調査研究論文【商工総合研究所 調査研究事業】

中小サービス業のサイバーセキュリティ対策

中　谷　京　子
（商工総合研究所
主　任　研　究　員）

＜要　旨＞

○近年、サイバー攻撃の脅威は増大しており、大企業だけでなく中小企業もその標的となっている。経営資源が限られる中小企業は、大規模なセキュリティ投資が難しい場合が多く、その結果、攻撃者にとって「狙いやすいターゲット」となることがある。デジタル化が進む時代のリスクとそれに対応する方法を理解していくことは、企業の継続性を守る上で非常に重要である。

○サイバー攻撃は、データの盗難、業務妨害、顧客信用の損失といった深刻な影響を及ぼす。例えば、従業員や顧客の個人情報が漏洩した場合、法的責任や賠償費用が発生するだけでなく、信用を回復するのに長い時間がかかることもある。また、ランサムウェア攻撃によって企業の業務が停止するケースも増加している。

○中小企業には、製造業における部品調達のような関係（以下、サプライチェーン）の中で、大企業等取引先の指示・要請によってサイバーセキュリティ対策を実施している企業がある。一方で、大企業の指導が届きにくい、地域に根差した小規模な個人事業者が多い業界、多様な顧客層に対応する必要がある業界、分散型の事業構造を持つ業界、例えば理美容業、旅館業、飲食業、小売業など（以下、中小サービス業という）は、対策が遅れている。

○これらの企業は、取引先等からの指示・要請がないことに加え、社内に特許や技術的な内容などの重要な情報が無いという考えや、他社のプラットホーム（決済やデータ管理など）を利用しているため、自社が責任を負うものではないと考えている、という結果が複数のアンケート調査から見てとれる。本稿では、中小サービス業がサイバーセキュリティ対策を推進するにはどのような支援が有効か、事例企業や中小企業支援機関へのインタビューから明らかにしたい。

○中小サービス業のサイバーセキュリティ対策推進には、「サイバーセキュリティ対策を進めざるを得ない環境にすること」、「リソースの不足やコスト面での負担を軽減すること」が必要である。具体的には、各業界の特長を踏まえた業界ごとのサイバーセキュリティガイドラインを経済産業省やIPAなどの政府関係機関等が策定することで、最低限の基準が提示される。これにより、企業は対策を進めざるを得ない環境になると思われる。また、対策を進めるための負担軽減策として、基準を満たしていないと判断した企業には、地域の中小企業支援機関である商工会議所や中小企業団体中央会などが、各企業の業種に基づき、企業の状況に応じて支援する。支援内容は、IT企業の紹介やサイバーリスク保険加入などのアドバイスを行うなどで、社内にIT人材を配置することが難しい中小サービス業の負担を補うことができる。中小サービス業には、このような、既にある体制を活用しながらハンズオンで支援することが、サイバーセキュリティ対策を浸透させるための一つの取りうる手段となるのではないだろうか。

目　次

はじめに

近年、サイバー攻撃の脅威は増大しており、大企業だけでなく中小企業もその標的となっている。経営資源が限られる中小企業は、大規模なセキュリティ投資が難しい場合が多く、その結果、攻撃者にとって「狙いやすいターゲット」となることがある。デジタル化が進む時代のリスクとそれに対応する方法を理解していくことは、企業の継続性を守る上で非常に重要である。

サイバー攻撃は、データの盗難、業務妨害、顧客信用の損失といった深刻な影響を及ぼす。例えば、従業員や顧客の個人情報が漏洩した場合、法的責任や賠償費用が発生するだけでなく、信用を回復するのに長い時間がかかることもある。また、ランサムウェア攻撃によって企業の業務が停止するケースも増加している。

中小企業には、製造業における部品調達のような関係（以下、サプライチェーン）の中で、大企業等取引先の指示・要請によってサイバーセキュリティ対策を実施している企業がある。一方で、大企業の指導が届きにくい、地域に根差した小規模な個人事業者が多い業界、多様な顧客層に対応する必要がある業界、分散型の事業構造を持つ業界、例えば理美容業、旅館業、飲食業、小売業など（以下、中小サービス業）は、対策が遅れている。これらの企業は、取引先等からの指示・要請がないことに加え、社内に特許や技術的な内容などの重要な情報が無いという考えや、他社のプラットホーム（決済やデータ管理など）を利用しているため、自社が責任を負うものではないと考えている、という結果が複数のアンケート調査から見てとれる。本稿では、これらの中小サービス業のサイ

バーセキュリティ対策推進に効果的な対策を、事例企業や中小企業支援機関へのインタビューを通じて明らかにしたい。

1．サイバーセキュリティの現状

(1) サイバー攻撃の変遷

サイバー攻撃は、国家に対するものとしてインフラ（通信網に障害を発生させる）への攻撃からスタートした。アメリカでは、2010年4月には（Committee on National Security Systems）の指令4009「国家安全保障システム委員会用語集」にて、サイバー攻撃を「サイバースペースを介して、企業のサイバースペース利用を標的とした攻撃で、コンピューティング環境やインフラを混乱させ、無効化、破壊し、悪意を持って制御し、データの完全性を破壊する、あるいは制御された情報を盗むことを目的とするもの。」と定義した。その後、国家に対するものだけではなく、企業が保有する「重要情報」である「製品開発に関する技術的な内容などの情報」から「個人情報（住所、資産状況、健康状況）」を盗み出す、というものに広がってきた。

これらの情報を盗み出し、闇で売買することで利益を上げるものが出てきた。それが進化して、盗み出さなくても「一旦システムが動作しないようにして、身代金を要求する」ものが出てきた。「ランサムウェア」である。さらに、犯罪者の分業も進化しており、脆弱なシステムを使用している企業のリストを作成する者、ランサムウェア（システム）を開発する者、実際に実行する者、などに分化し、闇サイトでリストやシステムの売買が行われるなど、いわゆる「特定流動化犯罪グループ（トクリュウ）」のような形になり、犯罪を取り締まるのがより難しくなっている。また、AIの発達により、英語圏だけではなくさまざまな言語に対応することができるようになったため、日本も標的にされやすくなっている。

つまり、サイバー攻撃の内容はどんどん進化しており、その進化したものに常に対峙しなければならないのである。

(2) サイバー攻撃による被害状況

サイバー攻撃の被害状況（**図表1**：インシデント報告関連件数）をみると、サイバー攻撃のインシデント[1]は毎月2,000件程度報告されている。ただし、この数はあくまでもサイバー攻撃の被害があった、もしくはインシデントが発生したが被害が無かったと企業が認識し、届出したものである。

そのうちフィッシングサイト[2]によるものが約80%となっている。巧妙な手口で企業や個人のIDやパスワードを盗み出している。ほかにも、自社のウェブサイトが改ざんされるというものや、マルウェアに感染するというものがある。マルウェアとは、コンピューターウイルスとよばれていたものの最近の呼び名で、感染するとデータの窃取や改ざんの他、メールサーバーが第三者への攻撃に使用されるものをいう。

1　コンピューターセキュリティにおけるインシデントとは、「情報および制御システムの運用におけるセキュリティ上の問題として捉えられる事象」をいう。（JPCERTHPより）https://www.jpcert.or.jp/aboutincident.html　2025年7月31日閲覧

2　フィッシングサイト（による事案）とは、携帯電話会社、宅配業者、金融機関をかたって電子メールやSMSを送信し、本物そっくりの偽サイト（フィッシングサイト）に誘導し、IDやパスワード等を入力させるもの。当該IDとパスワードは不正な取引に利用される。警察庁HPフィッシング対策ページ https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html　2025年7月31日閲覧

（図表1）インシデント報告関連件数（2024年4月1日～2025年3月31日）

インシデント	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	合計	割合
フィッシングサイト	1,685	1,733	1,607	1,490	1,423	1,320	1,619	1,476	1,685	1,585	1,779	1,903	19,305	83%
Webサイト改ざん	8	20	15	61	25	7	8	21	24	53	25	17	284	1%
マルウェアサイト	28	12	5	9	10	6	11	11	14	10	1	12	129	1%
スキャン	252	285	152	154	127	93	74	77	82	105	72	79	1,552	7%
DoS/Ddos	0	1	2	0	5	4	0	3	1	4	0	2	22	0%
標的型攻撃	2	0	0	0	1	5	0	2	0	1	0	0	11	0%
その他	305	347	145	107	188	112	177	123	153	161	137	135	2,090	9%
合計	2,280	2,398	1,926	1,821	1,779	1,547	1,889	1,713	1,959	1,919	2,014	2,148	23,393	100%

（出所）一般社団法人JPCERTコーディネーションセンター「インシデント報告対応レポート」
https://www.jpcert.or.jp/pr/2025/IR_Report2024Q4.pdf　20250731閲覧
（筆者作成）

独立行政法人情報処理推進機構（IPA）（以下IPA）の中小企業に対する調査では、2022年から2025年までの3期にわたるサイバーインシデントによる被害発生額は、平均で73万円、最大値は約1億円となっている。また、被害後の復旧期間は平均で5.8日とほぼ1週間で、最大では360日（約1年）を要したというデータがある（**図表2**）。

（図表2）過去3期におけるサイバーインシデントによる被害発生額など

項目	平均値	最大値
被害総額	約73万円	1億円
発生回数（回）	1.1	40
復旧期間（日）	5.8	360

（出所）「中小企業における情報セキュリティ対策に関する実態調査―報告書－」（2025）IPA
https://www.ipa.go.jp/security/reports/sme/nl10bi000000fbvc-att/sme-chousa-report2024r1.pdf

また、令和6年のランサムウェア被害件数は、前年と比較して大企業の被害件数が減少する一方、中小企業の被害件数が増加している[3]。

これらはインシデントの届出データからの分析であり、被害が発生したが届出していないケースや、いまだ被害が発覚していないケース（マルウェアが侵入しているが気づいていない場合など）は含まれていないという点にも注意したい。

（3）サイバーセキュリティの定義とセキュリティガイドライン

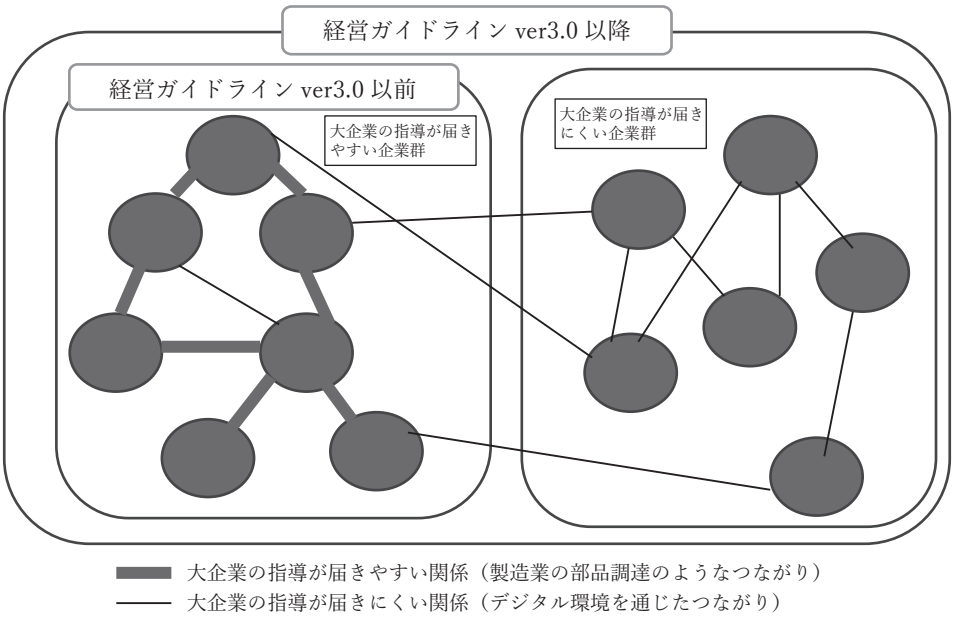
サイバーセキュリティの定義については、サイバーセキュリティ基本法（平成26年法律第104号、以下「基本法」）第2条に記載されている。保護すべきもの（措置対象：①情報、②情報システム、③情報通信ネットワーク）について必要な措置が講じられ、それが適切に維持管理されていることを目的としている。情報のCIA（機密性（Confidentiality）、完全性（Integrity）、可用性（Availability））が守られることや、外部からのサイバー攻撃のみならず、「その他の当該情報の安全管理のために必要な措置」という内部不正に対する対策等も含まれる。

また、基本法の他にガイドラインが作成されている。サイバーセキュリティ経営ガイドラインVer3.0[4]（以下、経営ガイドライン）では、サイバ

3 「令和6年におけるサイバー空間をめぐる脅威の情勢等について」警視庁サイバー警察局（令和7年3月）https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/info_security.files/graph.pdf
4 サイバーセキュリティ経営ガイドラインVer3.0.　経済産業省　IPA　https://www.meti.go.jp/policy/netsecurity/mng_guide.html

ー攻撃の内容の変化に対応して「サプライチェーンには製造業における部品調達のような関係のみならず、外部のデジタルサービスの利用やシステム同士の連携など、デジタル環境を通じた多様かつ非定型の企業間のつながりも含む」と定義し、従来のサプライチェーンの定義を変更している（**図表3**）。デジタル環境を利用している企業は全て対策が必要であるということだ。

（図表3）　サイバーセキュリティ対策が必要な企業



（筆者作成）

中小企業には、サプライチェーンの中で、大企業等取引先の指示・要請によってサイバーセキュリティ対策を実施している企業がある一方、大企業の指導が届きにくい、地域に根差した小規模な個人事業者が多い業界、多様な顧客層に対応する必要がある業界、分散型の事業構造を持つ業界がある。主には理美容業、旅館業、飲食業、小売業などである。これらの中小サービス業は、取引先等からの指示・要請がないことに加え、社内に特許や技術的な内容などの重要な情報が無いという考えや、他社のプラットホーム（決済やデータ管理など）を利用しているため、自社が責任を負うものではないと考えている、というアンケート結果がある。

（4）中小企業のサイバー攻撃対策の状況

中小企業に対して実施した、さまざまなリスクが発生した際の反省点に関するアンケート結果がある（**図表4**）。この調査は、一般社団法人日本損害保険協会が中小企業の自社を取り巻くリスクの認識状況について調査したもので、リスクが発生したと答えた回答者に対し、リスク発生時の反省点を複数回答で聞いている。

（図表4）リスク発生時の反省点など

（n＝リスク発生件数、発生比率は％）

		n	リスクに対する備えが不足していたと思う	被害額がこんなにも高くなるとは思っていなかった	うちの会社ではまさか起こらないと思っていた	現状の対策で十分だろうと思っていた	社内体制を整えられていなかった	社員教育／啓発／研修が不足していたと思う	業務フローにもともと不安を感じていた	業績が順調だったので、リスクに目を向けていなかった	相談できる相手がいなかった	リスク管理の責任者が定まっていなかった	風評被害など、二次的な被害まで想定していなかった	被害により取引先の信頼が落ちたと思う
全体		276	47.8	47.5	39.9	37.7	31.2	29.3	27.5	26.4	26.4	25.7	23.6	23.6
リスク	自然災害	120	45.8	54.2	37.5	35.0	29.2	26.7	21.7	23.3	25.8	27.5	21.7	17.5
	サイバーリスク	45	64.4	53.3	64.4	51.1	48.9	44.4	40.0	48.9	44.4	33.3	46.7	40.0
	経済環境リスク	78	48.7	50.0	35.9	37.2	33.3	28.2	30.8	23.1	28.2	21.8	20.5	20.5
	顧客取引先の廃業や倒産等による売上の減少	101	53.5	49.5	41.6	35.6	27.7	25.7	30.7	24.8	30.7	23.8	21.8	23.8
	製造物に関する損害賠償	31	51.6	51.6	45.2	41.9	51.6	61.3	48.4	29.0	29.0	35.5	38.7	32.3
	従業員からの損害賠償請求	10	70.0	40.0	60.0	50.0	70.0	80.0	30.0	40.0	30.0	40.0	60.0	30.0
	勤務中や移動中における損害賠償	37	54.1	51.4	43.2	54.1	45.9	48.6	35.1	32.4	40.5	40.5	32.4	24.3
	知的財産権侵害リスク	8	37.5	62.5	50.0	25.0	37.5	25.0	50.0	12.5	50.0	25.0	37.5	37.5
	人材流出リスク	41	48.8	43.9	43.9	39.0	46.3	41.5	41.5	31.7	24.4	24.4	31.7	29.3
	その他	15	40.0	26.7	20.0	33.3	6.7	13.3	13.3	13.3	13.3	6.7	13.3	13.3

（出典）「中小企業におけるリスク意識・対策実態調査2024調査結果報告書2025年3月」一般社団法人日本損害保険協会
https://www.sonpo.or.jp/sme_insurance/assets/pdf/sme_report2024.pdf

サイバーリスクに関しては、「うちの会社では、まさか起こらないと思っていた」が64.4%、「現状の対策で十分だろうと思っていた」51.1%など、総じて他のリスクより高い数値となっている。これは、サイバーインシデントの発生が多くなっているにも関わらず、対策を取ろうという意識が低いということである。と同時に、「相談できる相手がいなかった」が44.4%であるなど、リスクとしてうすうす認識してはいたものの、具体的に何をすべきかわからないというのも本音だったと思われる。

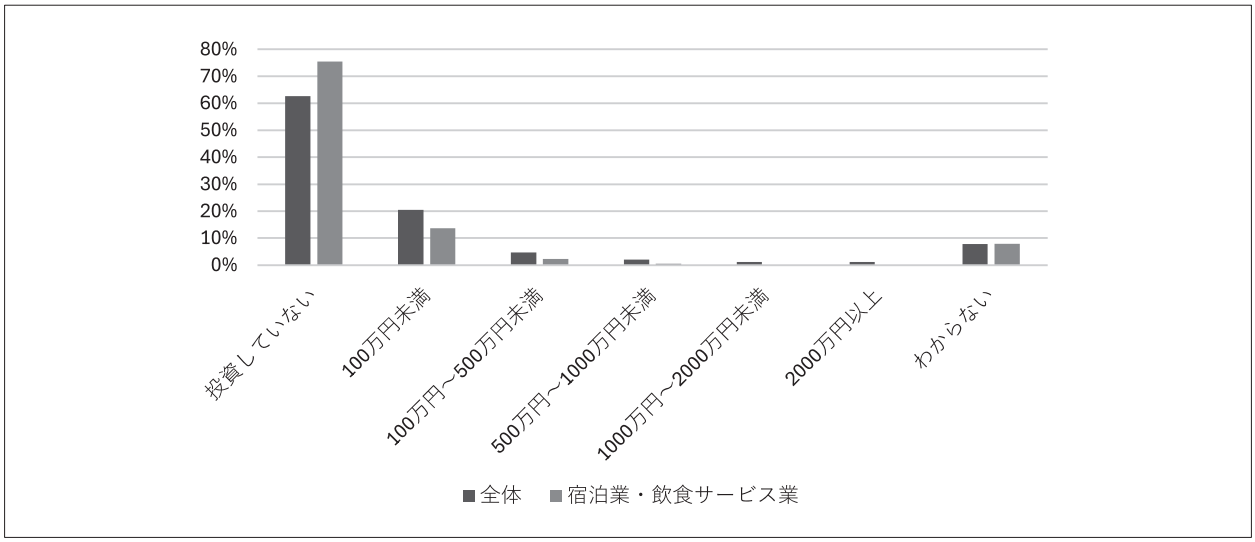
中小企業では、一貫生産し販売まで手掛けている企業は少ない。従って、大企業のサプライチェーンに属する製造業においては、大企業からの指導が届きやすい関係にあり、サイバーセキュリティ対策の具体的な指示のもと、対策が進んでいると言えよう。

経営ガイドラインではサイバー攻撃の変化に対応し、サイバーセキュリティ対策が必要な企業の枠を広げ、対策の強化を推奨している。

ここでは中小サービス業の例として、サービス業のうち企業数が一番多い[5]、宿泊業・飲食サービス業の状況を見る。**図表5**は中小企業のIT関連投資額である。中小企業全体ではIT投資をしていない企業が約60%であるのに対し宿泊業･飲食サービス業では70%を超えている。また、いずれの金額層においても、宿泊業・飲食サービス業が全体よりも低い結果になっている。

5　総務省・経済産業省「令和3年経済センサス－活動調査」産業別規模別企業数（民営、非一次産業、2021年）より（2025年版中小企業白書、付属統計資料）　https://www.chusho.meti.go.jp/pamflet/hakusyo/2025/chusho/f1.html

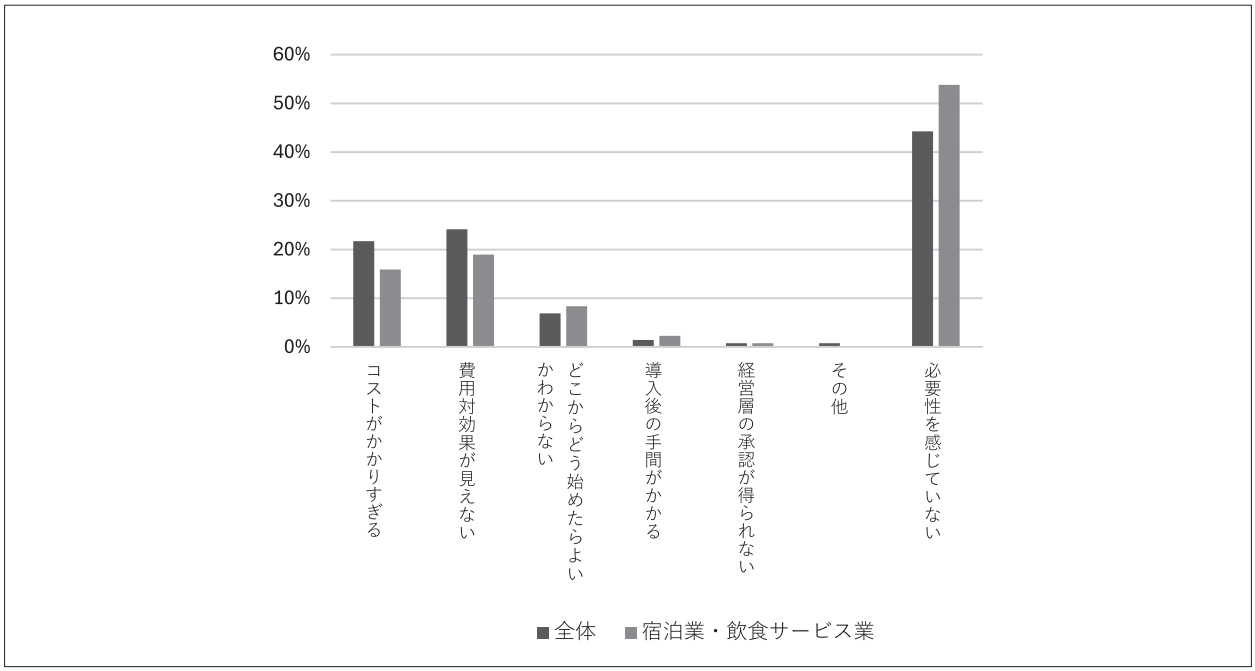
（図表5）情報セキュリティ対策投資額（IT機器や社員への教育等も含む）



（出典）「2024年度中小企業における情報セキュリティ対策に関する実態調査－報告書－」2025年5月独立行政法人情報処理推進機構
https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html
（筆者作成）

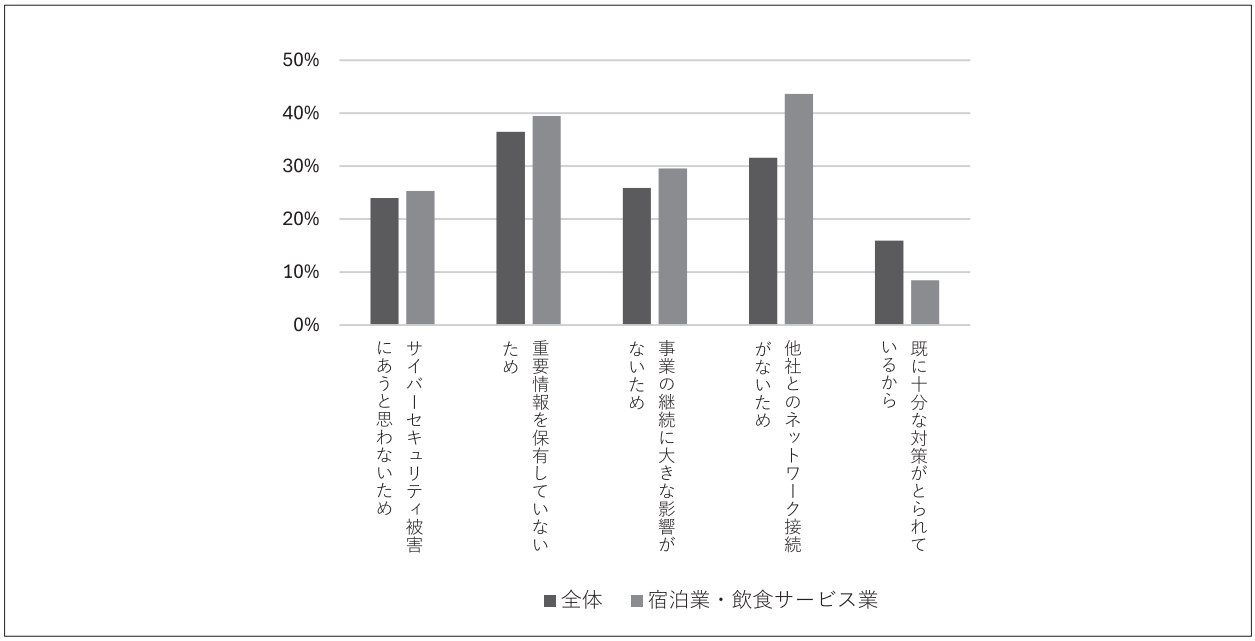
投資していない企業の投資しない理由のうち、「コストがかかりすぎる」「費用対効果が見えない」という理由は全体に比べて宿泊業・飲食サービス業のほうが低い。一方で、「必要性を感じていない」という理由は全体が約44%なのに対し、宿泊業・飲食サービス業は約54%となっている（**図表6**）。

（図表6）投資していない企業の投資しない理由



（出典）「2024年度中小企業における情報セキュリティ対策に関する実態調査－報告書－」2025年5月独立行政法人情報処理推進機構
https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html
（筆者作成）

（図表7）必要性を感じない理由



（出典）「2024年度中小企業における情報セキュリティ対策に関する実態調査－報告書－」2025年5月独立行政法人情報処理推進機構
https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html
（注）「他社とのネットワーク接続がない」とは、販売先（発注元企業）や仕入先（委託・協力企業）のネットワークと直接システムが接続している状況をいう。インターネットを介して他社のシステムを「使用している」ものは含まない。
（筆者作成）

さらに、必要性を感じないと回答した者にその理由を尋ねたところ（**図表7**）、「他社とのネットワーク接続がないため」が全体では約31%に対し、宿泊業・飲食サービス業では約44%となっている。多くの宿泊業・飲食サービス業は、販売先（発注元企業）や仕入先（委託・協力企業）のネットワークと直接システム開発・構築したものを使用していないということであろう。その他に、「重要情報を保有していないため」や「事業の継続に大きな影響がないため」という理由が宿泊業・飲食サービス業では全体よりも高い。一方で、「既に十分な対策がとられているから」という理由は全体のほうが宿泊業・飲食サービス業よりも高い。多くの宿泊業・飲食サービス業はサイバーリスク対策の必要性を感じていないのである。

ところが、サイバー攻撃が時代とともに変化していることを踏まえた対策が必要になっている。もちろん、今も個別企業（組織）に狙いを定めたサイバー攻撃があると思われるが、単純に身代金を要求する「ランサムウェア攻撃」も増加している。こうした攻撃を受けた場合は、自社の業務が停止してしまう。そのため、業務が停止したときのリカバリーや事業継続などを踏まえた対策が必要である。

２．サイバーセキュリティ対策に関する先行研究

(1) 中小企業における対策の遅れ

中小企業におけるサイバーセキュリティ対策の遅れについて指摘する研究は多く、その背景への言及も多い。

佐久間・猪俣（2019）は、中小企業のサイバーセキュリティ対策が遅れている背景に、サイバー攻撃により発生するリスクやその対策、保険商品の内容の不透明さがあるとしている。また、企業規模が小さいほど、社内に情報セキュリティ担当者を置いていないことや情報セキュリティ教育を実施していないことについても指摘している。

田中ほか（2022）は、中小企業がセキュリティ対策を進めていくにあたっては、自組織のセキュリティ対策状況が十分であるかどうかを安価に可視化し、足りない点にどういった機能や対策が必要であるかをわかりやすく提言するような仕組みやサービスが必要である、と指摘している。

竹内(2022)は、中小企業はサイバーセキュリティ対策が必要と感じていても、取り組む優先順位が低いために、対策を実施していないのであり、中小企業がサイバーセキュリティ対策を進めざるを得ないような環境をつくることの必要性を示唆している。具体策として環境整備、動機づけ等を挙げているが、いずれも既に実施されていながらも成果が無いものと認識している。

中小企業のサイバー攻撃対策が進んでいないという実態が、アンケート結果からも見てとれる。大企業が自社のサプライチェーン全体でサイバーセキュリティ対策を行う中で、必要な対策を指示され、それを実行しなければならない企業は既に対策済もしくは対策に着手しているものと筆者は考える。例えば、自動車産業では、自工会／部工会・サイバーセキュリティガイドライン[6]で、企業の規模によらず、必要最低限実施すべき項目などをとりまとめ、公表している。自動車メーカーやサプライチェーンを構成する企業に対するサイバーセキュリティ対策の基準として活用されている。

辰巳（2023）は、サイバー攻撃に備えるためのサイバーセキュリティ投資は、「コスト」ではなく、「財・サービスの価値やブランドイメージを低めないための投資」ととらえるべきだと主張する。

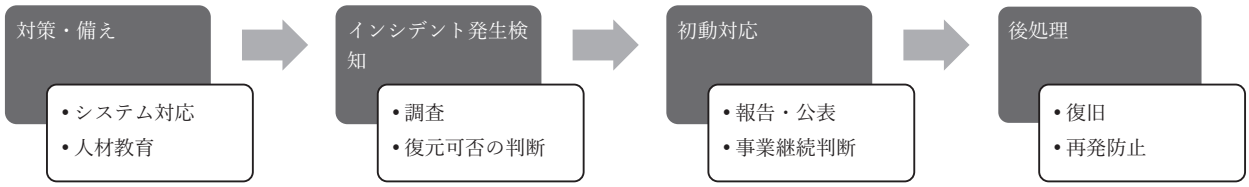
（**図表4**）にある通り、リスク発生時の反省点の中にも、「風評被害など、二次的な被害まで想定していなかった」46.7%や「被害により取引先の信頼が落ちたと思う」40.0%などの回答比率が自然災害や経済環境リスクなど他のリスクと比べて高くなっている。準備をしていなかったことが、財・サービスの価値やブランドイメージを他社のそれよりも低くしてしまうということであろう。だとするならば、中小サービス業である、宿泊業・飲食サービス業のような中小企業も、自社の評価を落とさないために、サイバーセキュリティ対策を行う必要がある。

6　一般社団法人日本自動車工業会HP「自動車産業サイバーセキュリティガイドライン」企業の規模によらずに利用できる必要最低限実施すべき項目に加え、更なるレベルアップ項目を追加したもの　https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html

(2) サイバーセキュリティに必要な対策

サイバー攻撃は受けないこと、受けてもインシデントに至らないことが第一である。しかしながら、近年のサイバー攻撃の進化を考えると、防御しているから安心とは言えない。攻撃を受けた際に、いかに被害を最小限に食い止め、自社の活動を継続できるかに軸足を置く必要がある。

(図表8) サイバー攻撃への対応



(出所) 損保協会HP　https://www.sonpo.or.jp/sme_insurance/cyber-hoken/　を参考に筆者作成

サイバー攻撃への対応は4段階に分かれる。発生前の対策・備え、インシデント発生時の行動、初動対応、そして後処理である(**図表8**)。

対策・備えについては、国家公安委員会ほか(2025)が、不正アクセス行為の認知・検挙状況から、不正アクセス行為の手口をまとめ、対策も記している。パスワードの設定・管理の甘さを起因とした犯行、識別符号(ID・パスワード)を知りうる立場にあった人物による犯行が多いことをあげ、従業員教育(パスワードの管理やフィッシングへの注意喚起)が必要と指摘する。また、日常的にシステムを最新の状態にする(サーバーやアプリケーションプログラムのセキュリティパッチ適用、ソフトウェアのバージョンアップを行う)ことがサイバー攻撃の抑止につながるとしている。さらに、多要素認証[7]の追加も推奨している。

山内ほか(2021)は、事前の備えとして組織間コミュニティ訓練を推奨している。サイバーセキュリティインシデント発生時は、組織内における特定の専門家のみが対応できれば良いものではなく、全員がそれぞれの役割を持った対応をする必要がある。様々な制約下でのシナリオを作成し継続的な訓練をすることがミスコミュニケーションを軽減し、迅速・的確な対応を行うことができるようになる、という。

石川(2023)も医療機関において医療部門、看護部門、事務部門など多職種間でボードゲームを用いた訓練を行うことで、インシデント発生時のそれぞれの行動を確認して置くことは効果的という。これも、組織間での連携がとれるように準備するということである。

但し、山内ほか(2021)、石川(2023)は、いずれもインシデント発生前(準備段階)の訓練で、かつ、それぞれの役割を綿密に作りこんだシナリオを作成していた。中小企業がこれだけの準備・訓練をするのは難しい。発生前の対策(準備)としての従業員教育は、従来からサ

7　多要素認証とは、ユーザーがシステムにログインする際に、知識情報(ID、パスワード)の他に所持情報(スマートフォンやICカードなど)もしくは生体情報(指紋や顔認証など)という異なる認証要素を組み合わせて本人確認を行う方法

イバーセキュリティ対策として言われてきたこと（国家公安委員会ほか（2025）：パスワード管理、ソフトを最新バージョンに更新、怪しいメールは開封しないなど）であり、中小企業でも理解が進んでいる。

また、対策・備えでの留意点という意味で、市瀬ほか（2021）は、サイバー攻撃等の脅威が進化していることを鑑み、脅威は境界外部にのみ存在するので境界内部に侵入しないようにすればよい（「境界防御モデル（ペリメタモデル）」）という考え方から、クラウドやインターネットを利用することで社内と社外の境界線がなくなり、いつ脅威が発生してもおかしくない（「ゼロトラストモデル」）と認識して対応する必要があると指摘する。

木村ほか（2017）は、経営者自身が主体となって、事業継続に影響を及ぼすリスクの洗い出しを行い、「（自社が提供している）サービスの中断」、「データの流出」、「レピュテーションリスク」の3つを意識した行動をとる必要があると指摘する。そして、サイバー攻撃を受けた際のリスクを可視化し、経営判断が可能な体制を作る必要があるとしている。

事後対策として、保険についての言及もある。教学（2021）は、今後企業にサイバー保険が必要になると主張する。多くの日本企業は自社のシステム運用を全面的にシステムベンダーに依存している。既知のサイバー攻撃の場合、これらの攻撃による損失については、システムベンダーにその責任を問うことができるかもしれないが、未知のサイバー攻撃が原因の場合は、不可抗力でもあり、その損失の責任を問うことは難しい、という必要理由を挙げている。

山下（2023）は、IPAが保険とコンサルティングを兼ね備えた形の支援策を提供しており、効果が期待されるとする一方で、中小企業に浸透していないことを指摘し、さらなる対応強化が必要としている。

(3) 先行研究を踏まえて

先行研究では、中小企業のサイバーセキュリティ対策が進んでいない背景として、人材不足、リスクを可視化するサービスが無い、対策推進をコストと認識しているなどの指摘がされている。従って、対策推進にはサイバーセキュリティ対策を進めざるを得ない環境をつくる必要が有るのではないかという意見がある。また、サイバー攻撃による被害を受けないために、企業によるシステム対応や人材教育の必要性に言及している。加えて、サイバー攻撃の進化により、常に新しい種類の攻撃があることから、被害の発生を免れないことを前提として、損失を補うためのサイバー保険加入を推奨している。

大企業の指導のもとにサイバーセキュリティ対策を進めている企業は、サイバーセキュリティ対策を進めざるを得ない環境にあり、リソースの不足やコスト面での負担を理由に後回しにできない状況にあると推測できる。

ところが、実際にサイバーセキュリティ対策が進んでいない、大企業の指導が届きにくい中小サービス業に対して、サイバーセキュリティ対策を進めざるを得ない環境を作り、リソースの不足やコスト面での負担を軽減するための方策を提供すれば、サイバーセキュリティ対策が促進されるというが、どのように中小企業に届けるのかについて言及するものは少ない。

本稿では、サイバーセキュリティ対策をより多くの中小企業に届けるにはどのような方策や体制が望ましいのかについて明らかにする。そのうえで、中小サービス業の取り組みを踏まえ、どうすればサイバーセキュリティ対策を進めざるを得ない環境になるのか、また、リソースの不足やコスト面での負担軽減の方策として地域の中小企業支援機関のサポート体制として何が有効かを確認する。

3．事例紹介

では、サイバーセキュリティ対策を進めざるを得ない環境をつくるには何が必要か、また、リソースの不足や対策推進コストの負担という理由で対策を後回しにしている企業に対してどのような支援が考えられるのか、個別企業（2社）と支援機関（1団体）へのヒアリング調査から明らかにしたい。

個別企業1社はサイバー攻撃により業務に使用するサーバーが停止するなどの被害を受け、その後対応を強化した企業である。サイバー攻撃を受けたことで、サイバーセキュリティ対策を強化せざるを得ない状況になった企業のその後の対応を確認した。もう1社はDXの強化に取り組む中でサイバーセキュリティ対策も進めている企業である。当社では、社内のIT人材がDX推進・管理とサイバーセキュリティ対策のバランスを取って進めており、自社の状況に合わせて、どのような水準までサイバーセキュリティ対策をするのかなどの考え方について確認した。また、地域の中小企業にサイバーセキュリティ対策を導入するサポートをしている組織がそのサポート体制をどのように構築したのかを確認した。

(1) サイバー攻撃により被害が発生し、その後対策を強化した事例

組合名	静岡給食協同組合　静岡給食センター
設立	1963年9月設立
代表者	代表理事　岩井泰次郎 （日本レーベル印刷㈱代表取締役社長）
出資金	78,762千円
事業内容	事業所向け弁当製造・配達（日替り弁当、幼稚園弁当、仕出し弁当）、各施設などの業務受託、食品の受託加工製造、冷凍事業
所在地	静岡県静岡市
組合員	342事業所
従業員数	216名

（注）静岡給食協同組合管理部長野崎雅代氏に2025年6月12日にインタビュー実施
（出所）静岡給食協同組合HP（https://sq-lanch.com/about/）2025年8月1日閲覧

静岡給食協同組合（以下、組合）は、静岡機械金属工業団地内の企業を中心に弁当を届ける給食事業を行っている。また、社員食堂などの外部施設での調理作業の受託も行っている。企業からの弁当の注文は、HP上からの直接入力の他、FAX・電話でも受付している。FAX・電話の分は組合でシステムに入力している。

ランサムウェアに侵入されるというサイバー攻撃を受けたのは、2021年2月8日（月）であった。早朝7:00頃に出社してくる栄養士がPCで作業用ファイルを開こうとしたところ、開けない状態になっていた。野崎管理部長が基幹サーバーのモニターを確認し、いつもと違う、おかしいと感じたため、基幹サーバーのベンダー企業A社に連絡を試みた。だが、ベンダーの保守メンテナンスは平日9:00－17:00であり、連絡が取れない状態であった。組合には基幹サーバーとは別にデータを保管しているサーバーがあり、こちらのサーバーのベンダー企業B社の担当者C氏に連絡し状況を説明すると、基幹サーバーがウイルスに侵入されていることが

判明。そこで、C氏から初期対応について説明され、その通りに野崎管理部長が組合内で指示をした（具体的には無線WIFI・有線のLANを外す、外部にあるPCは利用しないなど）。

当日の給食の注文連絡は、PCでの作業ができず、顧客情報の確認と給食注文内容の入力ができない状態であった。野崎管理部長は顧客の信頼を損なわないためにも事業継続が第一と判断し、配達担当者に対して、電話・FAXで連絡があったものなど、確認伝票を手修正して対応するという指示を出した。そして、混乱が予想されるため、給食を多めに作り、配達担当は配達車に多めに積み込み、先方に届ける際に給食の数を確認して置いてくる、という体制で臨んだ。

一方、当日の業務運営と並行して、サーバーの回復のための対応も急がれた。9:00に基幹サーバーのサポート担当に連絡がついたが、既に事務所内は大混乱となっていた。組合は基幹サーバーのSEと組合の役員ならびに事務局長、野崎管理部長で翌日以降の営業、今後の対策や方針を検討した。業務の継続が第一であるという結論から、具体的な行動が決まっていった。

ランサムウェアに感染していたサーバーには、社内の共有ファイルが入っており、データはすべて暗号化されていた。その下に2つのシステムがついていたが、こちらは別のパスワードを使っていたため、顧客情報が入っていたシステムは感染しておらず、そちらは動かすことができた。また、クラウド上のバックアップからデータを戻すことができた。

当日を乗り越えた後の処理も困難であった。日常業務の正常化のため、社内の共有ファイルが消失したため、毎日使うエクセルシートなどを緊急性の高いものから作り直すのに残業で対応した。復旧までに1か月程度要した。

システム面での対応も必要になった。ランサムウェアに感染した経路は当社が当時使用していたUTM[8]ではログを追い切れず、明確な感染経路がわからなかった。なお、事後対応としてセキュリティ強化のために、サーバーやクラウドについての契約の追加・変更や、新たなツールの導入が必要となった。

取引先・顧客への対応も急務であった。取引先や顧客に対しては、翌日には個別に文書でランサムウェアに感染したことを説明した。HP上にも文書同様の説明文を掲載した。電話での照会に対しても文書内容と同様の説明を行った。文書の内容は、「不便や心配をかけていることの『謝罪』」に加えて、①ランサムウェアに感染したこと、②（連絡には）メールを使用せず電話かFAXで連絡してもらいたいこと、③メールが使用できるようになったら改めて連絡すること、に加え、④（被害を拡大させないために）メールを直接担当者に送付しないでもらいたい」とした。当時は「メールによる感染拡大」が気になっていたことや、組合内部でも一時的に「メールの使用を停止していた」ためである。

組合の対応として、①すぐに取引先（仕入先、販売先）に連絡したこと、②取引先側に被害が無かったこと、③個人情報等の情報が漏れることがなかったこと、④初期対応で最低限6台のパソコンが動かせるようになったこと、⑤6台のPCにはクラウドストレージからデータの復旧ができたことなどから、当日以降配達も通常

8　UTM（Unified Threat Management：統合脅威管理）とは、企業のネットワークを守るために、必要な機能を一台で提供する製品。

通り行うことができた。

後日談になるが、当日朝、ランサムウェア感染かどうか明確になっていな段階で、早期にネットワーク遮断を行ったので、被害が拡大しなかった。組合ではサーバーを複数使用しており、「顧客リスト」に該当するものを保管しているものについては、「被害（流出・暗号化）」が無く、被害発生翌日から業務継続体制を整える行動ができたことが幸いであった。

被害発生翌日朝、ランサムウェアに感染したサーバーには、モニターに英文で「BITCOINで日本円で2千万円相当額を支払え」という指示がでたが、ベンダーから「身代金を支払うことは犯罪に加担することになる」と言われたこと、顧客リストが流出していないこと、業務継続ができたこと、から支払うことはなかった。

この時の被害を受けた後、サイバーセキュリティに対する職員の意識は高くなった。組合は、この後、インターネット上での不正アクセスへの対応として、ID・パスワードのログが残るようにしている。

また、職員に対する定期的な研修が必要と再認識した。事務所の職員は全員受講するものとし、現場でもPCでの作業が始まったので、順次研修で意識向上を図っている。

サイバー攻撃の被害の教訓の一つに、事象が発生したときの費用も考慮しておく必要がある。本件では、200万円程度の費用が発生した。サイバー攻撃の被害に遭っている中では、システムの復旧や対策についていちいち相見積もりを取って対応するということはできない。この時も、リカバリーが最優先で、費用について考えている余裕はなかった。復旧のための残業代も予定外に発生した。

その後、組合が静岡県中小企業団体中央会にサイバー攻撃への対応策を相談したところ、「サイバーセキュリティ対策保険」の紹介があり、加入した（保険料は年6－7万円で、サイバー攻撃を受けた際に必要な費用をカバーするもの）。保険に入っているというだけでも安心感がある。この保険は、事象発生時に24時間365日対応しており、使用しているサーバーやPCがウイルスに感染しているかどうか確認する初期対応費用もカバーしている。必要費用の中には、身代金は含まないが、残業代、サーバーやPCの代替費用なども含まれている[9]。

このケースでは、ランサムウェア攻撃による想定外の事象の発生に対し、総務担当者の臨機応変の判断と、その指示のもと異例事務に対応した現場の職員の働きが大きかった。まさに、異例事務対応については人材育成ができていたということである。事業継続判断や「取引先企業への報告・公表」が早かったことも、取引先に評価された。サイバー攻撃に対する対応マニュアルは無かったが、現場が迅速に誠実に対応したことで、その後の評価も上がっている。

組合は、外部のITベンダーを通じてサーバーの管理やPCの導入などを行っており、サーバーやシステムなどはITベンダーに任せていれば問題ないとの認識から、組合として特にサイバーセキュリティ対策を行っていなかった。

組合は、サイバー攻撃の被害に遭ったことで、サイバーセキュリティ対策を進めざるを得ない環境となり、リソース不足、コスト負担の観点で

9　全国中小企業団体中央会提供「サイバー保険制度」 https://www.chuokai.or.jp/index.php/supportservice/insurance/privacy/

事前の予防には限界があるので、人材育成、保険など発生時の対応力やリカバリーとしての保険など事後対応に重点を置いた対応を行った。

(2) サイバーセキュリティを含めたDXの強化に取り組んでいる事例

社名	株式会社ホテルおかだ
設立	1953年設立
代表者	代表取締役社長　岡田茂幸
資本金	4,930万円
事業内容	宿泊業（温泉旅館）
所在地	神奈川県足柄下郡箱根町
従業員数	120名（2024年12月現在）

（注）常務取締役営業本部長原洋平氏に2025年5月29日にインタビュー実施
（出所）株式会社ホテルおかだHP（https://www.hotel-okada.co.jp/concept/）2025年8月4日閲覧

株式会社ホテルおかだ（以下、ホテルおかだ）は5本の自家源泉を持つ箱根湯本の老舗温泉である。東京から電車で75分という好アクセスに位置する箱根で、客室数122室、露天風呂付客室、内湯・露天風呂などの設備を備えており、家族・カップル・団体など、さまざまなグループのニーズに合わせることができる施設となっている。また、グループ内の施設には日帰り温泉もある。

ホテルおかだの原洋平常務は、IT企業での勤務経験があることを自らの強味の一つとしており、現在は社内で使用しているシステムの管理、新しいシステムの導入、システムの活用方法の従業員への周知、などを行っている。また、2024年（令和6年）6月に、日本旅館協会のEC/DX委員会の委員長に就任し、業界全体の取り組みも進めている。

令和6年度に実施された環境庁の「観光DXにおける生成AIの適切かつ効果的な活用に関する調査事業[10]」における課題解決へのAI活用の実証実験にも協力した。この実験では、生成AIを活用した「業務効率化」や「経営の高度化」を主眼としている。

ホテルおかだでは、当該実証実験の中で、生成AIを導入した「社内のノウハウやマニュアルを活用した自動回答」、「予約状況・予測データを活用した従業員シフト最適化」、「顧客データの一元化・要約による最適な接客業務の実施」、「口コミ分析による宿泊プランの改善」という課題に対する取り組みを行った。この取り組みにより、例えば社内のノウハウやマニュアルを生成AIで迅速に回答し、問い合わせ対応の効率化と情報検索時間の短縮が大きく進んだ。その他の課題に対しても、生成AIで対応することで、情報が瞬時に整理され、判断業務を行う際の時間短縮につながっている。さらに、口コミ分析では生成AIを活用することで膨大な情報の中から具体的な課題を抽出することが可能となり、従来の経験や勘に頼った判断では見落とされがちだった改善点を見つけることが可能となった。

実証実験では、生成AIでデータを活用するために生成AIが学習するためのデータを読み込ませる必要があった。その際にも、個人情報やその他重要な情報が外部に流出することが無いよう、扱うデータの内容や範囲を明確化するなどの対策を行った。

原常務は、一般論として、「システムベンダーは、製品を紹介する際に『セキュリティ対策』

10　観光庁は令和6年度「観光DXにおける生成AIの適切かつ効果的な活用に関する調査事業」にて、「観光DXにおける生成AIの適切かつ効果的な活用に関する調査」を実施。ホテルおかだは「生成AIの効果的な活用に係る実証実験」に参加した。環境庁HP　https://www.mlit.go.jp/kankocho/content/001889635.pdf　2025年8月5日閲覧

そのものを前面に出すことは少なく、むしろ『業務効率化』や『顧客情報の活用』といった利点を強調する。その中で『導入すれば結果的にセキュリティも強化できる』という説明がなされることが多い。企業側も効率化や高度化に意識が向きやすく、セキュリティはベンダーに任せきりになってしまう傾向がある。」という。

原常務はIT関連知識を持ち、ベンダーと対等に話ができるため、「営業推進」や「効率化」の観点からのIT導入やDX化の際にも、セキュリティの観点からの確認を欠かすことなく行っている。

中小企業においては自社の環境を把握し、優先順位をつけて対策を取る必要がある。生産管理を行う製造業と旅館業では、扱うデータが違うし、セキュリティの考え方が違う。ホテルおかだでは、社内データ、特に個人情報が含まれるデータは従業員のうちでもごく限られたメンバーしか取り扱うことができない体制を敷いている。さらに、何かあった場合に、どこに相談（連絡）すれば良いかを把握し行動に移せるように教育している。

システム活用に関しては、便利さとセキュリティのバランスを考えられる人物が経営層にいると良いが、中小企業の場合、常にITに詳しい人物が社内にいるとは限らない。筆者は、原常務というITに詳しい人物が社内のそれも経営層に存在することが、自社の経営方針に合ったIT化やDXの推進に寄与していると考える。なお、ホテルおかだでは、システム導入時点での状態を、経営層が関与して継続的に微修正しており、自社に適した形にアップグレードできる体制になっている。

ホテルおかだは、サイバー攻撃を受けたとしても、重要な情報は従業員のアクセス制限を設けるなどにより、被害を受けないようにデータを隔離している。旅館業の業務内容は、予約システム、決済システムなど他社のシステムを使用することも多い。他社のシステムが原因のリスクは他社のシステムの責任である。しかしながら、当該旅館を利用するお客様がシステムの不稼働により被害を受ければ、どうしても面前で対応しているホテルスタッフに負荷がかかるし、風評被害につながる恐れがある。被害に遭わないことが第一だが、人材育成により被害を最小限に抑える対応ができることも大切である。

また、原常務からは、それぞれの業界が最低限対応する必要がある項目が明示されると対応しやすいのではないかという示唆があった。

確かに、旅館業が実施するサイバーセキュリティ対策のスタンダードな基準があれば、業界に属する企業が「まずそこから対処しよう」という行動をとると思われる。リソースの不足やコスト面での負担があったとしても、最低限の基準を満たすことが優先され、業界としてサイバーセキュリティ対策が進むのではないか。

ITに精通した人材が社内にいることで、ホテルおかだは自社に即したサイバーセキュリティ対策を実施することが可能となっている。IT人材が社内にいない企業は、「最低限の基準」を認識することもなく、もしくは認識していてもリソースの不足やコスト面から対応が困難になっているのではないだろうか。

(3) サイバーセキュリティ対策導入サポート提供に取り組んでいる事例

組織名	名古屋商工会議所
設立	1881年
代表者	会頭　嶋尾正（大同特殊鋼㈱相談役）
事業内容	名古屋市内（守山区、鳴海・有松地区を除く）の事業者を会員とする民間総合経済団体で、経営支援、会員支援、政策提言、地域振興を行う
所在地	愛知県名古屋市
会員数	約17,400社
事務局	約150名

（注）名古屋商工会議所（中小企業相談所）創業・専門相談ユニット　ユニット長織田浩氏、同　創業・専門相談担当係長田中利直氏に2025年7月3日にインタビュー実施
（出所）名古屋商工会議所HP（https://www.nagoya-cci.or.jp/index.html）2025年8月6日閲覧

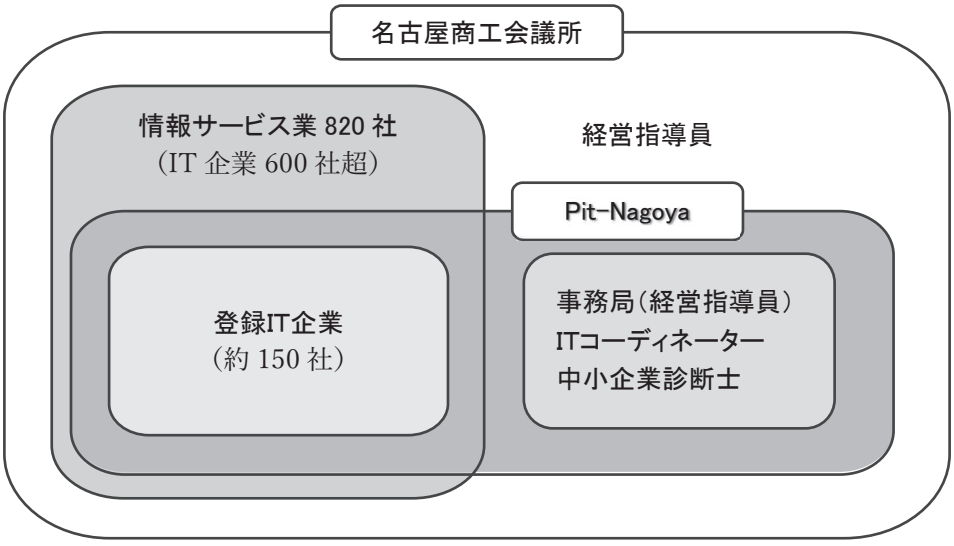
組織名	Pit-Nagoya（ピットナゴヤ）
設立	2019年10月
構成	名古屋商工会議所会員IT企業150社（2025年7月1日現在）
事業内容	事業者に対する無料IT相談、IT事業者とのマッチング支援、サイバーセキュリティサービスの提供、先進事例の紹介、会員相互交流（アライアンス促進）、他地域との連携
所在地	愛知県名古屋市（名古屋商工会議所内）
事務局	名古屋商工会議所、㈱日立システムズ、NTT西日本㈱

（出所）Pit-Nagoya HP（https://pit-n.nagoya-cci.or.jp/）2025年8月6日閲覧

Pit-Nagoyaは名古屋地域のIT企業（登録ベンダー150社）が連携し、中小企業向けサービスを強化・展開するために設立されたコンソーシアムで、名古屋商工会議所（以下、商工会議所）会員のIT企業により組織され、事例共有や勉強会、サービス連携のための基盤を整えることを目的とした活動をしている。それぞれの活動は商工会議所が主催しており、主導的な立場で運営している。事務局は商工会議所の中小企業部内に設置されている（**図表9**）。

従前より商工会議所の経営指導員に対し、会員の中小企業から、業務効率化やデジタル化の必要性が高まる中で、「IT導入の方法がわからない」、「自社の課題に合ったITツールを知りたい」といった悩みや要請が多く寄せられていた。Pit-Nagoyaは、これらのニーズや課題に応える形で、地域のIT企業が連携し、実践的な支援体制を構築するために設立されたという経緯がある。

（図表9）Pit-Nagoyaの体制



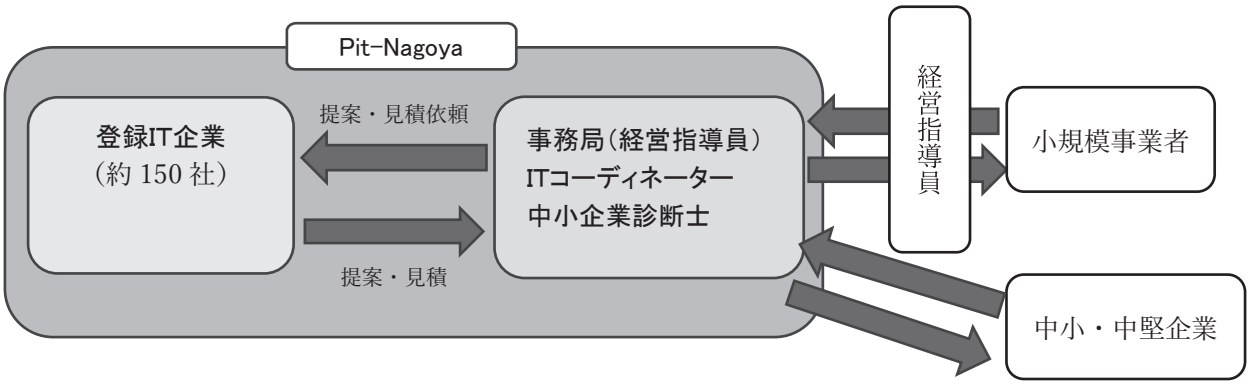
（筆者作成）

名古屋は全国有数の製造業集積地であり、サプライチェーン全体のリスク管理が重視されているため、取引先企業からの要請・発注条件として、サイバーセキュリティ対策が求められるケースが増えている。日本自動車工業会・日本自動車部品工業会による「自動車産業サイバーセキュリティガイドライン」[11]でも、発注側企業が受注側に対策レベルを提示し、実施状況を確認する仕組みが定着しつつあるようだ。この対策の中では、マルウェア侵入のリスク管理、ネットワーク分離、脆弱性診断、アクセス制御などの技術的対策も進められており、サプライチェーン全体での底上げが図られている。

一方、中小企業の中でも大企業への依存度が低く、大企業の指導が届きにくい企業においてはセキュリティ対策の浸透度にばらつきがあり、十分な対策がとられていない企業も少なくない。特に、経営層の関与や社内ルールの整備、ソフトウェアの最新化、ウイルス対策など、基本的な対策が十分ではないケースが多い。

Pit-Nagoyaでは、公式サイト上でIT企業の検索ができるだけでなく、ITコーディネーター[12]や中小企業診断士、(Pit-Nagoya)事務局が相談内容をヒアリングし、課題に応じてIT企業やサービスを紹介･マッチングしている(**図表10**)。ポイントは、ITと経営の両方を理解し調整できる人が対応するという点である。中小企業は予算制約がある場合も多い。その場合にはどの程度までシステムを導入するのかなどの相談にも対応している。

(図表10) Pit-Nagoyaのマッチング体制



(筆者作成)

企業はITを推進したいと考えてはいるものの、IT企業との接点がなく、また、ITに疎い場合は、IT企業の説明内容が理解できない。Pit-Nagoyaの経営指導員も当初は、企業からの相談内容をIT企業に伝えて相談したが、うまく伝えることができなかった。そこで、ITコーディネーターを導入し、経営指導員と同行してヒアリングを行い、企業のニーズをまとめてIT企業に説明し、ギャップを埋めていった。現在は、企業のニーズをPit-Nagoyaの事務局が整

11 「自動車産業サイバーセキュリティガイドライン」https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html
当該ガイドラインページに「自工会／部工会・サイバーセキュリティガイドライン」が添付されている。
12 ITコーディネーターとは、ITコーディネータ協会が認定する民間資格で、経済産業省が推奨している。

理し、会員150社に展開する。うち10社の提案を企業側に提示し、相談企業の希望に応じ、それぞれの違いやメリット・デメリットもITコーディネーターが説明することとしている。

IT企業側も、自社の広告や相談会・説明会などでPRをしているが、それだけでは取引に結びつけることは難しい。Pit-Nagoyaでは、企業側にニーズや課題があり、それを解決したいというところからのスタートなので、やりがいのある仕事ができると言っている。

中小企業の場合、IT推進は「売上向上」、「業務の効率化」が第一で、セキュリティ対策は劣後になる。システム導入時にセキュリティ対策も含めた対応になるように指導している。

Pit-Nagoyaは東海3県の企業であれば、会員非会員問わず利用できる。地域全体のDXが進むことが大切である。同時に、Pit-Nagoyaは150社のIT企業に支えてもらっているので、利用者が増えることが、IT企業にとってのビジネスチャンスとなる。

最近の特徴的なサイバー攻撃では、ランサムウェアによる被害が増えている。名古屋地区では自動車部品サプライヤーや物流を担う港湾関連企業が攻撃を受けている。ランサムウェアの場合、企業規模や業種を問わず、「脆弱性のある企業が狙われる」というのが現在の傾向であり、全企業が例外なくターゲットとなりうる状況にある。

事業会社において、IT人材を社内に配置できれば、事業の競争力強化や業務効率化、セキュリティ対策の観点から極めて有効である。このような社内でのIT推進を支える人材は、採用からその後の育成・定着など、中小企業にとって重要なテーマとなっている。Pit-Nagoyaでは、ITパスポート試験対策講座やデジタル人材育成プログラムの案内など、地域の中小企業が社内IT人材を育てるための支援策を提供・紹介している。

一方で、中小企業にとってIT人材の確保・定着には課題も多い。従って、自社でIT人材を抱えることが難しい場合、Pit-Nagoyaが提供するIT企業とのマッチングを活用することで、外部の専門家と協力しながらIT活用を進めることができる。

業務効率化やDX推進への関心の高まり（IT導入補助金制度[13]拡充内容への関心）などから、IT導入への問い合わせは増加傾向にある。

Pit-Nagoyaでは、「情報セキュリティ対策サービス」の一環として、サイバーリスク保険（サイバーセキュリティ保険）を含んだセキュリティサービス（Pit-Nagoyaセキュリティ[14]）を提供している。このサービスは商工会議所の会員企業を対象に、セキュリティ機器の設置や24時間365日の運用監視、ウイルス駆除などのサポートに、万が一の情報漏えいやサイバー攻撃による損害賠償・費用負担を補償する保険を付帯したものである。

サイバーセキュリティ保険自体は「攻撃を未然に防ぐ」機能はないが、保険加入の条件として一定のセキュリティ対策や診断が求められる

13　IT導入補助金制度2025において、補助対象経費の拡充（導入時の費用の他、導入後のIT活用定着を促す支援にかかる費用も補助対象）、補助上限額の引き上げ（セキュリティ対策推進枠の補助上限額：100万円⇒150万円）などの拡充策がとられた。詳しくは中小企業庁HP参照　https://www.chusho.meti.go.jp/koukai/yosan/r7/r6_it_summary.pdf

14　中小・小規模事業者が導入しやすい低価格のセキュリティ対策パック。①UTMによりネットワークの出入り口で不正アクセスやサイバー攻撃を防御、②運用管理サポート、③サイバーリスク保険がセットになっている。

場合が多く、企業のセキュリティ水準向上のきっかけになるという役割がある。Pit-Nagoyaのサービスには、セキュリティ機器の導入、運用管理サポートがセットになっており、日常的なリスク低減に寄与している。

サイバー攻撃は完全に防ぐことは難しいため、事後対策として保険を活用することが現実的なリスクマネジメントになる。具体的には、情報漏えいやサイバー攻撃による損害賠償、原因調査費用、などの幅広い補償が受けられる。事故発生後の早期復旧や、取引先・顧客への対応、社会的信用の維持など、経営被害の最小化に有効である。但し、日本ではランサムウェア被害の身代金は補償に含まれていない。

なお、Pit-Nagoyaセキュリティに含まれる保証額は少額のため、自社の想定被害額などを勘案の上、保険の上乗せを検討することも可能。商工会議所は損保各社と連携し、会員用の保険商品を提供している。

Pit-Nagoyaの取り組みは、企業がIT導入やDXを進める際にサイバーセキュリティ面での対応を含めた対策を提供するもので、IT導入やDXを進める際にはサイバーセキュリティ対策を進めざるを得ない環境となっている。また、IT人材が社内にいない中小企業にとって、ITコーディネーターのアドバイスを受けながら、IT企業からの提案を吟味できることは、IT人材不足というリソース面での負担軽減に寄与するものとなっている。また、補助金制度の利用や保険の活用により、対策推進コスト面での負担軽減にも資するものとなっている。そして何よりも、地域の中小企業の支援機関として日頃から接点がある商工会議所という組織だからこそ、地域の中小企業の信頼を得て、相談しやすい体制を作り上げている。

４．企業側のサイバーセキュリティ対策

サイバー攻撃対策を始める際に確認しておきたいのが、誰が何のためにサイバーセキュリティ対策をおこなわなければならないか、である。サイバー攻撃は、国家の重大な脅威となるような、インフラ設備等への攻撃を目的としていた。ところが、それが民間企業への攻撃、さらには大企業を標的とした攻撃から中小企業に対する攻撃に対象が変化してきている。つまり、いまだサイバーセキュリティ対策を取っていない企業は、サイバー攻撃を受けるのは、国家的なプロジェクトや大企業とそのサプライチェーンに存在する企業であり、大企業の指導が届きにくい企業の場合は、自分ごととして考えていないケースが多いのではないか。攻撃の内容が標的型から身代金請求型に変わってきたということは、自らがサイバー攻撃を受けたときには、自ら対応しなければいけないということである。

先行研究やガイドラインはサイバー攻撃による被害を発生させないための対策に言及するものが多い。しかしながら、経営資源が限られた中小企業にとって、システムが止まり、一時的にでも事業が継続できない場合の営業損失や、個人情報を含むような情報漏えいが発生した場合の損害賠償金の支払い、ウイルス感染したサーバーやPCの入替・代替品購入などの費用の負担は大きい。加えて、システム内のデータがバックアップから復旧できない場合の手作業による復元などに従業員が対応した場合は残業代もかかる。これらを念頭に、サイバーセキュ

リティ対策を進める必要がある。

(1) IPAによる取り組み

IPAは2016年に「中小企業の情報セキュリティ対策ガイドライン[15]（以下、ガイドライン）」を公開した。現在はテレワークの普及やDX推進という社会動向の変化を踏まえた対応を盛り込んだ第3.1版にバージョンアップしている。また、「中小企業のためのセキュリティインシデント対応の手引き」も付録として追加されている。

IPAは、中小企業に対するサイバー攻撃への対処として「サイバーセキュリティお助け隊サービス[16]（以下、お助け隊サービス）制度」を運営している。お助け隊サービスは「見守り」、「駆付け」、「簡易サイバー保険」などの中小企業にとって不可欠なサービスをワンパッケージとして民間事業者が提供するものであり、安価に利用できる。IT導入補助金制度を利用することで、お助け隊利用料（最大2年分（上限150万円、補助率1/2－2/3（企業規模による））の補助を受けることができる。

IPAによるサイバー攻撃への対処策はお助け隊サービスに登録した民間事業者が提供するものであり、個別企業がサイバーセキュリティ対策の相談をしてきて初めてサポートができる。お助け隊サービスに登録した企業にヒアリングしたところ、登録してから1件の相談も受けていないという話もあり、中小企業にお助け隊サービスを推進するにはなんらかの工夫が必要ではないだろうか。

(2) 被害を「受けない」ための対策

サイバー攻撃の被害を受けないようにする、もしくは被害を最小限に食い止めるための対策としては、以下のようなものがある。

①社員研修
②IT開発企業（システム担当業者）との連携
③サイバーリスク保険に付帯するサービスの活用

まず、①の社員研修は比較的安価に実施できるものであり、かつ、フィッシングを活用した攻撃も増加していることから、サイバー攻撃をさせないという効果も大きい。ホテルおかだでは、社内データ、特に個人情報を含むデータについては、ごく限られた従業員しか取り扱えないように制限している。また、万一の事態が発生した際にどこへ相談・連絡すべきかを把握し、適切に行動できるよう周知している。中小企業にとって、大切なデータにアクセスできる人数を制限し、そのうえでアクセスできる者に対して十分な研修を行うことは有効だと思われる。また、アクセス制限を実施することで、万が一にも情報漏えいなどが発生した場合には、ログ記録なども限定された人員のものを確認すれば良い。

次に、②のIT開発企業との連携について考えたい。自社で使用しているシステム等を開発した企業やサーバーやシステムの保守を行っている会社と連携し、日頃からサイバー攻撃の新しい手口に対する情報を得ることは重要である。静岡給食の事例では、B社の担当者が早朝から対応し、初動動作のアドバイスを行い、ラ

15 「中小企業の情報セキュリティ対策ガイドライン」 https://www.ipa.go.jp/security/guide/sme/about.html
16 「サイバーセキュリティお助け隊サービス」https://www.ipa.go.jp/security/otasuketai-pr/

ンサムウェア被害を最小限に食い止め、かつ、動かせるPCを特定し、利用できるように復旧した。

さらに、③のサイバーリスク保険に付帯するサービスの活用も効果的である。サイバーリスク保険[17]には、経済的な損害補償をする以外に、リスクに対応する各種サービスが利用可能である。例えば、対策・備えとして「情報・ツール提供サービス」や「ベンチマークレポートサービス」を提供している。これらは、サイバーセキュリティの最新の情報を提供して注意喚起を促すものである。また、「簡易リスク診断サービス」でサイバーリスクによる想定損害額を算出し、被害発生時に必要な資金額を認識することができる。想定損害額を算出して被害を想定すると、必然的に対応策を検討しなければならないと考えるのではないだろうか。加えて、「サイバーソリューションナビ」はサイバー攻撃への対策が必要と認識した企業がどのようなセキュリティ対策をすれば良いか、ソリューションを提供する企業を紹介するというサービスである。これらを活用することで、インシデント発生時のリスク想定を踏まえた「対策・備え」ができる。

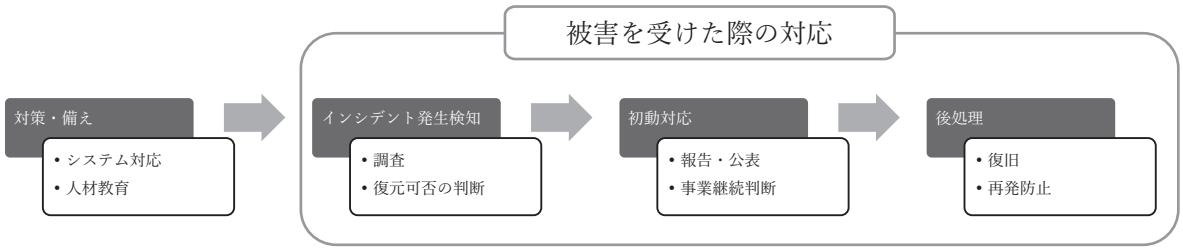
特に②、③は中小企業が自ら意識しないと活用できない。従って、②と③を広く知らしめる動きが必要ではないか。

(3) 被害を「受けた」際の対応と復旧

サイバー攻撃を「受けた」状況は、インシデント発生を検知したところから始まる（**図表11**）。インシデント発生が本当にサイバー攻撃によるものなのか、単純にシステムの不具合によるものなのか、調査が必要である。複数のIT企業に確認したところ、サイバー攻撃を受けたかどうかの確認には、PC1台あたり100万円から150万円程度の費用がかかるという。中小企業にとっては、大きな金額である。

静岡給食のケースでは、緊急事態であり、復旧対応費用は言い値での支払いを行わざるを得なかった。調査や復旧対応はシステム開発を行ったIT企業に依頼するのが一番だが、その際、見積もりをとり、他社と比較しながら対応するのは時間的猶予がない中難しいという問題がある。そこで、静岡給食では、静岡県中小企業団体中央会に相談し、サイバーリスク保険への加入を決定した。

（図表11）サイバー攻撃への対応（被害を受けた際の対応）



（出所）損保協会HP　https://www.sonpo.or.jp/sme_insurance/cyber-hoken/　を参考に筆者作成

17　ここでは、東京海上日動火災保険「サイバーリスク保険」https://www.tokiomarine-nichido.co.jp/hojin/baiseki/cyber/を参考にした

サイバーリスク保険は、サイバーリスクに起因して発生した各種損害を一つの保険で包括的に補償する。対象となる補償とは、①損害賠償責任に関する費用、②サイバーセキュリティ事故対応費用に関する補償、③コンピュータシステム中断に関する補償、である。また、サイバー攻撃の“おそれ”に対応する調査費用、コンピュータシステムの復旧費用、再発防止費用等についても補償する（東京海上日動火災保険「サイバーリスク保険[18]」より）。

火災保険や地震保険など、万が一災害が発生した場合のために、企業は保険に加入している。同様に、サイバー攻撃もいつ、何時、発生するかわからないような時代になっているため、保険は対応策として有効である。

5. サイバーセキュリティ対策を企業に浸透させるには

中小企業がとりうる対策については、IPAのガイドラインの他に、ネット上に多く掲載されている。しかしながら、依然として多くの中小企業がサイバーセキュリティ対策を実施していない、もしくは十分に実施していない状況にある。

(1) 業界ごとのガイドラインの必要性

サイバー攻撃の変化は速いので、個別企業が自社の対策を策定し、それを徹底するにも限界がある。IPAの提供するサイバーセキュリティ対策ガイドラインは、全ての業種に網羅的なものとなっており、個別企業の事情に合わせたものにはなっていない。自社で優先順位を決めて対応すればよいとの記載はあるが、優先順位を決めるという作業も中小企業には負担である。

中小企業にとって、業界のガイドラインが存在すれば、ガイドラインに即した対応をしようと考える企業が増えるのではないか。業界ごとに、守らなければならないデータの種類が違っていたり、社員全員が全てのデータにアクセスする必要が無い場合がある。データを使用するシステムについても、他社と直接接続されているもの、インターネットにはつながっているが自社単独で使用しているもの、全くインターネットなどに接続していない、など、ある程度業界ごとに差があると思われる。

一般社団法人日本自動車工業会（以下、自工会）では、国に先行する形でサプライチェーンのサイバーセキュリティ対策[19]に段階を設け、サプライチェーンの企業に対応を指示している。経済産業省においても、サプライチェーン強化に向けたセキュリティ対策評価制度の構築に向けて取り組みを進めている[20]（具体的にはセキュリティ対策の段階において、第三者評価を採り入れ、認証段階に応じ星の数で評価結果を見える化するもの）。これによると、第三者評価機関を設置し、評価機関で評価を行う者の資格制度を作り、資格認定機関を設けるなど、評価体制を確立したいと考えているようだ。

大企業の指導が届きやすい企業の対策が進む中、中小サービス業のような大企業の指導が届きにくい企業のサイバーセキュリティ対策を

18　東京海上日動火災保険「サイバーリスク保険」https://www.tokiomarine-nichido.co.jp/hojin/baiseki/cyber/
19　一般社団法人日本自動車工業会HP「サイバーセキュリティガイドライン最新情報」 https://www.japia.or.jp/work/ict/cybersecurity-newest
20　経済産業省「サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ（概要）」サプライチェーン強化に向けたセキュリティ対策評価制度に関するサブワーキンググループ事務局　2025年4月14日
https://www.nisc.go.jp/pdf/council/wg_supply_chain/outline_of_interim_report.pdf

進めるために、業界ごとのサイバーセキュリティ対策ガイドラインの作成は有効と思われる。IPAの指針では、記載されている対応策の中から自社に必要な対応を、優先順位を決めて実施すれば良いとされているが、その判断をする社内のIT人材がいない企業の場合、業界ごとのガイドラインで示された内容がわかれば、自社だけが遅れを取ることはできず、横並びでの対応が必要という認識を持つと思われる。

経済産業省などの政府機関が、各業界で必要な認証段階を明確にするなどの対策も有効ではないか。

(2) サイバー保険を活用した想定被害額および自社のリスクの認識

サイバー攻撃に遭った際に必要となる費用をあらかじめ想定しておくことも、サイバーセキュリティ意識を高めるために重要である。

例えば、フォレンジック調査[21]ではPC1台で約150万円かかる、となると、インシデントが発生した際に、どの程度の支出が発生するのか、それらの費用を捻出することができるのかなど、経営者が判断しなければならないことは多い。

また、被害からの復旧対応費用として、従業員の残業代なども含めて考える必要がある。このような費用負担に対しては、サイバーリスク保険に加入することが有効であろう。

例えば、東京海上日動火災保険のサイバーリスク総合支援サービスには「簡易リスク診断サービス」がある。想定最大損失額を算出して被害を想定すると、必然的に対応策を検討しなければならないと考えるのではないだろうか。

サイバー攻撃への対応は自然災害などが発生した際のBCPと同様である。発生する確率は「低い」かもしれないが、損失額が「大きい」ものとして、「自然災害（地震など）」「火災」「自動車事故」があり、「保険」でカバーしている。サイバー攻撃も発生する確率は「低い」が、被害額は大きい。従って、「保険」でカバーすることも選択肢の一つである。

加えて、サイバー保険の付帯サービスで出来ることを、より多くの企業に周知させることが、サイバーセキュリティ対策浸透手段の一つになりうると考える。

なお、保険でカバーできないものとして、「報告・公表の実施判断」や「経営層による事業継続判断」という企業の判断を伴う対応がある。これらは人材育成や研修を通しての備えとなる。その際に、インシデント発生検知時の調査や代替手段の確保に保険を活用することができるという安心感があれば、調査や判断を速やかに行うことができ、「報告・公表」などの初動対応を速やかに行うことが可能となる。

(3) 社内の人材育成の限界と外部人材の活用

中小企業のサイバーセキュリティ対策では、人材育成も重要なポイントである。パスワード管理や不審なメールは開封しないなどの基本的な行動が大切なことは言うまでもない。併せて、「インシデントが発生したのかどうか」に気付くような、気配り・目配りができるような従業員に育成することが大切である。

21 フォレンジック（forensic）とは事件の証拠収集・解析を行うことで、事実関係を明らかにする犯罪捜査の手法の一つ。一般企業においては、サイバー攻撃や内部不正によるデータ改ざん・情報漏えい事故などの実態把握、原因究明に利用される調査・分析技術を指す。

現在のサイバー空間内の動きは日進月歩で進んでいるため、守るだけではなく、インシデントが発生したときの、リカバリーする体制も重要である。中小企業にとって、ITに詳しく、サイバー攻撃を受けたときに素早くリカバリーするために行動できる人材を社内で育成することは難しい。また、ITに対応するだけのために人材を確保するコストを負担することも難しい。そこで、中小企業は、IT企業と連携した対応を行ってはどうか。通常、システム導入時に対応したIT企業が保守も行っている場合が多いので、当該企業に依頼すると良い。Pit-Nagoyaのように、システム導入する際に相談できる外部機関があれば、自社にとって必要十分なIT企業の紹介を受けることが可能と思われる。中立的に対応する専門家がいることは、中小企業のサイバーセキュリティ対策に資すると思われる。

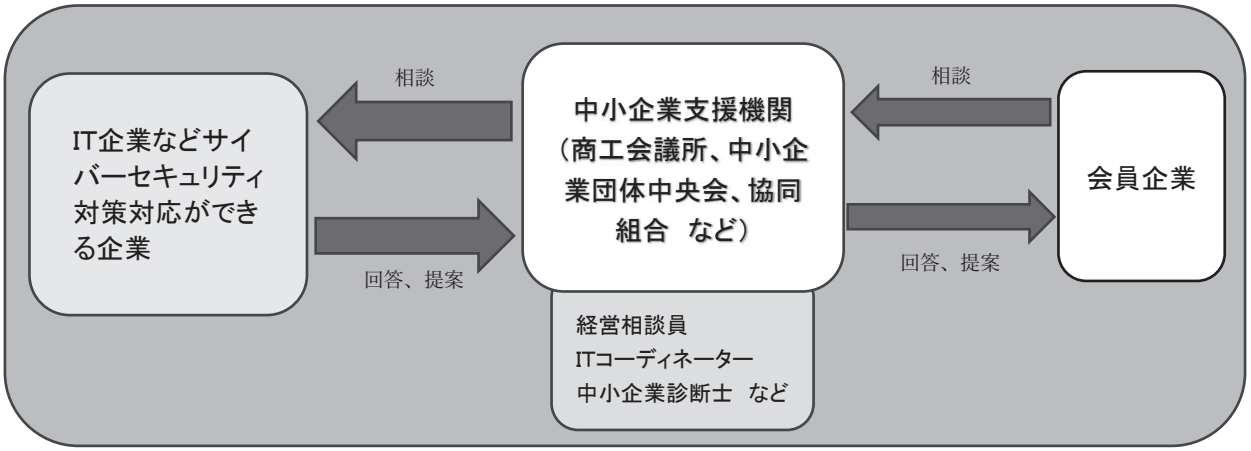
おわりに
～地域の中小企業支援機関の活用～

大企業の指導が届きにくい中小サービス業にサイバーセキュリティ対策を浸透させるには、業界毎のガイドラインで最低限の対応を定めて対策を講じざるを得ない環境を作り、リソースの不足やコスト面での負担を軽減するための方策として地域の中小企業支援機関を活用したIT企業とのマッチング体制構築や保険商品などの情報提供は有効と考える。

経済産業省のセキュリティ対策評価制度構築にあたり、業界団体と連携して各業界の特徴を踏まえ、必要な認証段階を明確にすれば、各業界の特徴を踏まえたガイドラインとして活用できるのではないか。

ただ、ガイドラインが出来たとしても、HPで公表するだけでは中小企業に浸透させることは難しい。そこで、サイバーセキュリティ対策を推進しているIPAなどの政府関係機関は、既に存在している地域ごとの中小企業支援機関を活用してはどうか。Pit-Nagoyaを擁する「名古屋商工会議所」などの商工会議所や、「静岡給食」が相談した静岡県中小企業団体中央会のような組織は全国にネットワークがある。これらの組織の活用は、あらたにサイバーセキュリティ対策のための組織を作ることなく、既に存在するネットワークを通して、多くの地域中小企業に情報提供し、公平な立場で必要なサポートを自ら提供したり、サポート企業を紹介することができる（**図表12**）。

（図表12）中小企業支援機関の活用



（筆者作成）

名古屋商工会議所は、Pit-Nagoyaの活動を他の商工会議所にも広げるような活動を行っている。また、IT企業が名古屋市ほど集積していない商工会議所には、Pit-NagoyaのIT企業を紹介するという活動も行っている。

保険会社各社も全国中小企業団体中央会や商工会議所等と連携して中小企業に適したサイバーリスク保険を開発し、提供している。全国中小企業団体中央会のサイバーリスク保険は、各県の中小企業団体中央会が、地域の中小企業からの相談に対応して紹介するほか、情報提供として研修会なども実施している。

中小サービス業のサイバーセキュリティ対策推進には、「サイバーセキュリティ対策を進めざるを得ない環境にすること」、「リソースの不足やコスト面での負担を軽減すること」が必要である。具体的には、各業界の特長を踏まえた業界ごとのサイバーセキュリティガイドラインを経済産業省やIPAなどの政府関係機関等が策定することで、最低限の基準が提示される。これにより、企業は対策を進めざるを得ない環境になると思われる。また、対策を進めるための負担軽減策として、基準を満たしていないと判断した企業には、地域の中小企業支援機関である商工会議所や中小企業団体中央会などが、各企業の業種に基づき、企業の状況に応じて支援する。支援内容は、IT企業の紹介やサイバーリスク保険加入などのアドバイスを行うなどで、社内にIT人材を配置することが難しい中小サービス業の負担を補うことができる。中小サービス業には、このような、既にある体制を活用しながらハンズオンで支援することが、サイバーセキュリティ対策を浸透させるための一つの取りうる手段となるのではないだろうか。

インタビュー実施企業

取材先名	取材日	取材協力（敬称略）	ホームページURL
株式会社アドバンストソフト（注）	2025.4.17	取締役社長　小柳憲章	https://www.advn.co.jp/
静岡給食協同組合	2025.6.12	管理部長　野崎雅代	https://sq-lanch.com/
静岡県協同振興株式会社	2025.6.12	取締役営業部長　町田昌恒	https://www.siz-sba.or.jp/s/about/dantai/sinkou.html
東京海上日動火災保険会社	2025.6.30	火災・企業新種業務部 サイバー室専門次長　教学大介 シニアアソシエイト　小田優奈 広報部広報グループ シニアアソシエイト　小川亜由美	https://www.tokiomarine-nichido.co.jp/
独立行政法人情報処理推進機構（IPA）	2025.7.4	セキュリティセンターセキュリティ普及啓発・推進部 普及啓発グループ グループリーダー　小野塚直人 主幹　佐藤栄城	https://www.ipa.go.jp/
損害保険ジャパン株式会社	2025.6.25	営業開発部課長代理　稲垣学	https://www.sompo-japan.co.jp/
名古屋商工会議所、Pit-Nagoya	2025.7.3	名古屋商工会議所(中小企業相談所)創業･専門相談ユニット ユニット長経営指導員　織田　浩 創業・専門相談担当係長　経営指導員　田中利直	https://www.nagoya-cci.or.jp/ https://pit-n.nagoya-cci.or.jp/
箱根湯本温泉 ホテルおかだ	2025.5.29	常務取締役　原　洋平	https://www.hotel-okada.co.jp/
株式会社モノリスワークス（注）	2025.4.18	副社長　吉村孝弘	https://monolithworks.co.jp/about-us/

（注）サイバーセキュリティに関する基本的事項についてインタビューを実施。

参考文献

○石川大介（2023）「医療機関におけるインシデント対応ボードゲームを用いたサイバーセキュリティ訓練の実施報告」医療情報学43（5）pp219-232

○市瀬幸雄、高橋静香、大谷佳裕（2021）「テレワーク時代のセキュリティ―ペリメタモデルからゼロトラストモデルへ―」通信ソサエティマガジン　No.56　春号2021　pp315-322

○木村裕一、赤尾嘉治、桜井由美子（2017）「中小企業へのサイバー攻撃を防御するためのCSIRT導入の考察」システム監査　2017年30巻1号　pp48-58

○教学大介（2021）「サイバー保険の開発と日本企業のセキュリティ実態」日本セキュリティマネジメント学会誌　Vol.35 No.2, 2021 pp30-38

○国家公安委員会、総務大臣、経済産業大臣（2025）「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」令和7年3月13日公表

○佐久間首里　猪俣敦夫（2019）「サイバー保険の調査・分析による加入率向上への提案」情報処理学会研究報告　pp1-8　情報処理学会研究報告　Vol.2019-IOT-44　No9

○竹内英二（2022）「中小企業におけるサイバーセキュリティ対策の実態」日本政策金融公庫論集第54号　2022年2月　pp87-105

○田中啓介　古川佳和　野田幹稀　上原哲太郎（2022）「中小企業における情報セキュリティ対策状況のインタビュー調査」情報処理学会研究報告　pp1-8　Vol2022-IOT-56　No43

○辰巳憲一（2023）「サイバー攻撃が損害保険業に及ぼす影響と対策―サイバーセキュリティ投資資産家の

方法と効果―」損害保険研究　85（2）2023年8月　pp55-77
○山内正人、坂倉基司、大島岳彦、砂原秀樹（2021）「サイバーセキュリティインシデント発生時におけるシナリオ型組織間コミュニケーション訓練の設計と評価」コンピュータソフトウェア　Vol.38　No.1　Feb.2021　pp18-30
○山下美若（2023）「ネットワーク理論を活用したサイバーセキュリティ・リスクシェアリング-中小企業サイバーセキュリティ対策促進に向けて-」経営論集　101号　pp65-79　東洋大学経営学部編

参考資料

○環境庁「令和6年度観光DXにおける生成AIの適切かつ効果的な活用に関する調査事業」
https://www.mlit.go.jp/kankocho/content/001889635.pdf
○経済産業省「サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ（概要）」
サプライチェーン強化に向けたセキュリティ対策評価制度に関するサブワーキンググループ事務局　2025年4月14日
https://www.nisc.go.jp/pdf/council/wg_supply_chain/outline_of_interim_report.pdf
○経済産業省「中小企業の実態判明 サイバー攻撃の7割は取引先へも影響」20250219
https://www.meti.go.jp/press/2024/02/20250219001/20250219001.html
○経済産業省「デジタル・ガバナンスコード2.0」2022年9月
https://www.meti.go.jp/policy/it_policy/investment/dgc/dgc2.pdf
○警視庁「令和6年におけるサイバー空間をめぐる脅威の情勢等について」警視庁広報資料令和7年3月13日
サイバー企画課　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf
○独立行政情報処理推進機構「中小企業等における情報セキュリティ対策の実態及び課題の把握」（2024）
https://www.ipa.go.jp/pressrelease/2024/press20250214.html#topics_01
○独立行政法人情報処理推進機構「2024年度中小企業における情報セキュリティ対策に関する実態調査－報告書－」
2025年5月　https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html
○独立行政法人情報処理推進機構「中小企業の情報セキュリティ対策ガイドライン」
https://www.ipa.go.jp/security/guide/sme/about.html
○独立行政法人情報処理推進機構「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」
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf
○独立行政法人情報処理推進機構「2024年度中小企業等実態調査結果」速報版　20250214
https://www.ipa.go.jp/pressrelease/2024/press20250214.html
○独立行政法人情報処理推進機構「サイバーセキュリティお助け隊サービス」
https://www.ipa.go.jp/security/otasuketai-pr/
○全国中小企業団体中央会「サイバー保険制度」
https://www.chuokai.or.jp/index.php/supportservice/insurance/privacy/
○総務省・経済産業省「令和3年経済センサス－活動調査」産業別規模別企業数（民営、非一次産業、2021年）より（2025年版中小企業白書、付属統計資料）　https://www.chusho.meti.go.jp/pamflet/hakusyo/2025/chusho/f1.html
○総務省「令和6年版情報通信白書　第Ⅱ部　情報通信分野の現状と課題」
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/html/nd21a100.html
○公益財団法人損害保険事業総合研究所「米国を中心とするサイバーインシデント・サイバー保険市場の動向」
損保総研レポート第134号2021.1
https://www.sonposoken.or.jp/reports/wp-content/uploads/2021/02/sonposokenreport134_1.pdf
○中小企業基盤整備機構「IT導入補助金2025」　https://it-shien.smrj.go.jp/about/
○中小企業庁「IT導入補助金制度2025」　https://www.chusho.meti.go.jp/koukai/yosan/r7/r6_it_summary.pdf

○中小企業庁「サービス等生産性向上IT導入支援事業『IT導入補助金2025』の概要　令和7年6月中小企業庁」
https://www.chusho.meti.go.jp/koukai/yosan/r7/r6_it_summary.pdf
○東京海上日動火災保険「サイバーリスク総合支援サービス」
https://www.tokiomarine-nichido.co.jp/hojin/baiseki/cyber/service.html
○東京海上日動火災保険「サイバーリスク保険」https://www.tokiomarine-nichido.co.jp/hojin/baiseki/cyber/
○一般社団法人日本損害保険協会「今注目のサイバー保険」 https://www.sonpo.or.jp/sme_insurance/cyber-hoken/
○一般社団法人日本自動車工業会「サイバーセキュリティガイドライン最新情報」
https://www.japia.or.jp/work/ict/cybersecurity-newest
○一般社団法人日本自動車工業会「自動車産業サイバーセキュリティガイドライン」
https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html
○一般社団法人日本損害保険協会「中小企業におけるリスク意識・対策実態調査2024調査結果報告書2025年3月」
https://www.sonpo.or.jp/sme_insurance/assets/pdf/sme_report2024.pdf
○一般社団法人JPCERTコーディネーションセンター「インシデント報告対応レポート」
https://www.jpcert.or.jp/pr/2025/IR_Report2024Q4.pdf　20250731閲覧
○Zenken株式会社　業種別のサイバーセキュリティ　https://www.ooda-security.com/case-study/