医療機関における医療機器のサイバーセキュリティ確保のための手引書」

（13）「作成中」、「作成・公表済」のガイドライン・文書で参考にした文書（設問 2-13）

（設問 2-12）の「作成中」、「作成・公表済」のガイドラインや文書について、参考にした文書を質問したところ、「ISO/IEC27000 シリーズ」と「その他」が最も多く、次いで「NIST サイバーセキュリティフレームワーク」、「NIST SP800 シリーズ」が多かった。

表 2-18 「作成中」、「作成・公表済」のガイドライン・文書で参考にした文書（設問 2-13）

回答	件数
サイバーセキュリティ経営ガイドライン	2
中小企業の情報セキュリティ対策ガイドライン	4
サイバー・フィジカル・セキュリティ・対策フレームワーク	3
IoT セキュリティガイドライン	2
ISO/IEC27000 シリーズ	7
NIST サイバーセキュリティフレームワーク	5
NISTSP800 シリーズ	6
IEC62443 シリーズ	4
その他	7

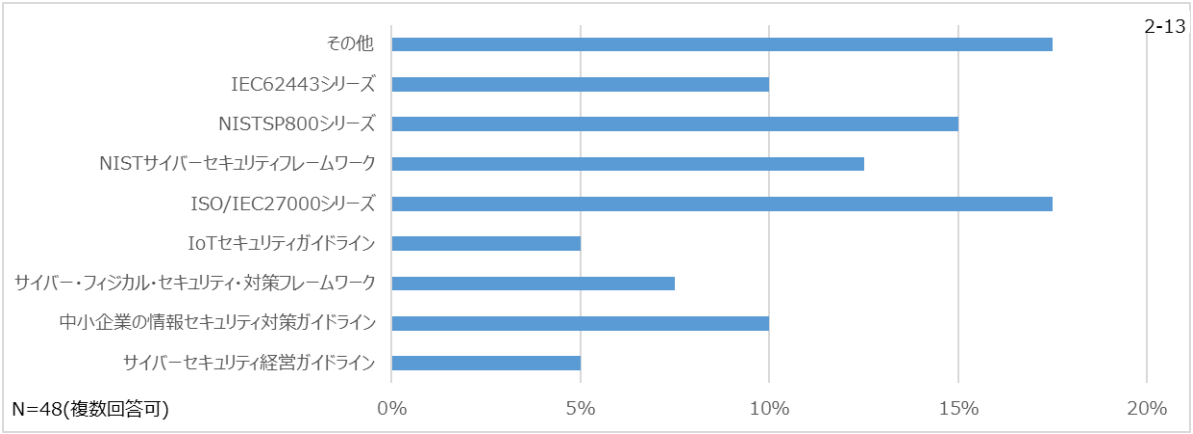

図 2-9 「作成中」、「作成・公表済」のガイドライン・文書で参考にした文書（設問 2-13）

1）「その他」の詳細

（設問 2-13）で「その他」と回答された詳細について、自由記述で得られた主な回答内容を以下に示す。

表 2-19 ガイドライン・文書で参考にした文書「その他」の場合の詳細

「政府機関等のサイバーセキュリティ対策のための統一基準」（令和3年度版） 「経済産業省情報セキュリティ管理規定」（平成18・03・22シ第1号） 「経済産業省情報セキュリティ対策基準」（平成18・03・24シ第1号）
医療情報システムの安全管理に関するガイドライン 医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン
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 スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン
他業界のマニュアル及び NISC 指針等
技術情報管理認証制度の認証取得の推進
IMDRF、N60:2020 Principles and Practices for Medical Device Cybersecurity IMDRF、N70:2023 Principles and Practices for the Cybersecurity of Legacy Medical Devices IMDRF、N73:2023 Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity IPA、脆弱性対処に向けた製品開発者向けガイド 2020 NTIA、How to Guide for SBOM Generation 2021 NTIA、Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM) Second Edition 2021 NTIA、The Minimum Elements For a Software Bill of Materials (SBOM) 2021

（14）ガイドライン・文書作成の際の参考文書を参考にした理由（設問 2-14）

（設問 2-13）のガイドライン・文書作成の際の参考文書を参考にした理由について、自由記述で得られた主な回答内容を以下に示す。

表 2-20 ガイドライン・文書作成の際の参考文書を参考にした理由（設問 2-14）

世界動向に合わせた対応が必要と考えたため
行政からの委託業務、補助金業務を担っているため
業界における要求事項であるため
サイバー・フィジカル・セキュリティを対象としたガイドラインであるため
事業類型が似ている業界を参考としたため。
ガイドラインに何を記載すればよいか全くわからない中、世界で標準的に使われている標準・フレームワークであり、また日本でそれをもとに作成されたフレームワークであったため。
中小企業がまず何を取り組むかについて、参考になる施策が中小企業ガイドラインには記載されていたから。
世界的に認知されている要件を取り込む必要があると考えたため。
国内外のセキュリティ関連基準・情報をウォッチしているため。
IMDRF N60, N70, N73 及び法規制を導入するために必要であるため。

2.2.3 IPA「中小企業のセキュリティ対策ガイドライン」の認知および活用状況

(1)「中小企業のセキュリティ対策ガイドライン(第 3.1 版)」の認知状況(設問 3-1)

「中小企業のセキュリティ対策ガイドライン(第 3.1 版)」の認知状況は、「ガイドラインについて認知しているが、内容までは確認できていない」(35.4%)が最も多く、次いで「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」(33.3%)であり、回答者全体の 68.8%が認知していた。

表 2-21「中小企業のセキュリティ対策ガイドライン(第 3.1 版)」の認知状況(設問 3-1)

回答	件数
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	16
ガイドラインについて認知しているが、内容までは確認できていない	17
本アンケートで初めて知った	14
無回答	1
総計	48

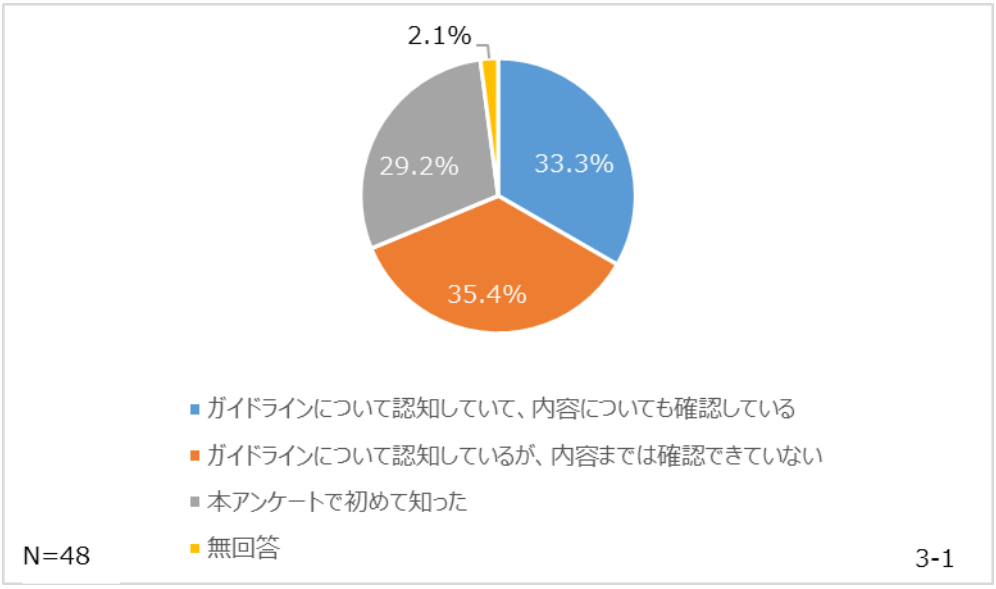

図 2-10「中小企業のセキュリティ対策ガイドライン(第 3.1 版)」の認知状況(設問 3-1)

(2)「中小企業のセキュリティ対策ガイドライン(第 3.1 版)」を認知できた経緯(設問 3-2)

「中小企業のセキュリティ対策ガイドライン(第 3.1 版)」を認知できた経緯は、「経済産業省の HP」(56.7%)が最も多く、次いで「その他」(23.3%)であった。

表 2-22「中小企業のセキュリティ対策ガイドライン(第 3.1 版)」を認知できた経緯(設問 3-2)

回答	件数
他業界団体からの案内	2
経済産業省の HP	17
セミナーでの案内	4
社内の上司・同僚等からの情報共有	0
その他	7
総計	30

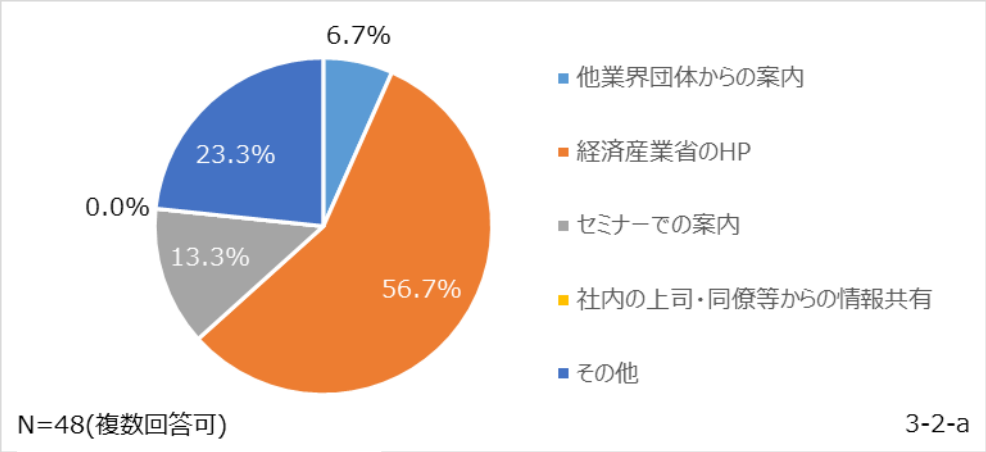

図 2-11「中小企業のセキュリティ対策ガイドライン(第 3.1 版)」を認知できた経緯(設問 3-2)

1)「その他」の詳細

(設問 3-2)で「その他」とした詳細について、自由記述で得られた主な回答内容を以下に示す。

表 2-23「中小企業のセキュリティ対策ガイドライン」を認知できた経緯「その他」の詳細

IPA からの情報共有、セキュリティニュース発行のための情報収集など
インターネット検索による情報収集
SC3 事務局からのメール
IPA の情報による
経済産業省からの周知連絡により、会員企業・団体に周知した経緯による。
SC3
「情報セキュリティ基本方針」、「情報セキュリティ関連規程」を策定するにあたり、IPA の当該ページは参照(検索して見出した)した。

(3)「中小企業のセキュリティ対策ガイドライン(第 3.1 版)」の活用状況(設問 3-3)

「中小企業のセキュリティ対策ガイドライン(第 3.1 版)」の活用状況は、実施済みと回答した活用内容は「全員への周知を行っている」(16.7%)が最も多く、一部実施(18.8%)を併せると 3 割強が周知を行っていた。次いで、「業界におけるサイバーセキュリティ施策検討の参考情報として利用している」が一部実施(20.8%)されていた。

表 2-24「中小企業のセキュリティ対策ガイドライン(第 3.1 版)」の活用状況(設問 3-3)

	未実施	一部実施	実施済み	無回答	全体
全員への周知を行っている	52.1%	18.8%	16.7%	12.5%	100.0%
ガイドライン作成の参考情報として利用している	75.0%	6.3%	2.1%	16.7%	100.0%
業界におけるサイバーセキュリティ施策検討の参考情報として利用している	64.6%	20.8%	0.0%	14.6%	100.0%

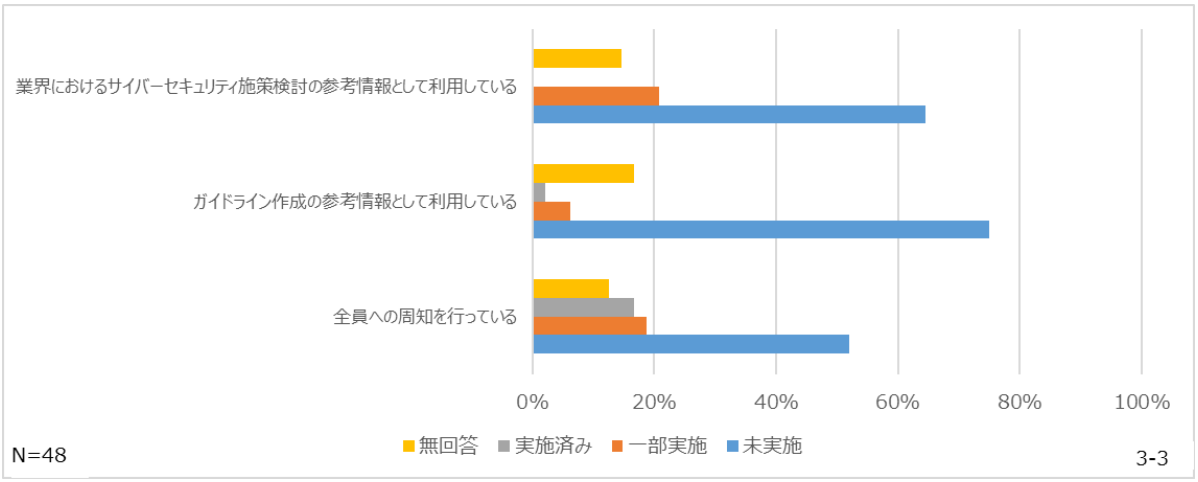

図 2-12「中小企業のセキュリティ対策ガイドライン(第 3.1 版)」の活用状況(設問 3-3)

2.2.4 業界ガイドライン作成支援および中小企業個別指導の活用意向

(1) 業界セキュリティガイドライン等や文書の作成または改訂の意向(設問 4-1)

業界セキュリティガイドライン等や文書の作成または改訂の意向は、「作成/改訂の意向無し」(52.1%)が最も多く、ついで「作成/改訂の意向あり」(27.1%)である。

表 2-25 業界セキュリティガイドライン等や文書の作成または改訂の意向(設問 4-1)

改定の意向について	件数
作成/改訂の意向あり	13
作成/改訂の意向無し	25
その他	4
無回答	6
総計	48

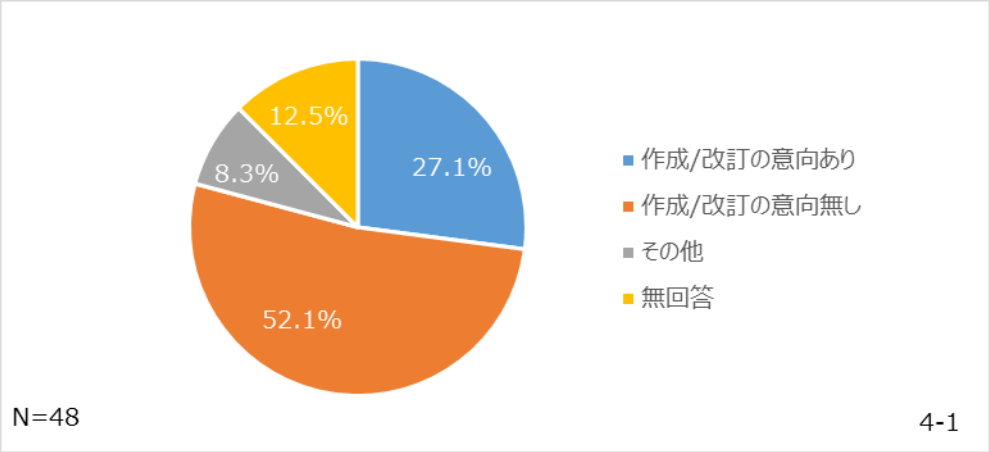

図 2-13 業界セキュリティガイドライン等や文書の作成または改訂の意向(設問 4-1)

1）「意向無し」の理由

（設問 4-1）で「作成または改訂の意向無し」とした理由について、自由記述で得られた主な回答内容を以下に示す。

表 2-26 業界セキュリティガイドライン等や文書の作成または改訂「意向無し」の理由

ごく少人数で運営しているため
会員全体の現状が把握できていないため。
個々の会社によりそこまで実施が出来ない、その事由は主に費用、並びに人材不足の問題と考えられる。
ガイドライン改定においては、日本電気協会主導で実施。改定の部会においては、IPA も委員として参加している。
参照しているガイドラインが異なるため
人材不足
加盟企業にて作成している。弊協会では作成する能力も人員もいない。
他の取組みがあるため
エンジン関連企業の業界団体であるが、企業規模によって対策がまちまちなので、基本各社の自助努力に任せている。
会員企業自身で行っていることと認識している。
特に理由はない
作成はしたいが、協力企業が無い状況
今のところないと思う。
協会内規程「情報セキュリティ対策基準」を整備済みのため。
業界業種業態が違う為
業界毎にガイドラインを作成する必要性を感じていないから。
専門的な知識がないため

2）「その他」の詳細

（設問 4-1）で「その他」とした理由について、自由記述で得られた主な回答内容を以下に示す。

表 2-27 業界セキュリティガイドライン等や文書の作成または改訂「その他」の詳細

検討中
問題認識はあるが，実行計画がない。
現状は会員企業にセキュリティ対策は任せているため。

(2) 業界団体内での業界セキュリティガイドライン等の作成/改訂可否(設問 4-2)

業界セキュリティガイドライン等の作成および改訂を業界団体内で行えるかの質問については、「外部の支援があれば自団体・協会で作成/改訂可」(33.3%)が最も多く、次いで「自団体・協会で作成/改訂可」(25.0%)であった。

表 2-28 業界団体内での業界セキュリティガイドライン等の作成/改訂可否(設問 4-2)

回答	件数
自団体・協会で作成/改訂可	12
外部の支援があれば自団体・協会で作成/改訂可	16
外部の支援があっても作成/改訂不可	10
無回答	10
総計	48

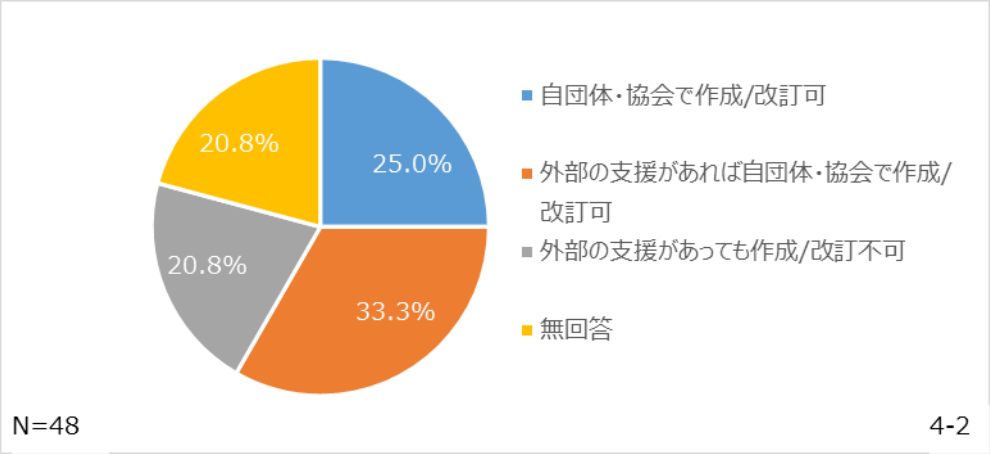

図 2-14 業界団体内での業界セキュリティガイドライン等の作成/改訂可否(設問 4-2)

(3)「中小企業の情報セキュリティガイドライン(第 3.1 版)をもとにした業界セキュリティガイドラインの策定支援」の活用意向(設問 4-3)

「中小企業の情報セキュリティガイドライン(第 3.1 版)をもとにした業界セキュリティガイドラインの策定支援」があった場合の活用意向は、「活用の意向あり」(29.2%)はであった。

表 2-29 IPA で実施予定の「中小企業の情報セキュリティガイドライン(第 3.1 版)をもとにした業界セキュリティガイドラインの策定支援」の活用意向(設問 4-3)

回答	件数
活用の意向あり	14
活用の意向無し	18
その他	10
無回答	6
総計	48

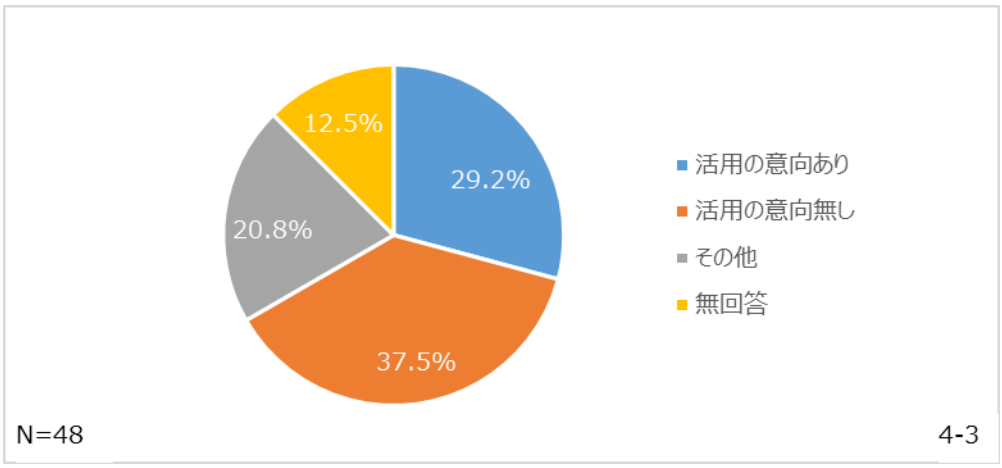

図 2-15 IPA で実施予定の「中小企業の情報セキュリティガイドライン（第 3.1 版）をもとにした業界セキュリティガイドラインの策定支援」の活用意向（設問 4-3）

1）「意向無し」の理由

（設問 4-3）で「活用の意向無し」とした理由について、自由記述で得られた主な回答内容を以下に示す。

表 2-30 業界セキュリティガイドラインの策定支援の活用意向 「意向無し」の理由

会員企業の業態が多岐に渡るため
参照しているガイドラインが異なるため
基本的に製品ならびにサービスに対する標準類を策定しているため、企業向けの標準類は策定の予定がない。
弊会で策定・改訂可能であるため。
既に策定済み。
防衛省の新情報セキュリティ基準に基づき実施しているため。
協会の各会員はおのおのガイドラインを作っている（大手）が、中小企業からは、現時点で特に協会側に支援要請がない。
会員企業自身で行っていることと認識している。
人手不足
作成はしたいが、協力企業が無い状況
人手不足
会員企業は大企業のみであるため
情報セキュリティを主眼に置いたガイドライン等の策定は、当団体の諸活動の目的とは一致していない。
業界業種業態が違う為、統一は難しい
業界毎にガイドラインを作成する必要性を感じていないから。
現時点では検討していなため

2)「その他」の詳細

(設問 4-3)で「その他」とした理由について、自由記述で得られた主な回答内容を以下に示す。

表 2-31 業界セキュリティガイドラインの策定支援の活用意向「その他」の詳細

制御系のサイバーセキュリティに関して、会員向けガイドラインの作成のための勉強会を実施中。
検討中
当該ガイドラインの評価が完了していないため
現状では不明
業界ガイドラインとしては、上部団体にならう
ガイドライン策定を検討するにあたり IPA から説明を伺いたい。
支援サービスの活用は未検討。

(4)「業界団体加盟の中小企業に対してセキュリティ専門家を派遣し、規程や体制を構築するための支援」の活用意向(設問 4-4)

「業界団体加盟の中小企業に対してセキュリティ専門家を派遣し、規程や体制を構築するための支援」があった場合の活用意向は、「活用の意向あり」(22.9%)であった。

表 2-32 IPA で実施予定の「業界団体加盟の中小企業に対してセキュリティ専門家を派遣し、規程や体制を構築するための支援」の活用意向(設問 4-4)

回答	件数
活用の意向あり	11
活用の意向無し	16
その他	15
無回答	6
総計	48

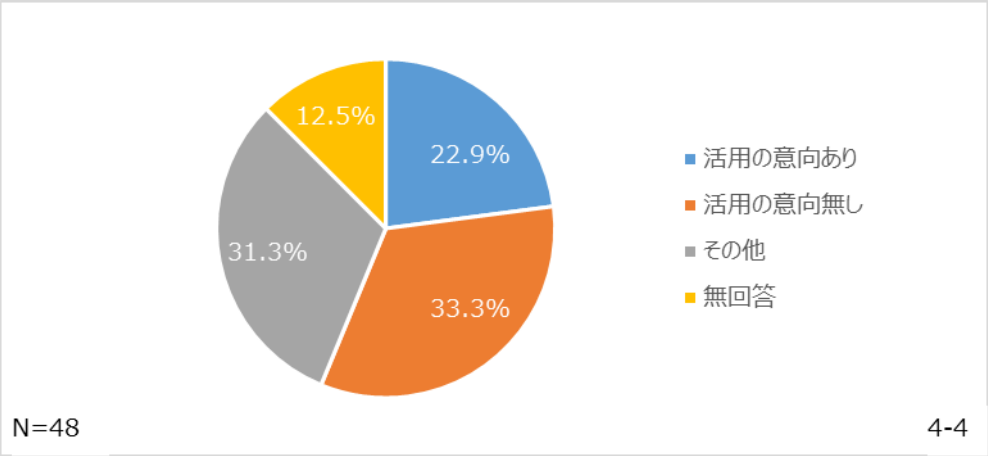

図 2-16 IPA で実施予定の「業界団体加盟の中小企業に対してセキュリティ専門家を派遣し、規程や体制を構築するための支援」の活用意向(設問 4-4)

1）「意向無し」の場合の理由

（設問 4-4）で「活用の意向無し」とした理由について、自由記述で得られた主な回答内容を以下に示す。

表 2-33 専門家を派遣し規程や体制を構築するための支援「意向無し」の場合の理由

個社が全国に散在し、事務局の人材不足もあることから、対応が困難と考えられる
参照しているガイドラインが異なるため
規定・体制については整備済みのため。
同等の支援を経済産業省で実施しているから
団体加盟会社への支援は特に必要ない。一方、ガイドラインの対象となる業界内企業への支援については、既に部工会様関係で業界としては支援いただいている認識。
会員が大企業で構成されておりすでに社内対策済のため
会員のニーズとしてまだ上がってきていない
協会の各会員はおのおのガイドラインを作っている（大手）が、中小企業からは、現時点で特に協会側に支援要請がない。
会員企業自身で判断することと認識している。
人手不足
会員企業は大企業のみであるため
現時点では考えていないため

2）「その他」の詳細

（設問 4-4）で「その他」とした理由について、自由記述で得られた主な回答内容を以下に示す。

表 2-34 専門家を派遣し規程や体制を構築するための支援「その他」の詳細

制御系のサイバーセキュリティに関して、会員向けガイドラインの作成のための勉強会を実施中。
セキュリティ対策についての関心のある会社が少ないように感じているため
加盟企業の判断による。
検討中
役員の意向を聞いてから
会員企業の中で希望があれば支援制度を紹介したい。
必要性の確認をしていないため
現状では不明
中小企業への体制構築支援を検討するにあたり IPA から説明を伺いたい。
中小企業においては、IT 担当者は不在で対応できる要員がいないため。
支援サービスの活用は未検討。
支援の必要性につき検討してから、活用するかどうか判断する。
JIPDEC 様に支援をいただいている
会員が専門家派遣による規程や体制を構築するための支援が必要か、把握していないため

(5) 業界におけるセキュリティガイドラインの普及を促進するにあたり、必要と思われる事項(設問 4-5)

回答者から自由記述で得られた主な回答内容を以下に示す。

表 2-35 業界におけるセキュリティガイドラインの普及を促進するにあたり、必要と思われる事項(設問 4-5)

国内におけるサイバーセキュリティ対策の認知度を向上することと、各国での動向や認証制度、ラベリング制度などが始まってくるため、各企業での認知度を向上させ、対策方法を普及すること。
サイバーセキュリティの演習を各企業にて実施し、サイバーセキュリティ攻撃での被害や損害などを認知してもらう。
個々の会社では、ISO27001 取得も行っているが、今後の課題として費用の捻出、人材の教育など問題がある。
最新情報のメール連絡、HP 掲載など
適切な啓発活動の実施
ガイドラインを利用する側に対して、必要性を説く教育が必要
会員企業の意識の高揚及び重要性の認識
経済産業省・IPA・自動車業界などの 1 本化の活動、経済産業省実施の技術情報管理認証制度の推進
サプライチェーンの隅々まで認知してもらうことはとても難しいので、どうやって周知できるかについてのノウハウが必要。
セミナーの実施
中小企業のセキュリティ対策ガイドライン(第 3.1 版)の骨子をまとめた簡略版があると、中小企業でも参考にできると思う。
質問の意味が不明確。中小企業へのセキュリティガイドライン普及を促進するのであれば、「業界」でやることではないと思われる。
サプライチェーンのセキュリティを確保するための必要条件として、会員企業(Tier 2、Tier 3 以下の中小企業)の意識改革、成功体験(セキュリティ対策を面倒だと思わせない)、セキュリティ対策費用の支援が必要。
商流での展開。
現状、特にない。
情報セキュリティだけがセキュリティの全てではないし、自動制御系だけが製造業のセキュリティでもない。
医療機器では、安全の視点も必要となることは理解いただきたい。そうでなければ医療機器分野では適用できない。これは、国際的な議論の場(IEC ACSEC, TC65 等)では理解されていることである。
当協会のような(公益・一般)財団法人ではなく、(公益・一般)社団法人が推進する必要がある
法律で規定すること。

2.3 アンケート調査から得られた考察

(1) 回答者の概要

本調査のアンケート回答団体は、製造業が過半数(52.1%)となっているが、SC3 加盟団体のうち、医療機器、福祉用具、印刷、音楽、石油、ガス、発電、電気、電子、発電、機械、金属、化学、情報、組込みシステム、建設、航空宇宙、自動車、化学、小売、素形材、銀行、損害保険など、幅広い業種の団体から回答を得ており、各業界団体におけるサイバーセキュリティ活動の実態、および業界セキュリティガイドラインの策定状況の現状を把握するための調査として十分な成果が得られた。

業界団体のサイバーセキュリティ活動のうち、脅威・インシデント等の情報共有に関する実施状況(設問 2-1)については、「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」は、「実施済み」と「一部実施」を合わせると回答団体のほとんど(95.8%)が実施しており、会員への脅威・インシデント等の情報提供の重要性は認識されていると見られる。一方、「会員間の情報共有」や「会員のインシデントに関する情報をもとにした注意喚起」は「実施済み」は 2 割に満たないことから、事務局からの情報提供ではなく、会員からの情報発信を促し共有する活動までには至っていない。

また、サイバーセキュリティ人材育成に関する活動状況(設問 2-5)については、教育・研修・セミナー等を「実施済み」の団体は 2 割に届かず(16.7%)、その他、「教育コンテンツ作成・演習」は「未実施」が 8 割を超えるなど、多くの業界団体において人材育成に関しては活動の対象外となっている。

業界団体における情報共有や人材育成に関しては、業界団体におけるニーズを踏まえ、業界団体への支援について検討の余地があると考えられる。

業界団体における業界セキュリティガイドラインの策定状況(設問 2-11)については、「組織」に関するガイドラインを「作成・公表済み」と回答した団体は全体の 2 割弱にとどまった。また、「工場」、「製品」、「サプライチェーン」に関するガイドラインについては「作成・公表済み」は各々1 割弱であり、ガイドラインの策定は進んでいないことがわかる。

(2) IPA 中小企業のセキュリティ対策ガイドラインの認知状況

業界団体における IPA「中小企業のセキュリティ対策ガイドライン(3.1 版)」の認知状況(設問 3-1)は、何らかの形で認知している業界団体が 6 割強(68.7%)となっており、一定程度、本ガイドラインが各業界団体に浸透していることが確認できた。

一方、活用状況(設問 3-3)については、「実施済」と「一部実施済」を合わせると 3 割強(35.5%)が会員への周知は行っており、一部においては業界のサイバーセキュリティ施策の参考情報にとして活用されていた。

(3) 業界セキュリティガイドライン策定支援および中小企業個別指導の活用意向

「業界セキュリティガイドライン等の策定支援」(設問 4-3)および「業界団体加盟の中小企業へのセキュリティ専門家派遣による規程や体制の構築支援」(設問 4-4)の活用意向については、ガイドライン

策定支援に 3 割弱（29.2%）、セキュリティ専門家派遣に 2 割強（22.9%）が「活用の意向あり」と回答しており、一定程度のニーズが見られた。

具体的には、業界ガイドライン策定支援とセキュリティ専門家派遣、いずれの支援について活用の意向ありと回答した業界団体は 8 団体であった。また、これらの業界団体の中にはすでに業界ガイドラインを作成していると回答（設問 2-11）している業界団体が 4 団体含まれており、策定した業界ガイドラインの見直しについても期待があると思われる。

また、ガイドライン策定支援についてのみ活用意向があり、セキュリティ専門家派遣は希望しないと回答した業界団体は 3 団体であり、ガイドライン適用を活用しない理由としては以下の回答であった。

- 会員が大企業で構成されておりすでに社内対策済のため
- 会員のニーズとしてまだ上がってきていない
- 個社が全国に散在し、事務局の人材不足もあることから、対応が困難と考えられる

同様に、セキュリティ専門家派遣についてのみ活用意向があり、ガイドライン策定支援は希望しないと回答した業界団体は 3 団体であり、策定支援を活用しない理由は以下の通りであった。

- 情報セキュリティを主眼に置いたガイドライン等の策定は、当団体の諸活動の目的とは一致していない。
- 基本的に製品ならびにサービスに対する標準類を策定しているため、企業向けの標準類は策定の予定がない。
- 会員企業の業態が多岐に渡るため

一方、業界ガイドライン策定支援とセキュリティ専門家派遣、いずれの支援とも「活用の意向無し」と回答した業界団体は 12 団体であり、このうち 4 団体は業界ガイドラインの策定が進んでおり支援の必要がないとの回答であったものの、その他の業界団体からは「大企業のみの団体である」「会員からの要請がない」「会員企業自身で行う」「参照しているガイドラインが異なる」などのほか、本支援を受けるにあたっても人手不足のため「意向無し」と回答している団体もあり、理由が多岐にわたることが確認できた。

以上のことから、業界団体における業界セキュリティガイドライン策定支援や、中小企業に対するガイドライン適用のためのセキュリティ専門家派遣への関心度は一定程度あることが確認できたが、業界団体ごとに状況やニーズが異なることを配慮したうえで、展開することが必要であると考えられる。

参考資料1　アンケート調査票

設問 1-1)氏名

1-1-a)　氏名

1-1-b)　氏名(フリガナ)

設問 1-2)所属

1-2-a)　団体名・協会名

1-2-b)　役職

設問 1-3)貴団体・協会の会員数をお選びください。※(正会員以外の会員も含む)

【選択肢】

1. 10 社未満
2. 10 社～50 社未満
3. 50 社～100 社未満
4. 100 社～500 社未満
5. 500 社～1,000 社未満
6. 1000 社以上

設問 1-4)貴団体・協会の会員における企業規模の割合についてお選びください。(大企業、中小企業、その他の合計が 100%になるようにお答えください。)

1-4-a)　大企業

1-4-b)　中小企業

1-4-c)　その他

設問 1-5)貴団体・協会の会員における製造業(工場を持つ企業)とサービス業の割合についてお選びください。(製造業、サービス業、その他の合計が 100%になるようにお答えください。)

1-5-a)　製造業

1-5-b)　サービス業

1-5-c)　その他

設問 1-6)貴団体・協会の会員における業種(小分類)をお選びください。

【選択肢】

1. 農業, 林業
2. 漁業
3. 鉱業, 採石業, 砂利採取業
4. 建設業
5. 製造業

6. 電気・ガス・熱供給・水道業
7. 情報通信業
8. 運輸業, 郵便業
9. 卸売業, 小売業
10. 金融業, 保険業
11. 不動産業, 物品賃貸業
12. 学術研究, 専門・技術サービス業
13. 宿泊業, 飲食サービス業
14. 生活関連サービス業, 娯楽業
15. 教育, 学習支援業
16. 医療, 福祉
17. その他
18.無回答

設問 2-1)貴団体・協会における脅威・インシデント等の情報共有に関するサイバーセキュリティ活動の実施状況についてのお選びください

2-1-a) 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
【選択肢】{1.未実施 2.一部実施 3.実施済み}

2-1-b) 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
【選択肢】{1.未実施 2.一部実施 3.実施済み}

2-1-c) 会員間の情報共有の仕組みの構築・運営
【選択肢】{1.未実施 2.一部実施 3.実施済み}

2-1-d) 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
【選択肢】{1.未実施 2.一部実施 3.実施済み}

2-1-e) その他
【選択肢】{1.未実施 2.一部実施 3.実施済み}

設問 2-2)(2-1)でご回答いただいたサイバーセキュリティ活動について、具体的な内容があればご回答ください

設問 2-3)貴団体・協会におけるサイバーセキュリティ対策事例の共有に関するサイバーセキュリティ活動の実施状況についてお選びください。

2-3-a) 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
【選択肢】{1.未実施 2.一部実施 3.実施済み}

2-3-b) 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
【選択肢】{1.未実施 2.一部実施 3.実施済み}

2-3-c) インシデント対応に関するマニュアル等の作成・提供
【選択肢】{1.未実施 2.一部実施 3.実施済み}

2-3-d) その他
【選択肢】{1.未実施 2.一部実施 3.実施済み}

設問 2-4)(2-3)でご回答いただいたサイバーセキュリティ活動について、具体的な内容があればご回答ください。

設問 2-5)貴団体・協会が実施しているサイバーセキュリティ人材育成に関するサイバーセキュリティ活動についてお選びください。

2-5-a) セキュリティに関する教育・研修、セミナー等の実施
【選択肢】{1.未実施 2.一部実施 3.実施済み}
2-5-b) サイバーセキュリティ教育コンテンツの作成・提供
【選択肢】{1.未実施 2.一部実施 3.実施済み}
2-5-c) 外部事業者のサイバーセキュリティ演習の提供
【選択肢】{1.未実施 2.一部実施 3.実施済み}
2-5-d) 業界独自のサイバーセキュリティ演習の企画・実施
【選択肢】{1.未実施 2.一部実施 3.実施済み}
2-5-e) 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
【選択肢】{1.未実施 2.一部実施 3.実施済み}
2-5-f) 国等が実施するサイバーセキュリティ演習への参加
【選択肢】{1.未実施 2.一部実施 3.実施済み}
2-5-g) その他
【選択肢】{1.未実施 2.一部実施 3.実施済み}

設問 2-6)(2-5)で回答いただいたサイバーセキュリティ活動について、具体的な内容があればご回答ください。

設問 2-7)貴団体・協会が実施している業界のセキュリティ向上に関する検討に関わる活動についてお選びください。

2-7-a) 会員が情報共有を行うための会議体の設置・運用
【選択肢】{1.未実施 2.一部実施 3.実施済み}
2-7-b) 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
【選択肢】{1.未実施 2.一部実施 3.実施済み}
2-7-c) インシデント発生時のサポート(助言、対策支援)
【選択肢】{1.未実施 2.一部実施 3.実施済み}
2-7-d) 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
【選択肢】{1.未実施 2.一部実施 3.実施済み}
2-7-e) 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
【選択肢】{1.未実施 2.一部実施 3.実施済み}
2-7-f) その他

【選択肢】｛1.未実施　2.一部実施　3.実施済み｝

設問 2-8)(2-7)で回答いただいたサイバーセキュリティ活動について、具体的な内容があればご回答ください。

設問 2-9)貴団体・協会におけるセキュリティ課題について全てお選びください。

2-9-a)【選択肢】

1. 会員企業のセキュリティの実態が把握できていない
2. 会員企業における共通のセキュリティ課題が明確にできていない
3. 業界団体にセキュリティに関する活動を推進するための知識・知見が不足している
4. 会員企業の実態を把握した上で、業界としてのガイドライン・指針等を策定するのが難しい
5. 会員企業に対して具体的なセキュリティ対策を示せていない
6. 特に無し
7. その他

設問2-10)(2-9)で回答いただいたサイバーセキュリティ活動について、具体的な内容があればご回答ください。

設問 2-11)貴団体・協会におけるサイバーセキュリティに関する業界セキュリティガイドライン等や文書の作成状況を対象範囲毎にお選びください。

2-11-a) 組織（例：企業が有する情報や、情報システムの設計・構築・運用に関するセキュリティ要件）

【選択肢】｛1.未作成　2.作成中　3.作成・公表済｝

2-11-b) 工場（例：工場やプラント等の制御システムの設計・構築・運用に関するセキュリティ要件）

【選択肢】｛1.未作成　2.作成中　3.作成・公表済｝

2-11-c) 製品（例：開発・製造する製品が備えるセキュリティ要件）

【選択肢】｛1.未作成　2.作成中　3.作成・公表済｝

2-11-d) サプライチェーン（例：部品、サービス、役務等提供を行う外部委託先に求めるセキュリティ要件）

【選択肢】｛1.未作成　2.作成中　3.作成・公表済｝

2-11-e) その他

【選択肢】｛1.未作成　2.作成中　3.作成・公表済｝

2-11-f) その他の場合の詳細

設問 2-12)(2-11)で「作成中」、「作成・公表済」とご回答いただいた方は、ガイドラインや文書の名称を

ご回答ください。（複数ある場合は、すべて記載ください）

設問 2-13)(2-12)にてご回答いただいたガイドライン・文書で参考にした文書について全てお選びください。

2-13-a)【選択肢】

1. サイバーセキュリティ経営ガイドライン
2. 中小企業の情報セキュリティ対策ガイドライン
3. サイバー・フィジカル・セキュリティ・対策フレームワーク
4. IoT セキュリティガイドライン
5. ISO/IEC27000 シリーズ
6. NIST サイバーセキュリティフレームワーク
7. NISTSP800 シリーズ
8. IEC62443 シリーズ
9. その他

2-13-b)その他の場合の詳細

設問 2-14)(2-13) にてご回答いただいた文書を参考にした理由をご回答ください。

設問 3-1)2023 年 4 月に改訂された「中小企業のセキュリティ対策ガイドライン（第 3.1 版）」の認知状況についてお選びください。

【選択肢】

1. 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
2. ガイドラインについて認知しているが、内容までは確認できていない
3. 本アンケートで初めて知った

設問 3-2)上記について、認知できた経緯について全てお選びください

3-2-a)【選択肢】

1. 他業界団体からの案内
2. 経済産業省の HP
3. セミナーでの案内
4. 社内の上司・同僚等からの情報共有
5. その他

3-2-b) その他の場合の詳細

設問 3-3)「中小企業のセキュリティ対策ガイドライン（第 3.1 版）」の活用状況についてお答えください

3-3-a) 全員への周知を行っている

【選択肢】｛1.未実施 2.一部実施 3.実施済み｝

3-3-b) ガイドライン作成の参考情報として利用している

【選択肢】｛1.未実施　2.一部実施　3.実施済み｝

3-3-c）業界におけるサイバーセキュリティ施策検討の参考情報として利用している

【選択肢】｛1.未実施　2.一部実施　3.実施済み｝

設問 4-1)貴団体・協会におけるサイバーセキュリティに関する業界セキュリティガイドライン等や文書の作成または改訂の意向についてお答えください。

4-1-a）【選択肢】｛1.作成/改訂の意向あり　2.作成/改訂の意向無し　3.その他｝

4-1-b）意向無しの場合の理由

4-1-c）その他の詳細

設問 4-2）貴団体・協会内での業界セキュリティガイドライン等の作成/改訂可否についてお答えください。

【選択肢】

1. 自団体・協会で作成可
2. 外部の支援があれば自団体・協会で作成可
3. 外部の支援があっても作成不可

設問 4-3）IPA では「中小企業の情報セキュリティガイドライン(第 3.1 版)をもとにした業界セキュリティガイドラインの策定支援を実施予定です。この支援の活用意向についてお答えください。

4-3-a）【選択肢】｛1. 活用の意向あり　2. 活用の意向無し｝

4-3-b）意向無しの場合の理由

4-3-c）その他の詳細

設問 4-4）IPA では業界団体加盟の中小企業に対してセキュリティ専門家を派遣し、規程や体制を構築するための支援を実施予定です。この支援の活用意向についてお答えください。

4-4-a）【選択肢】｛1. 活用の意向あり　2. 活用の意向無し｝

4-4-b）意向無しの場合の理由

4-4-c）その他の詳細

設問 4-5）業界におけるセキュリティガイドラインの普及を促進するにあたり、必要と思われる事項をお答えください。

参考資料 2 アンケート回答団体一覧表

No	業界団体名称	業界
1	一般社団法人日本化学工業協会	製造業
2	一般社団法人日本自動車機械器具工業会	製造業
3	日本フォーム印刷工業連合会	製造業
4	組込みシステム技術協会	製造業
5	日本ドキュメントサービス協同組合連合会	その他
6	全日本印刷工業組合連合会	その他
7	電気事業連合会	電気・ガス・熱供給・水道業
8	一般社団法人太陽光発電協会	その他
9	全日本光沢化工紙協同組合連合会	製造業
10	せんい強化セメント板協会	製造業
11	一般社団法人日本レコード協会	情報通信業
12	一般社団法人日本工業炉協会	製造業
13	鋳型ロール会	製造業
14	一般社団法人日本印刷産業連合会	その他
15	全国カレンダー出版協同組合連合会	その他
16	一般社団法人保健医療福祉情報システム工業会	-
17	日本小売業協会	卸売業, 小売業
18	一般社団法人電子情報技術産業協会	製造業
19	一般社団法人日本ガス協会	電気・ガス・熱供給・水道業
20	一般社団法人日本金属熱処理工業会	製造業
21	一般社団法人日本鉄鋼連盟	製造業
22	一般社団法人日本金型工業会	製造業
23	一般社団法人日本鋳鍛鋼会	製造業
24	一般社団法人日本自動車工業会	製造業
25	一般社団法人日本機械工業連合会	製造業
26	一般社団法人日本防衛装備工業会	製造業
27	日本筆記具工業会	製造業
28	一般社団法人日本陸用内燃機関協会	製造業
29	一般社団法人ビジネス機械・情報システム産業協会	製造業
30	一般財団法人日本自動車査定協会	卸売業, 小売業
31	一般社団法人日本中古自動車販売協会連合会	卸売業, 小売業
32	一般社団法人第二地方銀行協会	金融業, 保険業
33	一般社団法人日本電子回路工業会	その他

34	全日本フレキソ製版工業組合	製造業
35	一般社団法人日本航空宇宙工業会	-
36	一般社団法人日本医療機器ネットワーク協会	医療, 福祉
37	一般社団法人日本風力発電協会	その他
38	一般社団法人日本電機工業会	製造業
39	一般社団法人日本自動車部品工業会	製造業
40	一般社団法人日本損害保険協会	金融業, 保険業
41	石油連盟	製造業
42	一般社団法人日本福祉用具供給協会	医療, 福祉
43	一般社団法人情報通信ネットワーク産業協会	製造業
44	一般社団法人日本医療機器産業連合会	医療, 福祉
45	一般財団法人デジタルコンテンツ協会	生活関連サービス業, 娯楽業
46	一社日本ボランタリーチェーン協会	その他
47	一般社団法人日本建設機械工業会	製造業
48	公益社団法人日本訪問販売協会	卸売業, 小売業

※1 「No.」は、回答日が早い順である。

※2 「業界」は設問 1-6 回答内容である。