業界セキュリティガイドライン等の策定支援業務

実施報告書

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、中小企業においても IT 化が進み、業務の効率化やサービスレベルの向上等が図られている。その一方で、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ことも事実である。また、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で、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、サプライチェーンを構成する中小企業におけるセキュリティ対策強化についての取組みを行っている。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業界標準やチェックリスト等の情報セキュリティガイドライン（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。

1.2 目的

本業務は、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、およ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ことを目的とする。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。

2. 本業務の概要

業界セキュリティガイドライン等の策定支援業務として以下の作業を実施した。

（1） 業界セキュリティガイドライン等の策定状況調査

（2） 業界セキュリティガイドライン等の策定支援

（3） 業界団体加盟の中小企業への業界セキュリティガイドライン適用

（4） 業界セキュリティガイドラインの導入手引きの作成

（5） 実施報告書の作成

3. 業務内容

3.1 業界セキュリティガイドライン等の策定状況調査

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、その結果を取りまとめた。

3.1.1 調査概要

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 1 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）の加盟団体のうち、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

3.1.2 アンケート調査結果の概要

（1） 業界団体のサイバーセキュリティ活動

1） 脅威・インシデント等の情報共有に関する実施状況

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。

2） 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

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。

3） サイバーセキュリティ人材育成に関する実施状況

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。

4） 業界のセキュリティ向上に関する検討に関わる活動

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。

（2） 業界団体におけるセキュリティ課題

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。

（3） 業界セキュリティガイドライン等や文書の作成状況

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。

（4） 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

「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。

「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（IPA からの情報等）」（23.3%）であった。

「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。

（5） 業界セキュリティガイドライン策定支援およびセキュリティ専門家派遣の活用意向

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%）であった。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。「

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%）であった。

「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。

3.1.3 アンケート調査から得られた考察

（1） 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

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セキュリティ専門家派遣の活用意向

「業界セキュリティガイドライン等の策定支援」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」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。

3.2 業界セキュリティガイドライン等の策定支援

セキュリティガイドラインが未整備で策定を必要とする業界団体、および業界セキュリティガイドラインが策定済であっても「中小企業の情報セキュリティガイドライン（第 3.1 版）」の活用促進を希望する業界団体に対して、本業務に関する説明と策定支援に関する打診を行い、協力いただける業界団体を策定支援団体として 2 団体選定した。

3.2.1 策定支援団体の選定

3.1 業界セキュリティガイドライン等の策定状況調査結果、および関係者との調整を踏まえ、業界セキュリティガイドライン等の策定支援について、一般社団法人日本自動車部品工業会と一般社団法人日本建設業連合会に協力いただいた。いずれの団体とも、業界セキュリティガイドラインは策定済であるため、「中小企業の情報セキュリティガイドライン（第 3.1 版）」の活用促進を念頭に置いて業務を推進した。

なお、上記の団体の他にも、業界セキュリティガイドラインを策定していない複数の業界団体に対して、本業務の案内および参加意向を確認した。いずれの業界団体においても、本業務の目的や意義は理解するものの、傘下の中小企業の規模が零細であり本業務の対象に合致しない、加盟企業のセキュリティ意識が低くガイドラインを策定するには時期尚早である、事務局のリソースが不足している等の理由により、本業務への協力は叶わなかった。

3.2.2 業界セキュリティガイドライン等の策定支援方法

「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、策定支援を行う業界団体の業種特性および業界固有の情報取扱い、業界専門用語等を反映した「業界向け情報セキュリティサンプル規程」（業界団体対応版）を策定した。策定した「業界向け情報セキュリティサンプル規程」は、業界団体の推奨ガイドライン、あるいはリファレンスマニュアル、ツール＆サンプル集として、今後、業界団体加盟の中小企業のセキュリティ対策向上に活用いただくことを目途とした。

（1） 日本自動車部品工業会向け取組内容

「自工会/部工会・サイバーセキュリティ ガイドライン 2.1 版」を補完するリファレンスマニュアル、ツール＆サンプル集として、「中小企業の情報セキュリティガイドライン（第 3.1 版）」をベースに、自動車部品業界を対象とした「業界向け情報セキュリティサンプル規程」を策定した。具体的には、「自工会/部工会・サイバーセキュリティ ガイドライン 2.1 版」LV1 50 項目と、「中小企業の情報セキュリティガイドライン（第 3.1 版）」の実施項目を突合し、「自工会/部工会・サイバーセキュリティ ガイドライン 2.1 版」のみに記載されている項目については、「中小企業の情報セキュリティガイドライン（第 3.1 版）」付録 5「情報セキュリティ関連規程（サンプル）」に追記した。

なお、日本自動車部品工業会からは、「業界向け情報セキュリティサンプル規程」の策定にあたり、以下の意見をいただき、策定作業に反映した。

- 中小企業が自動車業界の規程に準拠するにあたって活用可能なドキュメントが望ましい。「自工会/部工会・サイバーセキュリティガイドライン」の各項目に対して、実践編として IPA の関連資料の内容が記載された「対策解説書」になっていると使いやすい。

（2） 日本建設業連合会向け取組内容

日本建設業連合会「協力会社における情報セキュリティガイドライン（2023 年 2 月改訂）」を補完するリファレンスマニュアル、ツール＆サンプル集として、「中小企業の情報セキュリティガイドライン（第 3.1 版）」をベースに、建設業界を対象とした「業界向け情報セキュリティサンプル規程」を策定した。具体的には、「協力会社における情報セキュリティガイドライン（2023 年 2 月改訂）」の内容と、「中小企業の情報セキュリティガイドライン（第 3.1 版）」の実施項目を突合し、「協力会社における情報セキュリティガイドライン（2023 年 2 月改訂）」のみに記載されている項目については、「中小企業の情報セキュリティガイドライン（第 3.1 版）」付録 5「情報セキュリティ関連規程（サンプル）」に追記した。

なお、日本建設業連合会からは、「業界向け情報セキュリティサンプル規程」の策定にあたり、以下の意見をいただき、策定作業に反映した。

- 多くの責任者を設置できるのは、大企業でないと難しいと思われる。体制図は簡素化してよい。
- 一般従業員へセキュリティ資格取得を推奨することはなく、セキュリティ担当者が資格を取得するように記載するとよい。

ただし、以下の意見については、今後の継続検討とした。

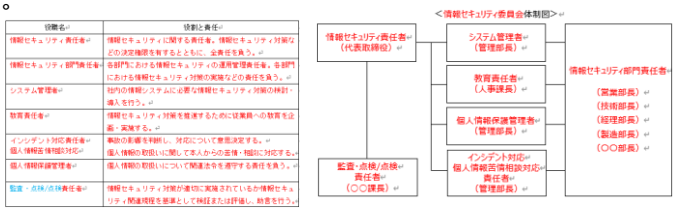
- 中小企業といっても、規模によって必要な対策が異なる。ボリュームも多いので、重要度（優先度）をつける、最低限実施すべき内容を示した版を作成するといった工夫が必要ではないか。
- 技術対策は随時更新が必要になるので、「マネジメント対策」「技術対策」は分割した方がいいのではないか。

3.2.3 業界ガイドライン等の策定支援結果

（1） 「中小企業の情報セキュリティ対策ガイドライン」の構造化

業界セキュリティガイドラインの策定には、「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」付録 5「情報セキュリティ関連規程（サンプル）」を活用した。「情報セキュリティ関連規程（サンプル）」は、「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」の記載内容を元にした、中小企業向けの情報セキュリティ関連規程のサンプルである。記載された対策から必要な対策を選択し、編集することで自社あるいは自業界の情報セキュリティ関連規程を作成することができる。ここから、業界セキュリティガイドラインを策定するにあたって、項目毎の内容を明確化し編集しやすくするために、表 2 のように構造化を行った。

表 2「情報セキュリティ関連規程（サンプル）」構造化（イメージ）

付録 5		
1.組織的対策	1.情報セキュリティのための組織	情報セキュリティ対策を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。 
1.組織的対策	2.情報セキュリティ取組みの監査・点検/点検	監査・点検/点検責任者は、情報セキュリティ関連規程の実施状況について、○月に点検を行い、監査・点検/点検結果を情報セキュリティ委員会に報告する。情報セキュリティ委員会は、報告に基づき、以下の点を考慮し、必要に応じて改善計画を立案する。 ●情報セキュリティ関連規程が有効に実施されていない場合は、その原因の特定と改善 ●情報セキュリティ関連規程に定められたルールが、対策として不十分または有効でない場合は、情報セキュリティ関連規程の改訂 ●情報セキュリティ関連規程に定められたルールが、関連法令や取引先の情報セキュリティに対する要求を満たしていない場合は、情報セキュリティ関連規程の改訂
1.組織的対策	3.情報セキュリティに関する情報共有	情報セキュリティ責任者は、新たな脅威及び脆弱性に関する警戒情報及び個人情報の保護に関する情報を専門機関等から適時に入手し、委員会で共有する。 ＜専門機関＞ ・独立行政法人情報処理推進機構（略称：IPA） ・JVN（Japan Vulnerability Notes） ・一般社団法人 JPCERT コーディネーションセンター（略称：JPCERT/CC） ・個人情報保護委員会

（2） 策定した業界向けセキュリティサンプル規程

今回協力いただいた 2 団体については、既に業界セキュリティガイドラインを有していることから、各業界団体に関係する中小企業が、「業界セキュリティガイドライン」に則ってセキュリティ対策を進めるために役立つ、リファレンスマニュアル、ツール＆サンプル集として「業界向け情報セキュリティサンプル規程」を提供することを目標とした。

最初に、各業界の業界セキュリティガイドラインと「中小企業の情報セキュリティガイドライン（第 3.1 版）」の実施項目を突合した。突合表としては、各業界団体が有する「業界セキュリティガイドライン」の記載項目を一覧化するとともに、「中小企業の情報セキュリティガイドライン（第 3.1 版）」本文の記載内容、および付録 3「5 分でできる！情報セキュリティ自社診断」・付録 4「情報セキュリティハンドブック（ひな形）」・付録 5「情報セキュリティ関連規程（サンプル）」・付録 8「中小企業のためのセキュリティインシデント対応手引き」の記載項目との対比付けを行った。

また、「中小企業の情報セキュリティガイドライン（第 3.1 版）」付録 5「情報セキュリティ関連規程（サンプル）」において、「業界セキュリティガイドライン」に記載があるものの、「情報セキュリティ関連規程（サンプル）」に記載がない項目については、「情報セキュリティ関連規程（サンプル）」に業界独自の項目として追記し、業界団体の業界に属する企業において活用しやすい形で「業界向け情報セキュリティサンプル規程」を策定した。

表 3　各業界の業界セキュリティガイドラインと「中小企業の情報セキュリティガイドライン」突合表（イメージ）

業界セキュリティガイドラインの記載項目　**「中小企業の情報セキュリティ対策ガイドライン」における記載内容**　**業界サンプル規程への反映案**

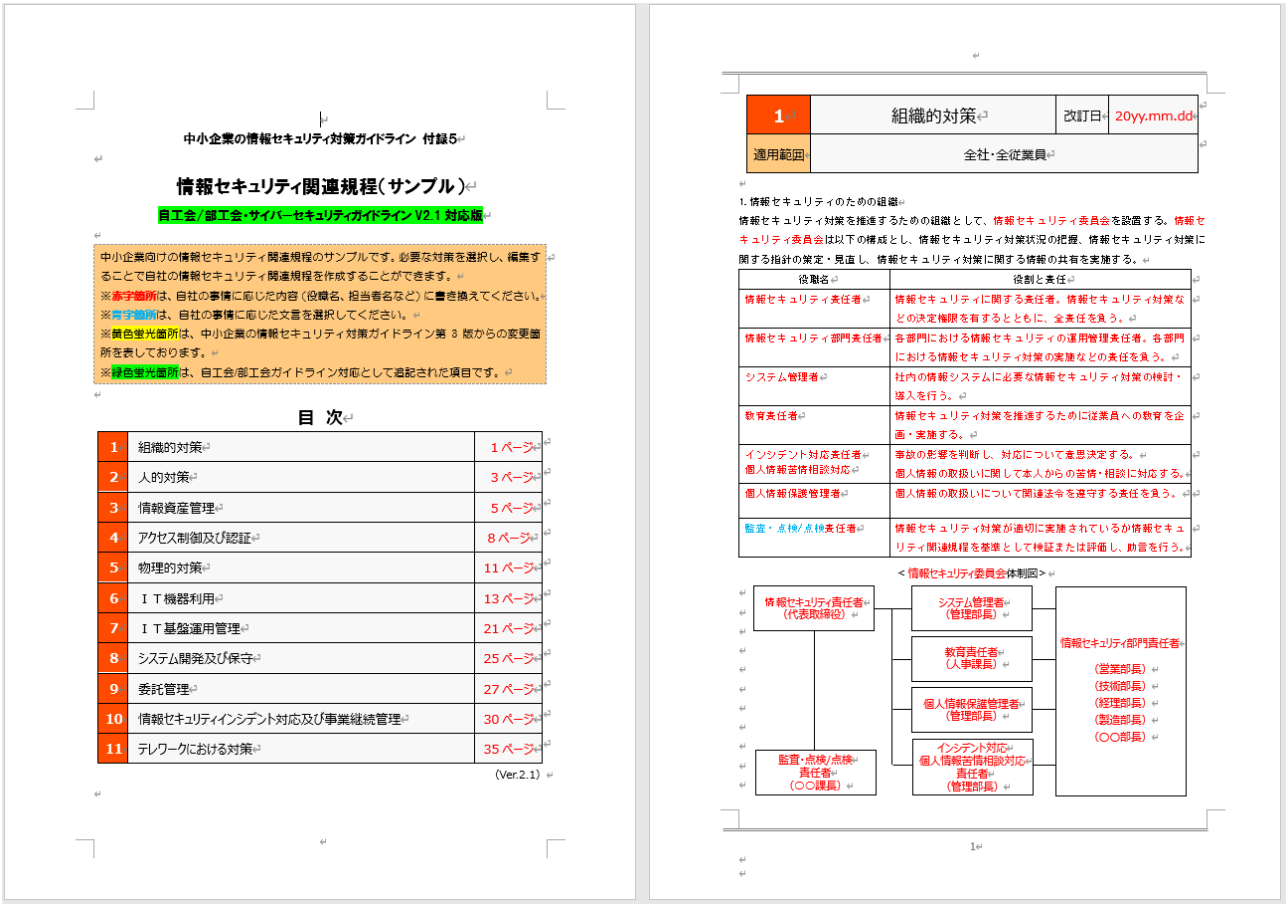
「中小企業の情報セキュリティ対策ガイドライン」業界サンプル規程（付録5）他、付録3・付録8等との対応
（左列「中小企業の情報セキュリティ対策ガイドライン」における記載内容の具体的な記載）

協力会社における情報セキュリティガイドライン			IPA「中小企業の情報セキュリティ対策ガイドライン」における記載内容	「業界版」の作成に向けた変更点(案)
1.はじめに		企業にとっての情報資産（紙媒体・電子データ等含む情報及び情報を管理する機器等）とは、面積されたノウハウであり、取引先の機密情報であり、お客様や従業員の個人情報です。情報資産は、様々な「脅威」にさらされており、脅威から守るために、「情報セキュリティ対策」が必要となります。 従来、建設業においては図面、パソコン等の紛失や、SNSへの工事写真の投稿など内部関係者の過失によって引き起こされる情報セキュリティ事故が多く、ルールの整備とその教育を通じた人的対策が有効であります。しかし、2016年以降、サイバー攻撃の脅威が高まり、2019年頃からは、企業のネットワークに侵入し機密情報を窃取したのに、パソコンやファイルサーバーのファイルを暗号化し、暗号化ファイルの復旧と窃取した情報の暴露をはめるための身代金を要求する、二重脅迫型ランサムウェアの被害が増加の一途をたどっています。そこで、今回、協力会社において、二重脅迫型ランサムウェアへの最低限の予防と対応について追記する方針のもと、ガイドラインを改訂しました。		
2.情報セキュリティ対策とは	(1)守るべき工事情報	① 図面、工程表、写真、打合せ記録 ② 発注者、近隣、工事関係者の個人情報（個人の名前が記載された書類等） ③ 建物の内部や設備の状況（写真等） ④ 工事の技術やノウハウ（標準仕様等） ⑤ 関係各社の管理情報 機密情報や個人情報（以下、重要情報という）の取扱いは工事情報の中でも特に厳しめの注意が必要です。 ■ 機密情報：機密事項と明記された文書や機密であることを前提にした情報 ■個人情報：個人を識別できる情報（氏名・性別・年齢・住所・電話番号等）	付録5 「情報セキュリティ管理規程（サンプル）」として、「1.情報資産の管理」に関連事項を記載している。	付録5 「情報セキュリティ管理規程（業界版）」として、「1.1情報資産の特定と機密性の評価」に、(1)守るべき工事情報に関する項目を記載する。
	(2)情報を守るための基本原則（システム＋ルール＋教育＝情報セキュリティ）	① 外部からの攻撃を防御する（技術的な安全措置：システム） 攻撃（ウイルス・ハッキング等）を受けて情報資産を奪い取られないように防御するシステム的な手段を講じておかなければなりません。 ② 盗難・紛失等による被害を減らす（ルール整備） 情報（機器）を社外に持ち出すことを制限・禁止して盗難・紛失のリスクを減らす必要があります。 ③ 一人一人の適切な行動（教育啓蒙） せっかくのルールも安全措置も、それを利用する従業員がルールを守らなければすべてが水の泡になります。情報漏えいの危険性を理解し、ルールを守るよう、従業員への継続した教育が必要となります。 情報セキュリティは、「鎖の理論」にたとえられます。一人でもセキュリティ意識、レベルの低い人がいると、そこから情報が漏れたりの懸念です。全員が同じレベルで、情報セキュリティを保たなければなりません。	付録3　No.25	

付録3			
対策	診断内容	説明	対策例
	#N/A	#N/A	#N/A
	#N/A	#N/A	#N/A
25. 情報セキュリティ対策をルール化する	情報セキュリティ対策（上記1～24 など）をルール化し、従業員に明示していますか？	経営者が情報セキュリティ対策に関する方針を決めていたとしても、それを具体的なルールとして明文化していなければ、従業員は都度経営者の指示を仰がなければなりません。従業員が日々ルールに従って行動できるように、「企業としてのルール」をまとめて明文化し、従業員がいつでも見られるようにしておく必要があります。	●情報セキュリティ対策として、診断シート項目のNo.1から24までをルール化して社内で共有する。 ●一度決めたルールでも問題があれば改善する。 ●テレワーク時のルールを規程にまとめ社内で共有する。

付録5					
項目	大項目	中項目	小項目		記載内容
	#N/A	#N/A	#N/A	#N/A	#N/A
3.情報資産管理/1.情報資産の管理/1.1情報資産の特定と機密性の評価	3.情報資産管理	1.情報資産の管理	1.1情報資産の特定と機密性の評価	0	当社事業に必要で価値がある情報及び個人情報（以下「情報資産」という）を特定し、「情報資産管理台帳」に記載する。情報資産の機密性は、以下の基準に従って評価する。
	#N/A	#N/A	#N/A	#N/A	#N/A

付録8					
項目	大項目	中項目	小項目	詳細項目	内容
	#N/A	#N/A	#N/A	#N/A	#N/A
	#N/A	#N/A	#N/A	#N/A	#N/A
	#N/A	#N/A	#N/A	#N/A	#N/A



中小企業の情報セキュリティ対策ガイドライン 付録5

情報セキュリティ関連規程（サンプル）

自工会/部工会・サイバーセキュリティガイドライン V2.1 対応版

中小企業向けの情報セキュリティ関連規程のサンプルです。必要な対策を選択し、編集することで自社の情報セキュリティ関連規程を作成することができます。
※赤字箇所は、自社の事情に応じた内容（役職名、担当者名など）に書き換えてください。
※青字箇所は、自社の事情に応じた文言を選択してください。
※黄色蛍光箇所は、中小企業の情報セキュリティ対策ガイドライン第 3 版からの変更箇所を表しております。
※緑色蛍光箇所は、自工会/部工会ガイドライン対応として追記された項目です。

目 次

（Ver.2.1）

1	組織的対策	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

1. 情報セキュリティのための組織

情報セキュリティ対策を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者。情報セキュリティ対策などの決定権限を有するとともに、全責任を負う。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者。各部門における情報セキュリティ対策の実施などの責任を負う。
システム管理者	社内の情報システムに必要な情報セキュリティ対策の検討・導入を行う。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施する。
インシデント対応責任者 個人情報苦情相談対応	事故の影響を判断し、対応について意思決定する。 個人情報の取扱いに関して本人からの苦情・相談に対応する。
個人情報保護管理者	個人情報の取扱いについて関連法令を遵守する責任を負う。
監査・点検/点検責任者	情報セキュリティ対策が適切に実施されているか情報セキュリティ関連規程を基準として検証または評価し、助言を行う。

＜情報セキュリティ委員会体制図＞

1

図 1 業界向け情報セキュリティサンプル規程（イメージ）

3.2.4 考察

本業務では、一般社団法人日本自動車部品工業会および一般社団法人日本建設業連合会の 2 団体に協力いただき、業界セキュリティガイドラインの策定支援を実施した。いずれの団体とも業界セキュリティガイドラインは策定済であるため、業界セキュリティガイドラインの項目と「中小企業の情報セキュリティ対策ガイドライン」本文の該当箇所や活用可能な付録との対応を示した突合表を策定し、セキュリティ対策を進める際に、項目毎に「中小企業の情報セキュリティ対策ガイドライン」本文や付録を参照することを可能とした。また、「情報セキュリティ関連規程（サンプル）」に対して、その業界のセキュリティガイドラインの要素を反映した「業界向け情報セキュリティサンプル規程」を策定した。

これらの支援に関しては、各業界団体の意見を伺いながら実施したが、今後の業界セキュリティガイドラインの普及に関しても、各業界団体の状況を踏まえ、連携した取組みを実施することが望ましい。

なお、業界セキュリティガイドラインを策定していない業界団体については、傘下の中小企業の規模が小さい、セキュリティ意識がまだ低い、業界団体の事務局リソースが不足している等の理由により、本業務の支援には至らなかった。このことから、業界セキュリティガイドラインの策定支援にあたっては、業界団体の固有の状況や業界に属する中小企業の規模・意識等の状況を踏まえながら進めることが望ましい。

3.3 業界団体加盟の中小企業への業界セキュリティガイドライン適用

策定した業界セキュリティガイドライン（業界向け情報セキュリティサンプル規程）を当該業界団体の業界に属する中小企業に適用いただくため、セキュリティ専門家によるマネジメント指導（個社の情報セキュリティ関連規程の整備、情報資産の洗い出しとリスク分析、セキュリティ対策導入計画策定の支援等）を支援対象企業 1 社当たり 4 回実施した。支援対象の中小企業は、当該業界団体より推薦、または了解を得た上で、候補企業への支援内容説明と打診を行い、6 社を選定した。

3.3.1 支援対象企業の選定

「業界セキュリティガイドライン」を有する業界団体傘下の企業、または「業界セキュリティガイドライン」が適用される業界に属する企業に対して、業界団体あるいは IPA より企業募集案内を行い、本業務に関心を持つ企業 6 社を選定した。

3.3.2 業界セキュリティガイドラインの適用方法

マネジメント指導業務の達成目標は以下のように定めた。

【達成目標１】情報セキュリティ基本方針の作成

【達成目標２】現状における自社の情報セキュリティリスクの洗い出し

【達成目標３】情報セキュリティ対策実行計画の策定

【達成目標４】自走化に向けた情報資産棚卸し/リスク分析および必要なセキュリティ対策の実装（継続対応）

また、成果物については以下を定めた。

- 今後、各社で取り組む情報セキュリティ対策の進め方をまとめた実行計画書
- 「業界向け情報セキュリティサンプル規程」を基に策定した個社の規程（案）

企業において実施する事項は以下の通りである。費用については無料とした。

- 専門家の指導への対応（訪問またはオンライン会議） 【１回 2~３時間 × 4~5 回】
- 企業側の検討体制の調整 【数時間】
- IPA「5 分でできる情報セキュリティ自社診断」の実施、対策状況が確認できる規程等の準備・更新/作成、対策計画書の作成 【専門家の指導に対する準備時間 １回数時間 × 4～5 回】

※ 所要工数は企業様の状況によって異なる。

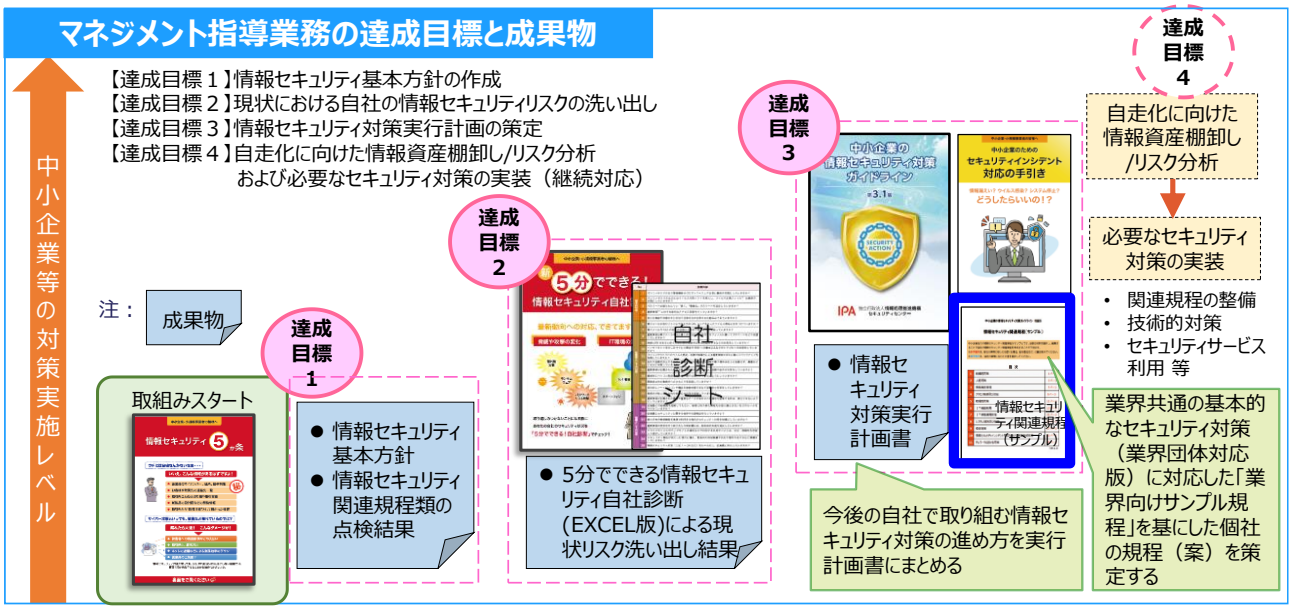


図 2 マネジメント指導業務の達成目標と成果物

実施項目	11月	12月	1月	2月
参加企業募集・決定	企業募集・決定			
専門家とのマッチング		専門家とのマッチング		
指導日程調整		日程調整		
専門家の指導			準備 ★ 指導① 準備 ★ 指導②	準備 ★ 指導③ 準備 ★ 指導④

図 3 マネジメント指導業務の実施スケジュール

1～2週間 **事前準備＃1**
*指導先企業の情報収集とヒアリングシートの作成
*IPA自社診断(EXCEL版)の実施依頼

第１回
<u>企業の事業や情報システム環境の理解と情報セキュリティリスクの洗い出し</u>
指導先企業の事業内容と情報システム環境を把握し、自社診断の結果をもとに、経営者が認識しているセキュリティ課題（リスク）と当事業への期待値を確認します。

1～2週間 **事前準備＃２**
*前回の指導を通じて得た情報をもとにした改善領域の見極め
*現行の基本方針や規程類の有無確認の依頼

第２回
<u>情報セキュリティ基本方針や関連規程整備の検討と重点改善領域の絞り込み</u>
基本方針の作成と、必要な関連規程類の検討を行うと共に、自社診断結果をもとに重点改善領域について、ディスカッションと対策の絞り込みを行います。

1～2週間 **事前準備＃３**
*前回結果に加え、経営施策に対する情報セキュリティリスクの検討

第３回
<u>情報セキュリティ対策の重点対策の検討と優先順位付け</u>
経営施策に対する情報セキュリティ面での対策状況を確認し、必要なアドバイスを行うと共に、重点対策と合わせた今後の実行計画を検討します。

1～2週間 **事前準備＃４**
*優先順位と実現性を考慮した実行計画案の作成

第４回
<u>情報セキュリティ対策の成果物レビューと訪問指導全体のまとめ</u>
専門家がまとめた業界セキュリティガイドライン適合のための実行計画案（一年間程度）についてディスカッションし、合意形成を図ります。また企業側で作成した基本方針や規程の見直し案について、マネジメントシステムの実効性の視点からレビューを行います。

計1.5ヶ月程度

図 4 「標準的な進め方」の全体構成

なお、支援対象企業へのマネジメント指導を実施する際には、「令和 2 年度中小企業の情報セキュリティマネジメント指導業務 」における指導要領（指導ツール）を参照し、「中小企業の情報セキュリティガイドライン(第 3.1 版)」の改訂箇所を反映した上で、指導要領（指導ツール）を更新して実施した。

この指導要領（指導ツール）は、セキュリティの専門家による指導の下、今後も継続して活用できるものとなるよう、標準カリキュラムを示しつつ、指導先企業の個別事情に応じた指導に必要なツールの活用方法、経験者の体験による気付きや工夫など実践的なノウハウを提供する内容とした。また、名称も「実施要領」とした。

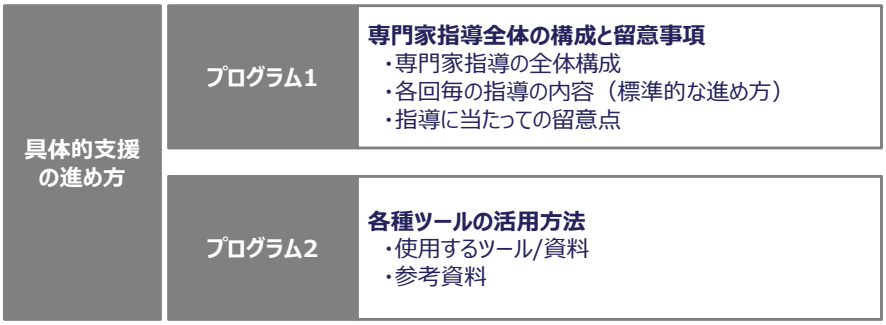


図 5 実施要領の内容

指導ツールとしては、以下の 3 点を更新し、マネジメント指導業務に活用した。

- 【様式 1】ヒアリングシート
- 【様式 2】関連規程類の点検結果シート
- 【様式 3】業界ガイドライン適合のための対策実行計画書

	ヒアリング項目	ヒアリング結果(今回の指導で考慮すべき点)
1	訪問先企業の事業内容(業態、製品/サービス、拠点/組織/従業員構成)	
2	業務プロセス(業務の全体像の見える化)とシステム化の状況	
3	顧客/取引先/仕入れ先などのサプライチェーン(事業関係者)	
4	経営施策と対応のための情報システム対策	
	*リモートワーク(テレワーク)の実施状況	
5	IT環境と活用状況(特徴的なことの訊き出し)	
	*自社の情報システム構成(事業系システムと社内(管理系)システム)	
	*社内外の情報/コミュニケーションシステムの状況(HP、メール、チャット等)	
	*外部のITサービス(クラウド,SNS)や取引先とのネットワーク接続の状況	
	*主要な情報システムで取り扱っているデータ(種類、量)	
	*IT関連組織体制(開発・保守、運用、ユーザーサポート、障害・事故対応)	
	*IT予算(内、情報セキュリティ関連予算)	
	*従業員のITスキル、リテラシー、情報管理・保護への意識	
	*重要な情報資産(個人情報、営業/特許等)の種類と量	
	*上記の重要情報資産の保管・管理状況(アクセス管理、バックアップ等)	
6	IT活用に関する課題認識と対応	
	*付加価値向上の面から(販路拡大、新規取引先獲得)	
	*使用システムの陳腐化、保守サポート切れ、新技術活用の遅れ	
	*既に計画中/実施中の対策(導入予定の情報システムも含め)	
7	情報セキュリティに関する状況	
	*過去に発生した事故(情報漏えい、詐欺などの被害)と実施した対策	
	*情報セキュリティ事故発生時の対応体制(連絡網、初動・緊急対応)	
	*特に気になっているリスクや、業界・取引先等からの要請(ガバナンス)	
	*計画・実施中の情報セキュリティ対策(研修・訓練、保険加入など)	
	*情報セキュリティインシデントに関する情報の入手先と対策の相談相手	

図 6 【様式 1】ヒアリングシート

	関連規程 / ガイド類	概要	※今回の見直し (プルダウンメニューで選択)
1	組織的対策	情報セキュリティ管理体制の構築や点検、情報共有などのルールを定めます。	
2	人的対策	取締役及び従業員の責務や教育、人材育成などのルールを定めます。	
3	情報資産管理	情報資産の管理や持ち出し方法、バックアップ、廃棄などのルールを定めます。	
4	アクセス制御及び認証	情報資産に対するアクセス制御方針や認証のルールを定めます。	
5	物理的対策	セキュリティ領域の設定や領域内での注意事項などのルールを定めます。	
6	ＩＴ機器利用	ＩＴ機器やソフトウェアの利用などのルールを定めます。	
7	ＩＴ基盤運用管理	サーバーやネットワーク等のＩＴインフラに関するルールを定めます。	
8	システム開発及び保守	独自に開発及び保守を行う情報システムに関するルールを定めます。	
9	委託管理	業務委託にあたっての選定や契約、評価のルールを定めます。業務委託契約書の機密保持に関する条項例と委託先チェックリストのサンプルが付属します。	
10	情報セキュリティインシデント対応及び事業継続管理	情報セキュリティに関する事故対応や事業継続管理などのルールを定めます。	
11	テレワークにおける対策	テレワークにおけるＩＴ機器利用やＩＴ基盤運用管理、勤務に関するルールを定めます。	

図 7 【様式 2】関連規程類の点検結果シート

改善分野	現状と課題	具体的改善対策	絞り込み			実施可否	実施期限	予算、要員等の懸念点
			緊急度	重要度	難易度			
組織的対策								
人的対策								
技術的対策								
物理的対策								

図 8 【様式 3】業界ガイドライン適合のための対策実行計画書

3.3.3 業界ガイドラインの適用結果

（1） マネジメント指導業務の実施概要

マネジメント指導業務の実施概要を以下に示す。

自動車産業４社、建設業２社の合計６社に対して、各４回の専門家の派遣を行い、マネジメント指導業務を実施した。

表 4 マネジメント指導業務概要

指導企業	自動車 A社	自動車 B社	自動車 C社	自動車 D社	建設 E社	建設 F社
1回目	1/9(火) 13:30-16:30	1/18(木) 13:30-16:30	1/15(月) 13:30-16:30	1/11(木) 13:30-16:30	1/11(木) 9:00-11:15	1/9(火) 15:00-17:00
2回目	1/23(火) 9:00-12:00※	1/26(金) 13:30-16:30※	1/29(月) 13:30-16:30	1/23(火) 13:30-16:30	1/18(木) 9:00-11:20	1/24(火) 14:00-16:20
3回目	1/31(水) 9:00-12:00※	2/5(月) 13:30-16:30※	2/5(月) 13:30-16:30	1/31(水) 13:30-16:30	1/25(木) 9:00-11:30	2/8(木) 10:00-12:00
4回目	2/9(金) 13:30-16:10	2/14(水) 13:30-15:30※	2/13(火) 13:30-16:00	2/6(火) 13:30-16:30	2/1(木) 9:00-11:40	2/15(木) 10:00-11:55

※ オンラインにて実施

（2） マネジメント指導業務の結果

1） 自動車部品業界

自動車部品業界の企業における業界セキュリティガイドライン適用結果は以下の通りである。

- 規程が未整備の企業の場合、業界向け情報セキュリティサンプル規程はそのまま活用可能であった。サンプル規程を参照して、自社の規程の見直しを行うことも有効であった。
- マネジメント指導業務は、対策の必要性の理解、自工会/部工会ガイドラインの内容理解、対策の優先順位付けや実行可能な対策の助言、リスク分析の支援に関して、効果的であった。

活用のヒントとしては以下の点が挙げられる。

- 製造業においては、既に ISO9001・14001 を取得している企業も多い。セキュリティ対策の推進にあたって、このような ISO に基づいた整備済の文書を活用することや、ISO 担当者をセキュリティ対策推進体制に加え、ISO の取組に関する知見を取り込むことも有効である。
- 複数の工場が存在する場合、1 つの工場で他工場の担当者も参加して業界向け情報セキュリティサンプル規程を用いた規程策定・適用を行った後、参加者が実施方法を自分の工場に持ち帰り、横展開することが有効である。
- 販売会社からセキュリティ対策に関する情報を入手し、アドバイスを得ることが有益である。ただし、複数の販売会社から様々な情報を得ることは重要であるが、実際の機器・サービスの導入時には、機能の重複がないよう注意する必要がある。

2） 建設業界

建設業界の企業における業界セキュリティガイドライン適用結果は以下の通りである。

- 自社の課題である対策を中心に業界向け情報セキュリティサンプル規程を参照して見直しする等、企業の状況に応じて活用することが効果的であった。
- マネジメント指導業務は、資産管理台帳の作成やリスクアセスメントは中小企業にとって難しく、セキュリティ専門家の支援により、情報資産の重要度設定や管理方法の策定に取り組めた事例が見られた。

活用のヒントとしては以下の点が挙げられる。

- マネジメント指導業務を、上司の巻き込みや経営を含めた体制構築等、組織的な対策を推進するきっかけとすることも有効である。専門家の助言により、担当者の上司も含めセキュリティの重要性に気づくことができ、対策推進の意欲を高めることもできる。
- 従業員への教育は、社外の専門家がわかりやすく説明することで、効果的に実施することができる。
- 情報管理のために、オフィスレイアウトの変更や施錠管理等、すぐにできるところから実施することも効果的である。
- 従業員の意識向上が課題であったが、組織のセキュリティ体制構築、基本方針策定、関連規程策定、周知の順で段階的に対策を推進する計画を立てることで、無理なく進めることができる。

（3） マネジメント指導業務の個社毎の結果

マネジメント指導業務の個社毎の実施概要を以下に示す。

表 5 A 社の業界ガイドライン適用結果

企業		A 社
所在地		三重県伊賀市
業種		軸受部品製造
現状		・生産管理システムが主。 ・重要な情報資産は、加工請負の図面、加工標準書（図面から加工データに落とし込み）、NC 加工データ、受注・出荷データ。クラウド上にバックアップ、紙の図面（正）はキャビネットに保管。 ・自工会/部工会サイバーセキュリティガイドライン LV1 の 2024 年度中の実施が課題。
業界向け情報セキュリティサンプル規程の適用評価		・規程は新規に作成予定。 ・2024 年度中に自工会/部工会ガイドライン LV1 を満たす為、情報セキュリティ関連規程（サンプル）を参考にし、自社の現状を踏まえて作成する。
実行計画	組織的対策	・情報セキュリティ関連規定の組織的対策、情報セキュリティインシデント対応ならびに事業継続管理で明確化する。 ・情報セキュリティ関連規定の情報資産管理で、資産管理台帳の記載運用を規定する。
	人的対策	・情報セキュリティ関連規定の人的対策で、情報セキュリティに関する定期的な教育計画の立案を規定する。
	技術的対策	・サーバのセキュリティ対策ツールのログ取得機能を有効化し、ログ情報が取得できるようにする。
	物理的対策	・情報セキュリティ関連規程の物理的対策で、情報資産の重要度に応じて社内の領域を区分する。フロアレイアウトを作成し、入退出制限エリアの見直しを行う。
派遣による企業の成果		・指導前は、情報セキュリティマネジメント全般についてほとんど理解されていなかったが、指導後は考え方、運用手法等を理解いただけた。
業界ガイドラインへの反映や考慮が必要な点		・情報端末の設定、トラブル時の対応、IT 基盤等の情報インフラの運用管理を外部業者へ委託しているので、できるだけ内部で対応できる要員の配置を推奨した。
その他、派遣業務で気づいた点 等		・今回は、スケジュールにあまり余裕がない状態で進めざるを得なかった。

表 6 B 社の業界ガイドライン適用結果

企業		B 社
所在地		愛知県名古屋市
業種		メッキ加工
現状		・製造工程の良品、不良数、製造フローの管理を実施。 ・外部 IT サービスとして、office365、取引先との受発注システム（一部あり）を利用。 ・重要な情報資産は、従業員の個人情報、営業機密情報等。 ・自工会からのセキュリティ要請への対応、およびクラウドサービスの増加によるパスワード管理が課題。
業界向け情報セキュリティサンプル規程の適用評価		・既存の規程を見直し改訂予定。 ・自工会ガイドライン Lv2 に相当するよう、情報セキュリティ関連規程（サンプル）を参考にし、既存の関連規定と比較、検討して作成する。
実行計画	組織的対策	・拠点ごとに担当者を新しく任命し組織体制を情報セキュリティ関連規程の組織的対策、情報セキュリティインシデント対応ならびに事業継続管理で明確化する。 ・情報セキュリティ関連規程の情報資産管理で、資産管理台帳の記載運用を規定する。
	人的対策	・教育資料を作成し、情報セキュリティ関連規程の人的対策で、情報セキュリティに関する定期的な教育計画の立案を規定する
	技術的対策	・オンプレ、クラウドで SSO が可能な方式を導入する。 ・メールで添付ファイルを送らず、別にダウンロードする仕組みを導入する。
	物理的対策	・情報セキュリティ関連規定の物理的対策で、情報資産の重要度に応じて社内の領域を区分する。フロアレイアウトを作成し、入退出制限エリアの見直しを行う。
派遣による企業の成果		・情報セキュリティの技術的な面は情報システム部を中心に進めているが、経営層を含めた組織的対応など管理的な面は構築段階であるため、今回の派遣の内容はその面で有益になる部分が多かった。
業界ガイドラインへの反映や考慮が必要な点		・最終的には、自工会/部工会サイバーセキュリティガイドライン LV2 に対応方針だが、まだ管理的、技術的の両面での課題が多い。とりあえず LV1 に対応できることを目標に進めていく方針である。 ・自工会/部工会サイバーセキュリティガイドライン対応の規程類作成の LV1 において業界向け情報セキュリティサンプル規程は概ね活用できる。今後 LV 2 に対応していく方針であるため、LV2 への業界向け情報セキュリティサンプル規程の活用度は検証できていない。 ・ガイドラインと業界向け情報セキュリティサンプル規程の文書構造が違うため、サンプル規程の文書中にコメントの形でガイドラインの対応部分のラベルや項目 No を表記した方が専門家としては使いやすい。
その他、派遣業務で気づいた点 等		・今回は、スケジュールにあまり余裕がない状態で進めざるを得なかった。

表 7 C 社の業界ガイドライン適用結果

企業		C 社
所在地		岐阜県関市
業種		プレス加工
現状		・ISO9001、14000 取得済、業務フロー作成済。情報セキュリティに関してルール化されておらず、現場の遵守はあいまい。 ・システム構成図、NW 構成図、社内使用の機器一覧あり。本社 NW に UTM 設置、監視サービスあり、拠点間は VPN 接続。MS Azure 利用、リモートアクセス、業務データはクラウド保存、MS365 利用。 ・重要な情報資産は、個人情報、図面情報、金型の技術情報。 ・主要顧客からのセキュリティ対策要求や、自工会/部工会ガイドラインへの準拠が求められている。
業界向け情報セキュリティサンプル規程の適用評価		・規程については新規に策定。 - 全般的にルールを文書化し、実施状況を点検する - ISO9000 に準じて教育の計画立案、実施手順を作成する - バックアップが行われていることを確認する手順を明文化する - 書類に秘密区分を表示する。重要文書は施錠管理する - アクセス権管理は ActiveDirectory で行うことを検討するよう提案 - 警備会社による警備を総務事務所以外に拡張した方がよい - 効率的な管理のために IT 資産管理ソフトの導入を検討するよう提案 - サーバ・ネットワーク構成図を作成する - 業者への開発依頼、受入検収、保守のルールを明文化する - 最新の動向を業務委託ルール、秘密保持契約に反映する。委託元責任、選定評価、再委託 - インシデントの種類ごとに対応手順を決める
実行計画	組織的対策	・情報セキュリティ管理規程のブラッシュアップ、自工会ガイドラインへの適合、運用可能な内容にする。 ・委託先評価基準を決める。委託契約書または秘密保持契約に情報セキュリティ要件を加え、委託先と更新する。
	人的対策	・情報セキュリティ教育を実施。管理規程の内容を理解。日常行う情報セキュリティ作業を理解。
	技術的対策	・情報資産の機密性区分を定義する。重要な情報資産を特定し、情報資産管理台帳を整備する。 ・アクセス権一覧の作成、アクセス権の付与、維持、削除の手順の策定、設定・変更内容を記録に残す。 ・サーバ、ネットワークの要件定義書、設計書を整備する。PC 資産を一覧にする。OS、ウィルス対策ソフトの更新状況を部門ごとに確認する運用方法を整備する
	物理的対策	・セキュリティ区域を定め、レベルごとの対策を決める。
派遣による企業の成果		・情報セキュリティ管理規程を既に作成中であったが、セキュリティ要件の解釈や社内の調整等で完成が遅れていた。本業務によりセキュリティの理解は深まり、完成にむけて弾みがついた。
業界ガイドラインへの反映や考慮が必要な点		・No.44（他社との間の機密情報の取り扱い方法明確化）、46（情報セキュリティ事件・事故時の他社との役割と責任明確化）に関して、顧客との責任を明確にすることは力関係からみて難しい。 ・No.66（情報資産における「機密性」「完全性」「可用性」の 3 要素が確保できなくなった場合のリスク特定）に関して、IT またはセキュリティ専任者がいない企業にとっては最初から取り組むのは難しい。正しくリスク評価するためには教育を受ける必要がある。
その他、派遣業務で気づいた点 等		・今回は自工会ガイドラインに基づく支援であるが、METI または IPA 標準の技術情報管理で行うプロセスとの連携がうまくできなかった。自工会ガイドライン主体で支援を進めることが多かった。

表 8 D 社の業界ガイドライン適用結果

企業		D 社
所在地		愛知県犬山市
業種		金属切削加工
現状		・ISO9001:2003 取得済、業務フロー等を文書化済。 ・システムの利用は、主要顧客との受注データ授受が主。サーバはあるが工作機械とは接続していない。図面を印刷し現場で使用。クラウドサーバの契約あり、活用はしていない。 ・重要な情報資産は、客先の図面情報、客先とのメール、社員名簿、製品情報、生産技術。 ・自工会/部工会ガイドラインへの適合状況がわからないことが課題。
業界向け情報セキュリティサンプル規程の適用評価		・規程については新規に作成。 - 情報セキュリティ管理委員会を組織化する。情報セキュリティ規程、運用手順を文書化する。 - 経営層および従業員の責任と職務を文書化する。定期的な教育・研修の実施→ISO9000 に追記または流用。 - 情報資産の入手・保管・廃棄および持出しの方法を文書化する。バックアップ、廃棄ルールを文書化する→ISO9000。 - 情報資産の重要性を判断し、情報資産一覧表を作成する。電子データに対しアクセス権の設定方法を文書化する。文書、電子データに秘密区分を表示する。 - サーバを部外者から見えないようにする。重要な情報を保管するキャビネットを施錠する。 - PC、情報システムのログインパスワードの設定ルール設定、IT 機器の社外持出し・私有機器の持込みルール文書化、利用ソフトウェアの一覧作成、ソフトウェアの利用ルール文書化を行う。 - 最新のネットワーク構成図を作成する。 - 業者への開発依頼、受入検収、保守のルールを文書化する。 - 既存の外注先への業務委託契約について、最近の動向を踏まえた内容に更新する。外注先の選定、契約、評価のルール→ISO9000 に追記または流用。 - 緊急連絡体制を明確にする→ISO9000 に同じ。想定するインシデントごとに対応手順を文書化。 - テレワークを行う場合は、ルールを決める。
実行計画	組織的対策	・情報セキュリティ委員会を整備する。任命された人は役割と責任を理解する。情報セキュリティ管理規程を整備する。情報セキュリティインシデント対応手順を整備する。 ・委託先評価基準を決める。委託契約書または秘密保持契約に現在の情報セキュリティ要件を加える。
	人的対策	・従業員に対する教育実施。情報セキュリティ管理規程の理解。
	技術的対策	・情報資産管理台帳の作成、重要な情報資産の特定・評価、秘密区分の表示を行う。 ・アクセス権管理ルールを整備する。アクセス権限一覧を作成する。パスワードの設定ルールを決める。 ・標準利用ソフトウェアを一覧にする。実施状況を見える化する。Windows アップデート、ウィルス対策ソフトのアップデート、ウィルス対策ソフト定義ファイルの更新、クリアスクリーンを実施する。 ・利用ソフトウェアの一覧化、セキュリティ要件の明確化、サーバ・ネットワーク機器の設定を文書化する。
	物理的対策	・セキュリティ領域を設定し、レベルごとに対策する。レベル 3 領域に関して、サーバの設置場所を改善する。重要書類は、鍵付きキャビネットに保管し、鍵管理する。
派遣による企業の成果		・情報セキュリティ管理規程および自工会/部工会ガイドラインの理解が深まり、実施事項が明確になった。
業界ガイドラインへの反映や考慮が必要な点		・小規模企業のため、サーバの設置場所については、鍵付きラックの導入も難しい。今回は、部外者から見えないよう衝立等で囲うよう依頼した。 ・委託先が零細企業の場合もあり、ガイドラインにあるような委託先管理は困難という懸念がある。
その他、派遣業務で気づいた点 等		–

表 9 E 社の業界ガイドライン適用結果

企業		E 社
所在地		千葉県佐倉市
業種		土木工事
現状		・業務プロセスを図字化したものは無し。積算システムを運用。 ・重要な情報資産は特定していない。担当者が、保管しておいた方が良いと判断したものを社長に確認し、鍵の掛かる所に保管。 ・担当者が委託先と図面データのやり取りはあるが、取扱いに関するルールは無い。
業界向け情報セキュリティサンプル規程の適用評価		・規程は新規に作成予定。 ・業界向け情報セキュリティサンプル規程をそのまま利用することを想定。
実行計画	組織的対策	・対応手順を作成し、従業員に周知する。 ・情報セキュリティ管理規程の作成。
	人的対策	・セキュリティ専門機関等のウェブサイトなどで最新の脅威や攻撃の手口を知り共有する。 ・不審の定義づけを行い、通常やり取りしている人以外や公共機関をかたったメール等についても確認が徹底されるようにする。 ・社員教育については、いつ、どのような内容について教育を行うかをルール化し、教育を行ったら、その記録を残すようにする。
	技術的対策	・パスワードは、「長く」「複雑な」パスワードを使用するようにする。文字数の制限、大文字小文字、数字、記号を入れるルールにする。 ・重要度を三段階に分け保存方法、保存期間、廃棄方法についての規定を設ける。 ・継続的にやりとりする相手であればクラウド上でやりとりする方法への変更を検討する。
	物理的対策	・メールは、同じ名前の人には、別名をつける。FAX は宛先登録、メールはアドレス帳に登録することで送信ミスを防止する。 ・重要度を三段階に分け保存方法、保存期間、廃棄方法についての規定を設ける。データについてはバックアップの規定を設ける。 ・重要度を三段階に分け保存方法、保存期間、廃棄方法についての規定を設ける。 ・事務所のレイアウトを変更し、来客が社員エリアに入れないようにする。来客の対応場所を決める。 ・施錠記録は、セコムから定期的にもらって、保管しておく。PC の施錠方法を検討する。 ・書類や媒体それぞれに破棄の手順、方法を明確にする。 ・利用時のルールを定め、共有する。
派遣による企業の成果		・セキュリティアクション 1，2 の実施 ・セキュリティ基本方針の策定 ・セキュリティ自己診断で自社の弱みが明確になった ・対策項目一覧表の作成と実行計画の作成 → セキュリティに対する認識が変わり、重要性に気づけたことが成果である。
業界ガイドラインへの反映や考慮が必要な点		・情報セキュリティ規程が全く作成されていなかったので、今回ガイドラインに沿って作成することとなった。 ・今後、クラウドを導入していく予定なので、セキュリティを考慮して進めることができる。
その他、派遣業務で気づいた点 等		・事務所に外部の人間が入れるようになっている、保存すべき書類の取り扱いも決まっていない等、セキュリティ対策はまだ不十分な状況であった。今回の取り組みで認識も改まり、実行計画が完了した時点では、大きな進歩が期待できると思われる。

表 10 F 社の業界ガイドライン適用結果

企業		F 社
所在地		神奈川県横須賀市
業種		建物修繕
現状		・事業拠点のほかに工事現場事務所がある。 ・基幹システムは社内にある。クラウドサービスも複数利用しており、SSO サービスも利用している。拠点、工事現場事務所等からは、VPN を使用して社内に接続している。工事現場はインターネット回線を敷き込むかモバイル Wi-Fi を使用し、PC は持ち帰る運用としている。 ・重要な情報資産は、工事関係情報（図面、居住者の連絡先、回収したアンケート等）。 ・従来のコンピュータ管理規程を元に情報セキュリティ規程を作成している。従業員の情報管理・保護への意識をどのように高めていけばよいかが課題。
業界向け情報セキュリティサンプル規程の適用評価		・物理的対策に関しては新規に策定、その他については、既存のものを見直し改定予定。 - 情報セキュリティ委員会は、他の委員会と統合した形で運営する。監査・点検責任者は当面、情報セキュリティ責任者が兼務する。 - 監査・点検の実施時期は「年 1 回」とし、時期は事業の年度計画の中で定める運用とする。 - 推奨資格は、IT パスポートと情報セキュリティマネジメント試験とする。 - 情報資産管理台帳は日建連の例を参考にしつつ、IPA の雛形に沿って作成する。 - 不要アカウントの削除は当日中に行うことにする。 - サーバは社内に設置していないことからレベル 3 領域は設定しない。 - 1.2 は削除し、許可されたソフトウェアだけが利用可能とする。 - 1.4.1 の EDR に関する記述は 7.IT 基盤運用に移す（システム管理者の実施事項のため）。 - 3.2 のスクリーンセーバー起動時間は当面 10 分とする。 - 4.2 のオンラインサービスには例示されていないサービスも含むことを明輝する。 - 4.7 から社内でのデータのやりとりは削除する（社内は専用メールを使用しているため）。 - 5.の私有 IT 機器等は利用禁止とする。 - 3.の侵入予防策から、ペネトレーションテストは当面削除する。 - 5.2 再委託先への教育等 で、日建連が準備した活用教材は、参考情報とする。 - 7.1 のサイバーセキュリティ保険は加入済み。 - テレワークについては、IT 機器利用等に必要なものを取り込む。
実行計画	組織的対策	・情報セキュリティ委員会の設置、情報セキュリティ基本方針の制定、情報セキュリティ関連規程の整備、再委託先への教育実施
	人的対策	・従業員への教育実施
	技術的対策	—
	物理的対策	—
派遣による企業の成果		・情報セキュリティに関する従業員の意識向上が悩みだったが、体勢の構築、基本方針の制定、関連規程の制定・周知の順で進めていけば良いことがわかり、それを推進する計画を作ることができた。
業界ガイドラインへの反映や考慮が必要な点		・業界向け情報セキュリティサンプル規程「ＩＴ基盤運用管理」「ＩＴ基盤の運用」の項目で、侵入予防策にある「ペネトレーションテスト、セキュリティ専門会社によるアセスメント・アドバイス」は、企業規模によっては負担が大きく、実施が困難である。 ・業界向け情報セキュリティサンプル規程「委託管理」の「再委託先への教育等」の項目で、「日建連様が準備した活用教材」を参考情報とした方がよい。
その他、派遣業務で気づいた点 等		・実行計画に基づいて対策を進めていく上で、特に情報資産管理台帳の作成や、社内教育などで、専門家の伴走支援が必要と感じられていた。

3.3.4 考察

自動車部品業界及び建設業界の 6 企業に対して業界セキュリティガイドラインを適用したところ、いずれの業界においても、規程が未整備の企業の場合、業界向け情報セキュリティサンプル規程はそのまま活用できるため有効であった。また、業界向け情報セキュリティサンプル規程を参照し、自社の規程を見直すことも有効であった。

マネジメント指導業務においても、セキュリティ対策の必要性の理解、業界で定められたセキュリティガイドラインの内容理解、対策の優先順位付けや段階的な対策計画の立案、すぐに取組可能な対策の実施、情報資産に対するリスク分析等、企業規模や企業の対策状況に合わせた専門家からの適切な助言によって、中小企業のセキュリティ対策を推進することが可能であった。マネジメント指導業務を通じて得られた効果的な対策事例から、セキュリティ対策実施にあたってのヒントもいくつか得ることができた。

業界毎の特性をみると、自動車部品業界においては、発注元と発注先となる業界団体が連携して策定された業界のセキュリティガイドラインがあり、業界団体やサプライチェーンを通じたガイドラインの周知や教育機会があることから、業界団体を通じたセキュリティ関連施策の展開が有効であると考えられる。一方、建設業界においては、発注先となる業界が多様でサプライチェーンが広いことから、セキュリティ対策推進にあたっては、業界団体からの普及や業界団体同士の連携はもちろん、地域なども巻き込んだ形で周知・教育や専門家派遣等のセキュリティ関連施策を展開していくことが望ましいと考えられる。

3.4 業界セキュリティガイドラインの導入手引きの作成

実施したマネジメント指導業務のモデルケース実証で得た知見をまとめ、業界セキュリティガイドラインの SC3 業界団体での活用促進に供するための「業界セキュリティガイドラインの導入手引き」を策定した。

3.4.1 業界セキュリティガイドラインの導入手引きの作成方法

「業界セキュリティガイドラインの導入手引き」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、業界における特に中小企業を対象としたセキュリティ対策を推進する業界団体に対して、業界セキュリティガイドラインの策定・展開を行うための方法やポイントを取りまとめたものである。

業界セキュリティガイドライン等の策定支援業務については、一般社団法人日本自動車部品工業会および一般社団法人日本建設業連合会に協力いただいたが、いずれの団体とも業界セキュリティガイドラインは策定済であったため、本業務において策定した 2 業界の「業界向け情報セキュリティサンプル規程」については、「業界セキュリティガイドラインが存在する場合の導入方法」に反映した。また、「業界セキュリティガイドラインが存在しない場合の導入方法」は、本業務で策定した「業界向け情報セキュリティサンプル規程」での知見を踏まえ、関係者との協議を踏まえて整理した。

3.4.2 業界セキュリティガイドラインの導入手引きの作成結果

「業界セキュリティガイドラインの導入手引き」は以下の構成で記載した。（詳細は「業界セキュリティガイドラインの導入手引き」を参照）

表 11 業界セキュリティガイドラインの導入手引き構成

1. はじめに 1.1 目的 1.2 使い方 1.3 本手引きの構成	「業界セキュリティガイドラインの導入手引き」の目的、読者・使い方、手引きの構成を説明。
2. 業界セキュリティガイドラインの導入 2.1 「業界向け情報セキュリティサンプル規程」の概要 2.2 業界セキュリティガイドラインが存在しない場合の導入方法 2.3 業界セキュリティガイドラインが存在する場合の導入方法	「中小企業の情報セキュリティ対策ガイドライン」の記載項目、および付録 5「情報セキュリティ関連規程（サンプル）」に関する説明を記載すると共に、業界セキュリティガイドラインの策定状況に応じた「業界向け情報セキュリティサンプル規程」の策定方法を説明。
3. 業界セキュリティガイドラインの活用 3.1 業界セキュリティガイドラインの適用	企業において「業界セキュリティガイドライン」を適用する際のポイントについて記載。
4. まとめ	「業界セキュリティガイドラインの導入手引き」まとめを記載。
5. 付録 5.1 「中小企業の情報セキュリティ対策ガイドライン第3.1 版」 記載項目の構造化 5.2 業界向け情報セキュリティサンプル規程（自工会／部工会） 5.3 突合表（自工会／部工会） 5.4 業界向け情報セキュリティサンプル規程（日本建設業連合会） 5.5 突合表（日本建設業連合会）	付録として、「業界セキュリティガイドライン」導入にあたって参考となる資料を提示。

また、「業界セキュリティガイドライン」導入方法としては以下の内容を記載した。

（1） 業界セキュリティガイドラインが存在しない場合の導入方法

業界セキュリティガイドラインが存在しない場合は、以下の順序で「業界セキュリティガイドライン（業界向け情報セキュリティサンプル規程）」を策定することを示した。

1. 業界独自の要素の抽出・修正
   「中小企業の情報セキュリティ対策ガイドライン」の記載項目を元に、業界独自の要素を抽出・反映、または業界の用語に修正する。「中小企業の情報セキュリティ対策ガイドライン」の記載項目と業界独自の内容の対比表が作成される。
2. 業界独自の要素を踏まえた修正案の「情報セキュリティ関連規程（サンプル）」への反映
   「情報セキュリティ関連規程（サンプル）」に業界独自の要素や用語を反映する。これらを反映した規程を「業界

向け情報セキュリティサンプル規程」とする。

（2） 業界セキュリティガイドラインが存在する場合の導入方法

業界セキュリティガイドラインが存在する場合、業界セキュリティガイドラインは業界において既に定められたガイドラインが該当するため、業界セキュリティガイドラインを新たに策定することはせず、対策を進めるための参考資料を作成することを示した。

1. 各業界の業界セキュリティガイドラインの記載項目の構造化
   自業界の業界セキュリティガイドラインの記載項目を構造化する。
2. 業界セキュリティガイドラインの記載項目と「情報セキュリティ関連規程（サンプル）」記載項目の対比
   業界セキュリティガイドラインの記載項目と「中小企業の情報セキュリティ対策ガイドライン」の記載項目との対比表を作成する。「情報セキュリティ関連規程（サンプル）」に対して、「業界向け情報セキュリティサンプル規程」への反映案を追記する。
3. 業界セキュリティガイドライン記載項目の「情報セキュリティ関連規程（サンプル）」への反映
   「情報セキュリティ関連規程（サンプル）」に業界ガイドラインの記載項目を反映する。これらを反映した規程を「業界向け情報セキュリティサンプル規程」とする。

なお、「業界セキュリティガイドライン（業界向け情報セキュリティサンプル規程）」の適用を実施したマネジメント指導業務の結果を踏まえ、「業界セキュリティガイドライン」の活用に促すにあたっての、自業界内または取引先の業界への展開、および企業において「業界セキュリティガイドライン」を適用する際のポイントについて記載した。

3.4.3 考察

業界セキュリティガイドラインの導入手引きの作成にあたっては、「中小企業の情報セキュリティガイドライン」を活用し、特に中小企業を対象としたセキュリティ対策を推進する業界団体に対して、業界セキュリティガイドライン（業界向け情報セキュリティサンプル規程）や関連するドキュメント等の策定・展開を行うための方法やポイントを取りまとめた。

本業務では、協力いただいた 2 団体とも業界セキュリティガイドラインは策定済であったため、業界セキュリティガイドラインが存在する場合の導入に関しては検証ができたが、業界セキュリティガイドラインが存在しない場合の導入方法に関しては実際の業界団体において検証ができていないので、今後、業界セキュリティガイドラインの策定支援に関心を持つ業界団体からのフィードバックを得る等、業界団体のニーズを取り込んだ形で導入手引きを更新していくことも検討することが望ましい。

4. 総括

本業務においては、業界セキュリティガイドライン等の策定状況調査、業界セキュリティガイドライン等の策定支援、業界団体加盟の中小企業への業界セキュリティガイドライン適用、業界セキュリティガイドラインの導入手引きの作成を実施し、実施報告書として取りまとめた。

業界セキュリティガイドライン等の策定状況調査では、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 団体に対して調査協力依頼を行い、有効回答数として 48 件を得た。「業界セキュリティガイドライン等の策定支援」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」の活用意向については、ガイドライン策定支援に 3 割弱、セキュリティ専門家派遣に 2 割強と、一定程度のニーズが見られた。

業界セキュリティガイドライン等の策定支援では、一般社団法人日本自動車部品工業会および一般社団法人日本建設業連合会の 2 団体に協力いただき、業界セキュリティガイドラインの策定支援を実施した。

業界団体加盟の中小企業への業界セキュリティガイドライン適用では、自動車産業 4 社、建設業から 2 社に対して専門家によるマネジメント指導業務を行った。特に、中小企業において情報セキュリティ規程が未整備の場合、業界向け情報セキュリティサンプル規程はそのまま活用できるため有効であった。また、業界向け情報セキュリティサンプル規程を参照し、自社の規程を見直すことも有効であった。マネジメント指導業務は、セキュリティ対策の必要性の理解、業界で定められたセキュリティガイドラインの内容理解、対策の優先順位付けや段階的な対策計画の立案、すぐに取組可能な対策の実施、情報資産に対するリスク分析等、企業規模や企業の対策状況に合わせた専門家からの適切な助言が有効であった。

業界セキュリティガイドラインの導入手引きの作成では、「中小企業の情報セキュリティガイドライン」を活用し、特に中小企業を対象としたセキュリティ対策を推進する業界団体に対して、業界セキュリティガイドライン（業界向け情報セキュリティサンプル規程）や関連するドキュメント等の策定・展開を行うための方法やポイントを取りまとめた。

業界セキュリティガイドライン等の策定状況調査においては、業界セキュリティガイドラインを策定しておらず、策定意向もある業界団体が複数見られた。本業務において作成した「業界セキュリティガイドラインの導入手引き」を活用し、業界団体を通じて各業界における中小企業のセキュリティ対策の普及を進めていくことが望ましい。ただし、業界団体においては、傘下の中小企業の規模やセキュリティ意識が異なる、業界団体の事務局のリソースが必要である等の課題もあるため、業界団体や業界傘下の中小企業の規模・意識等の状況を踏まえながら進めることが必要である。

今回、業界セキュリティガイドライン策定支援にご協力いただいた業界団体 2 団体からは、業界セキュリティガイドライン普及の取組みについて継続協力のご示唆をいただいた。今後も業界セキュリティガイドライン普及を通じた、セキュリティ対策の推進を継続していくことが望ましい。

以上