令和２年度
中小企業サイバーセキュリティ対策促進事業
(中部地域における中小製造企業等のサイバーセキュリティ促進強化事業)
に係る調査報告書

令和３年３月

中部経済産業局

調査委託先：株式会社ブレインワークス

目次

１．はじめに(目的)

近年、我が国を取り巻く経済環境は、デジタル化の進展（IoT・ビッグデータ等）、人工知能、生産技術（3D プリンタなど）、ロボットなどの技術革新、消費者ニーズの変化などに起因して、急激な変貌を遂げている。

こうした状況下、新型コロナウイルス感染拡大の危機に際して、その克服に向けたテレワークの普及定着や、生産現場の自動化、省人化への取り組みをはじめ、高度なデジタル技術の活用により、地域製造業に於いても、高まる不確実性に対処できるよう企業の変革力を高めていく必要がある。

一方、IoT 等のデジタル技術活用の進展に伴い中小製造業に対するサイバー攻撃の脅威は、これまで以上に増大しているところ。今後は、攻撃を受けた企業を起点として、サプライチェーン全体に甚大な被害をもたらす恐れもあるため、中小製造業に於けるサイバーセキュリティ対策の強化が急務となっている。

そこで本事業では、ものづくり企業が集積する中部地域（富山県、石川県、岐阜県、愛知県、三重県）において、IoT を積極的に活用している中小製造業等を対象に、サイバーセキュリティ対策への実施状況等を掌握するとともに、中部地域に於ける各支援機関等の具体的な支援策についての調査結果を取りまとめ、さらには、サイバーセキュリティに対する意識醸成に向けて、中小製造業等を対象としたサイバーインシデント演習会を開催し、多角的に中部地域のサイバーセキュリティ対策の促進・強化につなげるための「中小企業サイバーセキュリティ対策促進事業」を実施するものである。

２．企業ヒアリング

２．１　ヒアリング調査の目的

本ヒアリング調査は、IoT やロボットの活用事例や課題、また活用前後における当該ものづくりのプロセスにおける変化、サイバーセキュリティに対する意識や対策状況などについてヒアリング調査し、特徴的な取り組みについて、経済産業省中部経済産業局（以下、「局」。）ＨＰで公開できるような形で取りまとめることを目的とする。

２．２　ヒアリング調査の概要

1). 調査対象

富山県、石川県、岐阜県、愛知県、三重県の IoT を積極的に活用している中小製造業等計２０社を選出した。

選出は、各地域の中小製造業のホームページ等を調査し、その中で IT や IoT を積極的に活用し、サイバーセキュリティに取り組んでいると思われる企業を選出し、ヒアリング調査を実施した。

2). 実施期間

令和２年 11 月～令和３年２月。

２．３　ヒアリング調査結果

IoT やロボットの活用を積極的に推進している中小製造業等では、生産性向上、コスト削減、省力化に効果が見られた。また、IoT の活用を通じて、人材の獲得、育成にも効果が及ぶなど、一定の成果をあげていた。

そうした企業の活動から得られた意見は下記のとおり。

(1).生産性の向上、業務の効率化

IoT やロボットの活用を通じて生産性の向上、業務の効率化の意見を抽出した。

・機械化と IoT 導入により工数のばらつきのある作業工程の細分化はできるようになり、省力化することでコストを削減しつつ、より付加価値の高い業務に集中させることが可能になった。
・人が行った方が早いのではないかという、ベテラン社員の意識を打破するために、実際に機械と人で競争してみて、効果（スピードは遅くても休まないなど）を実感されたことでベテラン社員達も理解を示した。
・自社ブランド品など取り扱う品種が増え、職場の職員だけでは対応できないので、ロボットの導入で、成果が上がった。
・設備稼働率などの数値を実数化できたことにより、作業員の気づきや生産性向上につながった。
・高生産性の実現には PDCA を繰り返しながら生産ラインの稼働計画を最適化していく必要があり、それを「IoT」で実現した。
・設備稼働率が１５％程度向上した。また、大幅な残業時間の削減を達成した。
・IoT 設備を早い時期に導入したこともあり、製造現場の業務効率と売上げは大幅に増加した。
・社内では、自動化による業務効率改善はもちろん、情報の共有化により無駄な問い合わせが減ったり、営業成績の見える化により、社員の士気向上に寄与している。また、社員の IT スキルも向上した。
・PLC データの収集により、多くの製造工程を１～２人で管理できるようになった。社員の負荷が減って働き方が改革され、社員の採用がしやすくなるなどの効果がでた。
・ロボットを導入したのは、人と比べてミスが少ないという点。また、社員の採用が難しい状況になり、この仕事をやりたい人も減っている実情もある。そのため、ロボットを増やさざるを得ない状況である。

(2). 人材獲得、人材育成

IoT やロボットの活用を通じた人材獲得、人材育成の意見を抽出した。

・夜間の稼働などもあり、人の採用が難しくなったため、いち早くロボットの導入にチャレンジ

した。
・ロボットが身近にあることにより、ベテラン社員の指導の下、若手社員の育成ができる。新しいチャレンジをしていることが評価され、新たな人材の採用に成功している。またロボット導入により重労働が軽減され、女性社員の割合も増えている。
・業務効率やコスト削減の成果も出ているが、現場の安全性が上がることや、「ロボットって楽しいね」といったように社内の雰囲気がよくなることで士気が向上した。また、まずは出来るところからやってみよう、という意識も醸成された。
・これまでは課題への取り組みを社長が率先して行っていたが、最近は社員に経験させるようにしている。社長の勘を「見える化」し、その手順を人材育成の制度として取り組む。
・オペレーションが自動化されたことで、比較的短期間での人材育成が可能となった。
・作業の標準化に対する意識が向上し、作業が整理された。標準化されたノウハウ、効果により、さらなる意識の向上が図られ、現場でチームを組み改善する意識が醸成された。
・中山間地の製造業が雇用を確保、維持しながら成長を図っていくには、効率化による作業環境の改善は避けて通れない課題であった。
・システム開発のプロジェクトを実質１名で対応していたことから、必要とされるリテラシーの不足等の課題も多かった。最初はラズベリーパイもよくわからないベンダーに頼んでいた。今後は、開発したシステムを改善できる人材を育成していく。
・世代間ギャップもあり、更に社内に専門人材もいないので IT 人材の育成が難しい。
・製造技術者４～５名が IoT ツール活用によりスキルアップして多能工となった。
・無線技術、マイクロセンサー技術は従業員でレベルアップしている。改善案が出てくるようになった。

(3). IoT やロボットへの導入サポートの必要性

IoT やロボットの活用企業での導入サポートへの課題の意見を抽出した。
・ロボットの導入後の変更など外部に依存しているので、自社でメンテナンスしていく体制を構築するのが重要。
・プログラム変更の対応や、自動化した仕組みにトラブルが起きると現場への影響が大きかった。
・自動機が停まったことがあるが、自動化したことで人を減らしていること、替わりの古い機械も片付けていることから迅速に復旧対応できないことがあった。
・IoT 技術に関して、なかなかいい相談先がない。大手だと費用感があわず、規模が小さいと業界特有の特殊さについての知識不足やスキル不足を感じる。
・一番苦労したのは CNC 旋盤や配線、センサーなどを含めフィジカル層に近い部分を構築できるベンダーがいないこと。
・作業が特殊で一品一品の受注生産であり、それに見合う IoT ツールをどのように探して導入していくかが課題。
・今後社内の IoT 化を推進していくにあたり IT 部門を担当する人材が不足していると感じている。

(4). サイバーセキュリティ対策への取り組み

IoT やロボットの活用企業でのサイバーセキュリティ対策への意見を抽出した。

・サイバー攻撃は脅威に感じており、自社でのセキュリティルールも整備している。ただし、なかなかルールが徹底されているか確認ができない。
・セキュリティの導入補助金等があればもっと企業の中で取組が進むと感じている。
・テレワークを推進していく際にセキュリティ対策の強化も検討する。
・対策として各種端末に 2 段階認証を設けたり、自社のセキュリティ対策の実施状況をチェックシートで点検し顧客に報告している。
・今後はコロナの影響などで働き方を変える必要もある。その際、社内のシステムをネットワークに繋げていくための方針および対策が必要になると考えている。
・サイバーセキュリティ対策について、会社の方針や進め方について手探りである。
・サイバーセキュリティ対策の課題として、どこから手をつけていけばよいか、他社との比較で自社がどれくらいの対策ができているかわからない。
・サイバーセキュリティ対策は今後ますます重要になってくると認識しているが、課題は、サイバーセキュリティの知識不足、人材不足、コスト。また体制を維持していくことも課題だと感じている。
・情報資産と情報セキュリティのルールを作成して実施している。また、年に 1 回程度、独立行政法人情報処理推進機構（以下、IPA）の資料を参考にしながら社内研修を行っている。
・セキュリティ研修や全体集会での啓蒙活動を実施、またコンサル会社のセキュリティ研修を受講している。
・今後 IoT、ロボットを本格的に使用していく場合、より強固なセキュリティ対策をとる必要があると考えている。
・セキュリティを意識しすぎるが故に、社外への接続について躊躇している。

３．支援機関ヒアリング

３．１　ヒアリング調査の目的

本ヒアリング調査は、中部地域の各県庁や政令指定都市などの有力市町村、県警察、支援センター、商工会議所など、IoT・ロボット等の活用促進施策やサイバーセキュリティ対策に取り組んでいる支援機関を訪問してヒアリング調査を行い、各支援機関が業務を遂行する上で日頃抱えている課題や各機関の取組の中で特に有効性の高いものを局ＨＰに公開できるように取りまとめることを目的とした。

３．２　ヒアリング調査の概要

1). 調査対象

富山県、石川県、岐阜県、愛知県、三重県の各県庁や政令指定都市などの有力市町村、県警察、支援センター、商工会議所など各県につき２機関以上として１０機関を選出した。

選出にあたっては、各県庁や政令指定都市などの地方自治体、県警察、支援センター、商工会議所に加えて、大学や民間で IT・IoT 関連分野において支援を行っている企業などから選抜して実施した。

2). 実施期間

令和２年 11 月～令和３年２月。

３．３　ヒアリング調査結果

「２．企業ヒアリング」では、企業において IoT やロボットの活用を積極的に推進しており、生産性向上、コスト削減、省力化に効果があることが見受けられた。また、IoT の活用を通じて、人材の獲得、育成にも効果が及んでおり予想以上の成果をあげていた。

一方、IoT の活用が進むほど、中小企業におけるサイバー攻撃の脅威と脆弱性の懸念はこれまで以上に増大している。

IPA が公開している「情報セキュリティ 10 大脅威 2021」でも示されているとおり、サプライチェーン上の関連企業に対して、攻撃された中小企業を通じて広く影響を及ぼす可能性があり、製造業全体のサイバー対策の推進・強化が必要であるが、中小企業では売上増に直接結び付かないものにコストは掛けられないなどの理由から情報セキュリティに対する意識は向上しているものの、情報セキリティに着手するか否かは経営者層の直接的な関与・理解が非常に重要になっている。

このような実態を踏まえ、支援機関の活動では、まだまだ企業の経営者層へのサイバーセキュリティ対策の促進・強化の必要性の動機づけが必要であるという認識が見受けられた。

以下では、支援機関の活動から得られたサイバーセキュリティ対策に関する調査結果をまとめた。

(1). 支援内容

支援機関での主な支援内容を以下に示す。

・サイバーセキュリティお助け隊事業として、セキュリティ簡易診断、セキュリティ監視ソフト・機器の導入、Web ブラウザのフィルタリング、問い合わせ窓口開設・駆けつけ支援を実施。
・ホームページ診断、ネットワーク診断、ＰＣ診断等を実施。標的型メール訓練も行い、社員教育を行う場合もある。
・情報セキュリティ・リスクアセスメントを行い、防御の穴を見つけ、対策としてどんな行動を

起こせば良いかを身につけてもらうことを重視している。また、小規模企業には簡易アセスメントの実施や、セキュリティ保険への加入を助言している。
・情報担当者向けにセキュリティ研修を行っている。
・サイバーセキュリティの視点を取り入れた企業支援の展開も検討。
・大学としての立場で支援や研究を実施している。各研究室の独立性が高い大学の組織構成は、中小企業の集合体に近いものがあり、様々な大学の学内向けのセキュリティ対策/運用/支援は、中小企業のセキュリティ対策/運用/支援に応用できるのではないかと考える。
・IoT 活用セミナーを通じて、サイバーインシデント事例等を紹介している。
・基本的なセキュリティ対策に関する啓蒙活動の重要性や、IoT の通信機器は初期設定値で使わないような指導の実施。
・学生に対してリテラシー、セキュリティ、認証や法律など関連分野も含めた講義を行っている。
・愛知県警が実施している「中小事業情報セキュリティ対策支援ネットワーク」に参加し、サイバー犯罪に対する情報共有を行っている。

(2). 中小企業のサイバーセキュリティの対策と課題

支援機関での中小企業のサイバーセキュリティ対策と課題を抽出した。
・中小企業の中には「セキュリティは後回し」、「お金をかけられない」、「当社には関係ない」という企業もある。
・経営層の強い意識・協力を得ないと着手されない傾向にある。
・セキュリティに対してコストパフォーマンスを考え、二の足を踏む企業が多い。
・サイバーセキュリティ対策は必要不可欠な取組であり、情報共有等に取り組んでいくことが必要ではあるが、ICT・データ活用を推進する取組を優先せざるを得ない状況にある。
・サイバーセキュリティ対策について、日本の中小企業が遅れているとまでは言えないと認識している。ただし、大企業と同じレベルの対策を行うことはコスト面や人材面から難しいと考えている。
・１時間程度のセミナーを、年１回程度継続して開催すべきではないか。毎年傾向が違うので、事例で疑似体験し、自分事として考えてもらう習慣を身につけてもらう必要がある。

(3). サイバーセキュリティに対する地域（支援範囲）の特徴

支援機関でのサイバーセキュリティに対する地域（支援範囲）の特徴を抽出した。
・地域性に関係なく売上増に結び付かないものにコストは掛けられない。ただし、近年、セキュリティに対する意識は向上していると考えている。
・情報セキュリティに着手するか否かは経営者の関与・理解が非常に重要である。
・外部のアドバイザーなどと連携することが多く、地域で取り組んでいく仕組みを構築している。
・自動車関連の企業が多い地域であり、１つの企業が攻撃を受けると連鎖的に被害が拡大するな

ど、影響が大きい。

(4). 支援先（中小企業）に望むこと

支援機関での支援先（中小企業）に望むことを抽出した。

・セキュリティの研修を毎年実施しているが、年々参加者が減少しているのでもっと関心を持って欲しい。
・サイバー犯罪の事例を収集し、その影響度を社内で共有することで脅威を身近に感じてもらうこと。
・日ごろからセミナーなどに参加し、更新される情報を獲得する習慣をつけて欲しい。また、UTM などを導入して終わりではなく、ログ情報などを活用できるようになって欲しい。
・ICT・データの活用とともに、セキュリティ対策の重要性をトップが認識すること。また、セキュリティ対策要員を専任でなくても設けること。
・完璧を求めすぎず事前対策、事後対策も８０点をとるという考えが良い。決して難しいことをやる必要はなく、IPA などの無料の資料を使用しながら学び始めたり、専任のセキュリティ人材を配置するのが難しいのであれば､最近は格安なところも出てきているセキュリティオペレーションサービスの活用などを検討しても良い。
・社長ではなく、サイバー担当の役員と担当者をつくり、ポリシーとルールを作成して文書化する。社内の詳しい人と外部の専門家との意見交換、セミナーへ参加するなど、自分事として取り組む必要がある。リスクを認識すること。
・まだまだ不十分である。ウィルス対策ソフトを導入した程度で終わっている。社長、経営者層はまだ認識が不足している。
・IT ベンダーに依存し過ぎており社内に人材が育っていない。大手顧客からセキュリティチェックシートの提出を迫られると急に右往左往している現状がある。

(5). 今後計画している支援策

支援機関での今後計画している支援策を抽出した。

・大阪商工会議所独自の「セキュリティお助け隊」のような活動を行っていきたい。
・県、市との連携活動や、北陸総合通信局との定期的勉強会で民間企業の事例研究を行っていく。
・情報セキュリティ各種診断メニューパッケージの提供など。
・普段セキュリティに対しては二の足を踏む企業も、サイバーセキュリティ対策のための補助金があれば積極的に導入できる。あとはその活用方法を継続的に支援することが必要となる。

４．セミナー開催報告

４．１　セミナー開催の目的

時々刻々と変化していくサイバーインシデント発生時への対応について、経営者の目線、セキ

ュリティ担当者の目線から対応すべきセキュリティ対策について、実際におきたサイバーセキュリティインシデントをもとにした、リアルなシナリオ形式のセミナーを実施した。

本セミナーを通じて、標的型攻撃、マルウェア感染、ビジネスメール詐欺による被害、脆弱性情報の悪用による被害等のインシデント発生時の状況判断・意思決定といった危機対応に必要な要素と考え方を理解するとともに、ウィルス等に感染していないか自社で簡単にできる検知方法から、実際に被害が出た際にまずすべき対応、報告の仕方などのインシデント対応を学ぶことができ、また、サイバーセキュリティにかかる自組織の課題や必要な取り組みについて発見できるようになることを目指した。

４．２　セミナー開催の概要

1). セミナー開催対象

第１部　11：00～12：00

（経営者向け）

【経営者がなすべきサイバーセキュリティ対策】

高まるサイバー攻撃のリスクは、IT、IoT、AI の導入を進める中小企業にとって桁違いとなっており、サイバー攻撃により、工場等を機能不全にした事例や、人命にかかわるような事例も出てきている。そこで、最新のサイバーセキュリティ対策情報を実際の国内外の幅広い事例を交えながら、経営者の立場から実施すべきサイバーセキュリティに対する心得と対策についても説明を行った。

（講師）

株式会社ブレインワークス　取締役　大西　信次

（セミナー概要）

１．高まるサイバー攻撃のリスク
２．IoT への脅威は桁違い
３．攻撃するＡＩ、防御するＡＩ
４．ＤＸとサイバーリスク
５．経営者がなすべきサイバーセキュリティ対策
６．各種認証制度、資格制度、サイバー保険

第２部　13：00～16：00

（担当者向け）

【セキュリティ担当者の心得】

企業の担当者が心得ておくべきサイバーセキュリティの動向やサイバー攻撃の手法について紹介した。また、今後ますます重要となるセキュリティポリシーの策定や脆弱性診断、緊急事態への対応について、実践的視点から解説を行った。

特に、最近の「サイバーセキュリティの動向」を示しながら、対応が急務となっている「テレワークで実施すべきセキュリティ対策」など、実践的に活用できるテーマを交えて解説を行った。

また、セキュリティ担当者の役割を明確にし、不正アクセス、サーバ等機器、Ｗｅｂアプリケーションなど、それぞれ個別の対策について解説を行った。

（講師）
１～５を担当：株式会社ブレインワークス　取締役　大西　信次
６～９を担当：株式会社ブレインワークス　経営サポート事業部　渡利　周司

１．サイバーセキュリティ動向
２．セキュリティポリシーの策定
３．テレワークで実施すべきセキュリティ対策
４．緊急事態への対応
５．IoT への対処方法
６．セキュリティ担当者の役割
７．不正アクセス手法と対策
８．サーバ等機器における対策
９．Ｗｅｂアプリケーションにおける対策

2). セミナー開催日時

令和２年１２月１５日　１１：００～１６：００

４．３　セミナー開催結果

・セミナー全体の申込者数は定員 30 名に対して 86 名の申し込みがあった。当日の最終参加者数は 70 名、アンケートの回収数は 44 名（回収率 62.9%）だった。
・第 1 部の参加者数は 46 名（アンケート回収数は 29 名（回収率 63.0%））、第 2 部の参加者数は 56 名（アンケート回収数は 35 名（62.5%））だった。
・アンケート回答企業（組織）の従業員数は、100 名以下の企業が 63.6%であったが、500 名以上の企業も 7 社あり、幅広い規模の企業において、この分野に対する関心の高さが示された。

(1). セミナーに対する満足度

第 1 部のセミナーの満足度は１０点満点中 8 以上が 55.1%、第 2 部は 60.0%だった。
なお、その理由については、以下のような回答があった。
・大変参考になった。一般の研修ではそこまで教えてもらえなかった。
・かなり濃い内容でびっくりしました。私は、手配業務のシステム管理者で情報システムのプロではありませんが、とても有益なお話だと感じた。
・最新の情報、ハッカーの手法が理解しやすかった。

また、上記に対して、

・サイバーセキュリティ実践について、経営層とセキュリティ対策技術者向けときいていましたので、経営層がすべき事について、もう少し言及が欲しかった。
　また、技術者向けも総花的であったので、最新の情報セキュリティ事件を深堀して対策まで聞きたかった。

という意見もあった。

(2). 現状の自社のセキュリティに対する対策の充実度

自社のセキュリティ対策の充実度は、6 以下（10 段階で 10 が良いとの認識）の回答が 72.7%を占めた。 5の回答が一番多く（27.3%）、次いで 6 の回答が多かった（20.5%）。これらから自社のセキュリティ対策の充実度は、決して高くないとの認識の企業が多く、課題を感じている企業が多いと言える。

なお、「上記の質問で自社のセキュリティ対策が充実している（評価 6 以上）とお答えいただいた方にお伺いいたします。差し支えない範囲で構いませんので自社内でどのような対策を行っていますか。」の問いに対しては、主に以下のような回答があった。

・セキュリティポリシーの遵守、ネットワークの分離
・公認システム監査人によるシステム監査
・定期的な社内教育の実施
・ファイアウォール、ウィルス対策ソフトの導入
・VPN 導入による閉域網の設置、クラウド UTM の導入

(3). 自社のセキュリティに対する社内研修体制の充実度

社内研修の充実度も 6 以下（10 段階）の回答が 86.3%あり、多くの企業で自社の課題であると感じていると考えられる。

(4). 現状の自社の IT・セキュリティに対するルール整備の充実度

ルールの整備状況に関しても 6 以下（10 段階）の回答が 79.5%となっており、これらについても社内研修の充実度と並び、多くの企業で自社の課題であると感じていると考えられる。

(5).最新のサイバーセキュリティ―の現状についての情報を収集

各企業とも定期的に最新のサイバーセキュリティの現状についての情報収集に対して、「よくしている」、「時々している」が合わせて 86.4%となっており、各企業とも情報収集には積極的であることが分かった。

５．総括

５．１　企業ヒアリング

IoT を成功させるためには、まずは「自社の課題を明確にすること」が重要だということが分かった。経営者による判断だけでなく、実際に製造に関わる現場の声を聞き、各部門の課題を知ることで、改善すべきボトルネックを見つける必要がある。また、実際に導入した後の業務フローの見直しや、担当者の配置変更など、現場で上手く活用ができる体制を整えることも不可欠である。

さらに、IT や IoT の仕組みをよく学びリスクや弊害も理解した上で用途・用法を考える必要がある。技術を正しく理解しないと誤用や乱用により損害を被ることになる。特に、サイバー攻撃や故障の対応のために、自ら予防策や復旧策を準備し日々訓練しておくことが重要である。

また、IoT が安全に使われているか常にチェックすることも重要である。事故につながる危険はないかを常に監視し IoT の安心・安全を守る当事者であるという自覚を持って導入する必要がある。

サイバーセキュリティ対策においては、「サイバーセキュリティ対策は今後ますます重要になってくると認識しているが、課題は、サイバーセキュリティの知識不足、人材不足、コスト。また体制を維持していくことも課題だと感じている。」という意見に代表されるように、セキュリティ対策への認識は高いが、知識不足、人材不足、コストへの課題があると思われる。全般的にサイバー攻撃などのリスクがあるのでセキュリティ対策をしなければならないと感じているが、取り組みが道半ばであるという自己評価であり、IoT やロボットに特化したセキュリティリスクに言及しているケースがほぼなかった。漠然とセキュリティリスクがあり、IoT・ロボットを活用している企業も、その他の一般企業と同様のパソコンからの情報漏洩などのリスクがあるのでその他の一般企業と同様にアクセス権設定やＯＳアップグレードなどの対策をしなければならないという意識と想定される。IoT 機器のハッキングによる財物・人体へのリスクや、ＯＳのアップグレードの難しさ、パスワード変更のしづらさなどは今回のヒアリングではなかなか意見として出てこなかったことからも IoT やロボット導入特有のセキュリティリスクにはまだあまり目を向けられていない現状がある。

今後 IoT、ロボットの導入が進む中、IoT、ロボット導入時特有のセキュリティリスクを学び、対応をしていく必要がある。

５．２　支援機関ヒアリング

企業では、IoT やロボットの活用を積極的に推進しており、生産性向上、コスト削減、省力化に効果があることが見受けられ、IoT の活用を通じて、人材の獲得、育成にも効果が及んでおり予想以上の成果をあげていた。

一方、IoT の活用が進むほど、中小企業におけるサイバー攻撃の脅威と脆弱性の懸念はこれまで以上に増大していることから、支援機関では、サイバーセキュリティ支援事業として、セキュリティ簡易診断、セキュリティ監視ソフト・機器の導入、Web ブラウザのフィルタリング、問い合わせ窓口開設・駆けつけ支援の実施、ホームページ診断、ネットワーク診断、ＰＣ診断等の

実施、企業向けサイバーセキュリティセミナーの開催、標的型メール訓練の社員教育など様々な支援を実施していた。

しかし、５．１で示したとおり、中小企業では、サイバーセキュリティ対策が経営層の強い意識・協力を得ないと着手されない傾向にあり、「情報セキュリティは後回し」、「お金をかけられない」、「当社には関係ない」という企業もあった。近年、情報セキュリティに対する意識は向上しているものの、大都市に比べてまだ意識が低い、対策が浸透していない状況であるという意見も支援機関へのヒアリングで散見された。

支援機関では、各機関がそれぞれセキュリティの研修を毎年実施しているが、企業の限られた情報セキュリティ担当者への研修が一巡したことから、年々参加者が減少している傾向も見られる。日ごろからセミナーなどでサイバー犯罪の事例を示して、その影響度を身近に共有し脅威を感じてもらうことで最新の情報を獲得する習慣をつけることが重要である。ヒアリングをした支援機関から「完璧を求めすぎず事前対策、事後対策も８０点をとるという考え方により、決して難しいことをやる必要はなく、IPA などの無償の資料を活用しながら学び始め、専任のセキュリティ人材を配置するのが難しいのであれば、外部のセキュリティオペレーションサービスを活用するなど、継続的なサイバーセキュリティ対策を実施する必要がある」という意見があった。

支援機関では、「IoT の通信機器は初期設定値で使わない」、「１つの企業が攻撃を受けると連鎖的に被害が拡大する（サプライチェーンを IoT でつなぐ場合）」といった意見が見られ、企業よりも IoT、ロボットゆえのセキュリティリスクについて意識が向いているようにも見られる。ただし、一般のオフィスにおけるセキュリティと、IoT を使う工場でのセキュリティの違いについて踏み込んだ話は聞けなかった。

以上のことから、支援機関として、今後も継続して、企業の経営者や情報セキュリティ責任者にサイバーセキュリティのリスク（影響度と脅威）の事例を示して情報セキュリティ対策実施の必要性の意識向上を図るとともに、経済的に負担の軽い、これならできると受け入れられるサイバーセキュリティソリューションを提供していく支援活動をしていくことが必要である。

５．３　セミナー開催

各企業とも大きな事故、損害の発生がない状況の中で、危機意識を持つことが難しい面もある。会社の売上・利益優先傾向にもあり、リスク管理の取り組みであるサイバーセキュリティの分野について積極的に対策を行っている企業は限定的であったとみられる。

ただ、昨今、サイバーセキュリティ対策は、経営に大きな影響を与えることが鮮明になってきている。セキュリティ対策を実施して対外的に安心・安全をアピールすることで、企業としての信頼性を確保し、売上を伸ばしている事例もある。

逆に、サイバーセキュリティ対策が不十分で、企業の機密情報や個人情報の漏洩が発生し、企業としての信用が失墜し、業績が大きく落ち込んだ事例も報告されている。そのような状況下にあって、各企業とも情報収集を積極的に行っていることが分かった。特に同業他社の対策の状況や事例などにも関心が高いことがうかがい知ることができた。

こうしたサイバーセキュリティの分野のセミナーは、事例研究を交えるなど、啓蒙活動の意味でも開催ニーズは確実に存在する。

５．４　全体として

各企業、各支援機関とも、サイバーセキュリティの対策状況や、実際に起こったサイバー事故等についての情報を公開していない現状もあり、実態としての状況については不明な点も多い。

各企業、各支援機関に対してヒアリングの依頼をした状況下において、ヒアリングの受け入れを拒む企業や支援機関もあった。自社の対策については非公開にしたいとの意見や、外部に公表できないといった意見もあった。

また、各企業との意見交換において、実際にサイバー攻撃等にあった場合の相談を、どこにすればよいか分からないという意見も少なからずあった。そのため、同業社間のネットワークの中での意見交換により解決をしようという場面もあった。

IoT、ロボットを導入した際のセキュリティリスクは、一般のオフィスでインターネットに接続している企業のセキュリティリスクとは異なる部分がある。オフィスでのセキュリティ対策は世間で普及しているが、工場でのセキュリティ対策は事例も少なければ、書籍や資料などの情報もまだまだ少ない。今回ヒアリングしたIoT・ロボットを活用している中小企業や、その支援機関でも、この世間の状況と同じく、IoT、ロボットを導入する上でのリスクやその対策について、十分ではなかった。今後、IoT、ロボット導入がますますさかんになることが想定されることからも、産学官などの支援機関等を通じたセミナーなどの啓蒙活動や、周知の徹底、大手企業や中小企業の先行事例の共有などを進めていく必要がある。

以上