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
(概要版)

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

１．１　事業目的

デジタル化の進展（IoT・ビッグデータなど）、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、ものづくりを取り巻く外部環境は、近年大きく変化している。

加えて、新型コロナウイルス感染症の影響によるテレワークの拡大、生産現場の自動化、省人化への取り組みなど、各企業の業務全般でデジタル化を加速させる必要性が生じている。

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。

さらに、サプライチェーン上の関連企業にも、攻撃された企業を通じて影響を及ぼす可能性があり製造業のサイバー対策の推進・強化が必要。

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のサイバーセキュリティ対策への実施状況および関心等について把握するとともに、中部地域の支援機関等の支援策について調査し取りまとめ、さらに中小製造業のサイバーセキュリティに対する意識を高めるためのサイバーインシデント演習会を開催するなど、一連の事業を実施することで、中部地域のサイバーセキュリティ対策の促進・強化につなげることを目的とする。

１．２　IoT活用事例及びセキュリティ実態調査

（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、「産業局」といいます。）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） 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社選出。
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。

3).ヒアリング内容

・生産性の向上、業務の効率化について
・人材獲得、人材育成について
・IoTやロボットへの導入サポートの必要性について
・サイバーセキュリティ対策への取り組みについて

4).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、育成にも効果が及んでおり一定の成果をあげていた。

１．３　IoT・ロボット等の活用促進施策及びサイバーセキュリティ対策施策調査

（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。

（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有力市町村、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).ヒアリング内容

・支援内容について
・中小企業のサイバーセキュリティの対策と課題について
・サイバーセキュリティに対する地域（支援範囲）の特徴について
・援先（中小企業）に望むことについて

１．３　IoT・ロボット等の活用促進施策及びサイバーセキュリティ対策施策調査

4).ヒアリング調査結果

・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、攻撃された中小企業を通じて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。

１．４　サイバーインシデント演習会の開催

（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。

（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。

１．４　サイバーインシデント演習会の開催

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。

2).セミナー開催日時：令和２年１２月１５日　１１：００～１６：００

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。

１．５　総括

（１）IoT活用事例及びセキュリティ実態調査

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、コストへの課題等があると思われる。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。

１．５　総括

（2）IoT・ロボット等の活用促進施策及びサイバーセキュリティ対策施策調査

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、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などの無料の資料を使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。

１．５　総括

（2）IoT・ロボット等の活用促進施策及びサイバーセキュリティ対策施策調査

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、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。

１．５　総括

（3）サイバーインシデント演習会の開催

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明確になってきている。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。

１．５　総括

（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く感じられた。

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に相談を、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。