中小企業サイバー攻撃被害事例収集等業務

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

第1章 背景・目的

第1節 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「攻撃動向分析・対策 WG」では、経営者への効果的な情報提供のあり方を検討するため、令和 4 年度において、経営者ヒアリングとして地域の商工会議所の協力を得て、「サイバーセキュリティ懇談会」を 2 回実施し計 11 社の中小企業の経営者からご意見をいただいた。

この中で、経営者が関心を持つサイバーセキュリティに関するテーマは、「自社が被害を被った時の影響や事業継続に係る考え方」、「同業他社の被害状況や対処の仕方、業界の動向」等であることが明らかになり、また、経営者への情報提供は、「商工会議所、商工会等の経済団体と連携した懇談会形式が有効」であることが分かった。

第2節 目的

令和 5 年度においては、攻撃動向分析・対策 WG にて検討してきた経営者に対する情報発信のあり方について、中小企業対策強化 WG 等の情報発信活動に反映することとし、商工会議所等の経済団体との連携による、被害企業事例コンテンツの作成と発信を行うこととした。具体的には令和 4 年度に実施した中小企業の経営者を対象とした「サイバーセキュリティ懇談会」について、これを拡充する方向で開催し、地域のセキュリティ専門家によるサイバーセキュリティお悩み相談の中から中小企業のサイバー攻撃被害事例や経営視点から判断した対応ポイント等を収集、収集した情報から中小企業のセキュリティ対策の啓発に資する事例を選択し、個別取材による被害事例のコンテンツ化を行うものである。

第3節 本事業の業務概要

中小企業サイバー攻撃被害事例収集等業務として、以下の業務を行った。

1.サイバーセキュリティ懇談会の開催

中小企業のサイバー攻撃被害事例や経営視点から判断した対応ポイント等の収集を目途として、商工会議所、商工会等の経済団体との連携により、中小企業の経営者を対象としたサイバーセキュリティ懇談会を 7 か所(計 8 回)開催した。開催後、他の中小企業経営者の啓発に有益なセキュリティ対策取組事例やインシデント対処方法について計 16 事例を収集し、概要を書面にまとめた。

2.サイバー攻撃被害事例のコンテンツ化

収集した 16 事例のうち、中小企業のセキュリティ対策の啓発に資する 3 事例を IPA と協議の上決定し、個別取材を行った。取材結果について取りまとめたコンテンツを Word/HTML 2 種類の形式にて作成した。

本業務の全体像は以下の図のとおりである。

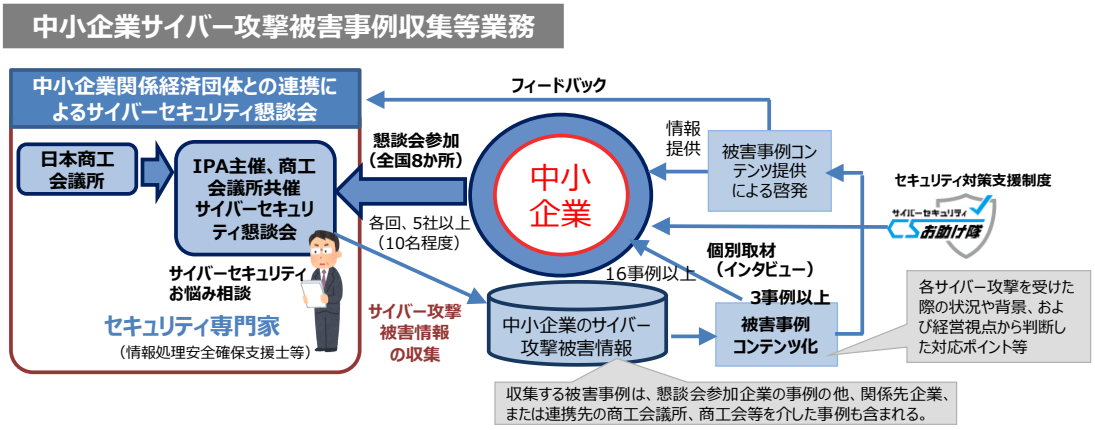

図 1-1 中小企業サイバー攻撃被害事例収集等業務全体図

第2章 業務の内容

第1節 サイバーセキュリティ懇談会の開催

第1項 懇談会開催主旨

「中小企業サイバー攻撃被害事例収集等業務」の一環として、地元の商工会議所と連携し、中小企業の経営層を対象とした「サイバーセキュリティ懇談会」を 7 か所、計 8 回開催した。

懇談会では、サイバー攻撃の被害にあった、または関心の高い経営者やシステム担当者の方々に集まっていただき、ゲストスピーカーによる情報提供、地域のセキュリティ専門家によるサイバーセキュリティお悩み相談を実施した。お悩み相談では、経営者から、サイバー攻撃被害に関する実例、攻撃を受けた際の状況や背景や経営視点から判断した対応ポイント、その他、サイバーセキュリティに関する悩み事などについての実際の声を聞き、中小企業のサイバーセキュリティの現状や、直面している課題の掘り起こしを行った。

第2項 懇談会開催概要

2-1.開催準備

(1)商工会議所との連携

本サイバーセキュリティ懇談会開催にあたっては、IPA からの共催依頼を受諾した商工会議所との連携のもと、7 カ所での開催に向けて、準備を行った。

なお、少人数の懇談会形式で実施することから、参加社数は開催回毎に 5 社以上、参加者数は経営者に加えて随行者各社 1 名まで、合計 10 名程度を想定し、各商工会議所を通して、サイバーセキュリティに関心を持つ中小企業を対象に広く参加募集を行った。

共催商工会議所は下記のとおりである。

共催：佐倉商工会議所、大阪商工会議所※、北大阪商工会議所※、豊中商工会議所※、 熊本商工会議所、横須賀商工会議所、高崎商工会議所、松本商工会議所、 新潟商工会議所

※大阪では、大阪商工会議所、北大阪商工会議所、豊中商工会議所の共催にて開催した。

(2)プログラム内容

サイバーセキュリティ懇談会のプログラム(2 時間程度/回)は、主にゲストスピーカーによるサイバーセキュリティへの取組み事例等の情報提供ならびに地域のセキュリティ専門家をファシリテーターとした「サイバーセキュリティお悩み相談」により構成し、経営者からサイバーセキュリティに関する悩み事や、サイバー攻撃被害に関する実例を聴取するものとした。

なお、ゲストスピーカーは、関係者と協議の上、IPA が指名し決定した。

また、ファシリテーターとなるセキュリティ専門家は開催地域の情報処理安全確保支援士(登録セキスペ)等とし、開催回毎に IPA「セキュリティプレゼンター」登録者の中から IPA が指名し決定した。

以下にゲストスピーカー、ファシリテーターならびにカッコ内に各担当地区を示す。

【ゲストスピーカー】

グローカルビジネスソリューションズ株式会社	代表取締役社長	白岡　健氏(佐倉)
創ネット株式会社	代表取締役社長	小口　幸士氏
	(大阪、熊本、横須賀、高崎、松本)	
太田油脂株式会社	代表取締役社長	太田　健介氏(新潟)

【ファシリテーター】

コメオ	代表	
	IT コーディネーター	米澤　國雄氏(佐倉)
コンサルティング・リンクスル	代表	田中　基貴氏(大阪)
特定非営利活動法人熊本県 IT コーディネーター協会		
	理事	森本　宗聡氏(熊本)
株式会社クロスウィズユー	代表取締役	田中　孝典氏(横須賀)
ミニティ株式会社	代表取締役	山本　哲也氏(高崎)
TakTools	代表	北嶋　　崇氏(松本)
株式会社ビックリマーク	代表取締役　班長	武内　正一郎氏(新潟)

(3)運営体制

主催団体(IPA)統括の下、商工会議所との連携を柱に、下記の体制にて、事前調整、準備を行った。

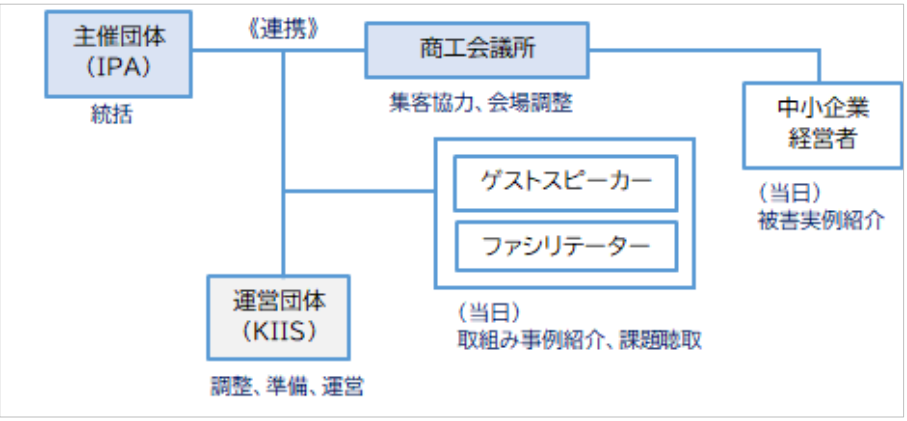

図 2-1　運営体制図

(4)準備作業の詳細

懇談会の開催に向けて、下記の調整ならびに準備等を行った。なお、会場は各商工会議所内の会議室を使用する方向で調整を図った。

① 関係者の調整(商工会議所、ゲストスピーカー、ファシリテーター)

② 具体的な開催内容の確定(開催日、開催場所、参加企業)

③ 懇談会開催に必要な機材等の手配

④ 当日配布資料の準備

進捗については、回毎にステータス管理を行い、関係各所と調整を図り、開催日時ならびに参加企業団体を確定させた。

(5)参加企業募集

参加企業募集にあたっては、チラシを作成し、各共催商工会議所を通して、開催周知に努めた。

(実施例：サイバーセキュリティ懇談会 in 佐倉)

図 2-2 周知チラシ例

2-2.開催内容

(1)開催プログラム

以下のプログラムを基本に、開催した。(各回共通／開催時間：2 時間)

(オープニング)IPA による開催主旨説明

第 1 部 ゲストスピーカーによる

「サイバーセキュリティへの取組み事例発表」

第 2 部 地域のセキュリティ専門家(ファシリテーター)による

「経営者のサイバーセキュリティお悩み相談コーナー」

第 3 部 経営者ヒアリング

サイバー攻撃を受けた際の状況や背景、経営視点から判断した対応ポイント、その他、日頃の業務を通して、ご関心をお持ちのサイバーセキュリティに関するテーマなどについてのヒアリング

(2)開催概要

下記のとおり、7 カ所、計 8 回の懇談会を共催商工会議所の会議室、日時にて開催し、各地域の中小企業経営者ならびにシステム担当者等、合計 40 社 53 名の参加を得た。

表 2-1 開催一覧

	共催商工会議所	開催日時	参加企業数(人数)
1	佐倉商工会議所	2023 年 11 月 13 日(月)13:30～15:30	5 社(5 名)
2※	大阪商工会議所	2023 年 11 月 14 日(火)13:00～15:00	6 社(7 名)
	北大阪商工会議所		
	豊中商工会議所		
3※	大阪商工会議所	2023 年 11 月 14 日(火)16:00～18:00	5 社(8 名)
	北大阪商工会議所		
	豊中商工会議所		
4	熊本商工会議所	2023 年 11 月 15 日(水)14:00～16:00	7 社(7 名)
5	横須賀商工会議所	2023 年 11 月 21 日(火)13:00～15:00	6 社(10 名)
6	高崎商工会議所	2023 年 11 月 24 日(金)13:00～15:00	5 社(7 名)
7	松本商工会議所	2023 年 11 月 28 日(火)13:00～15:00	3 社(5 名)
8	新潟商工会議所	2023 年 12 月 4 日(月)10:00～12:00	3 社(4 名)
		合計	**40 社 (53 名)**

※2 ならびに 3 は「大阪商工会議所」の会議室を使用し、開催した。

(3)準備・当日作業の詳細

事務局として、サイバーセキュリティ懇談会の開催当日に以下の作業を行った。

① 配布資料の印刷配布
② 懇談会開催当日の作業(設備の配置、終了後撤収等)
③ 懇談会の進行表の作成ならびに司会進行
④ 懇談会の内容を議事録として記録

(4)開催まとめ

本懇談会での各参加企業からのヒアリングをもとに、開催回毎に 2 事例、計 16 の被害事例を決定し、まとめを作成した。2 事例の決定の際には、「経営者視点のセキュリティ意識」「サイバー攻撃被害事例」「自社内セキュリティ対策の現状」「対取引先のセキュリティ対策の現状」の 4 点を重視し、IPA と協議した。なお、該当事例については、別添 1 にて報告するものとする。

第3項 懇談会　各地域の実施報告

関係者との調整、準備を経て、下記のとおり、7 カ所、計 8 回の懇談会を開催した。

1.佐倉

・日時：2023 年 11 月 13 日(月)13:30～15:30

・会場：佐倉商工会議所　会議室(千葉県佐倉市表町 3 丁目 3-10)

・参加企業(人数)：5 社(5 名)

参加企業	A 社(化学品製造業)　DX 推進課　課長(K.A 氏) B 社(空調設備製造・施工業)　代表取締役(K.T 氏) C 社(土木建設業)　営業部(S.H 氏) D 社(造園業)　IT 担当(T.A 氏) E 社(社会保険労務士事務所)　代表(Y.H 氏)
ゲストスピーカー	グローカルビジネスソリューションズ株式会社　代表取締役社長　白岡　健氏
ファシリテーター	コメオ代表　IT コーディネーター　米澤　國雄氏
主催者	独立行政法人情報処理推進機構(IPA)　セキュリティセンター セキュリティ普及啓発・振興部普及啓発グループ　芳賀　政伸氏、伊藤　由佳氏
共催者	佐倉商工会議所　販路拡大・企画事業室　　室長　三谷　晃生氏
オブザーバー	八街商工会議所　総務課　主事　嶋田　佑介氏 東金商工会議所　中小企業相談所補助員　田邉　亮平氏 (以下、オンライン参加) 経済産業省　関東経済産業局　地域経済部デジタル経済課　田中　隆誠氏 日本商工会議所　情報化推進部　原　伸一氏 佐原商工会議所　中小企業相談所　所長　伊能　将人氏、指導員　石田　江里奈氏

図 2-3　佐倉_写真 1

図 2-4　佐倉_写真 2

2.大阪①

・日時：2023 年 11 月 14 日(火)13:00～15:00

・会場：大阪商工会議所　会議室(大阪府大阪市中央区本町橋 2-8)

・参加企業(人数)：6 社(7 名)

参加企業	A 社(EC サイト運営)　代表取締役社長(S.E 氏)、情報システム担当(H.T 氏) B 社(樹脂成型品製造業)　専務取締役(H.K 氏) C 社(旅行業)　代表取締役(M.M 氏) D 社(ソフトウエア開発業)　代表取締役(M.N 氏) E 社(医薬品卸売業)　情報システム室　室長(M.H 氏) F 社(デジタルコンテンツ開発業)　ＤＸ推進チーム　課長代理(T.S 氏)
ゲストスピーカー	創ネット株式会社　代表取締役社長　小口　幸士氏
ファシリテーター	コンサルティング・リンクスル　代表　田中　基貴氏
主催者	独立行政法人情報処理推進機構(IPA)　セキュリティセンター セキュリティ普及啓発・振興部普及啓発グループ　芳賀　政伸氏、伊藤　由佳氏
共催者	大阪商工会議所　経営情報センター　所長　湯谷　康文氏、次長　古川　佳和氏 課長　野田　幹稀氏、課長　石田　貴志氏、登坂　文香氏 北大阪商工会議所　情報センター　森下　健太郎氏
オブザーバー	経済産業省　近畿経済産業局 地域経済部　次世代産業・情報政策課　総括係長　竹村　祐樹氏、 情報化推進係長　中村　憲司氏 (以下、オンライン参加) 日本商工会議所　情報化推進部　部長　原　伸一氏、主席調査役　和田　昌昭氏

図 2-5　大阪①_写真 1

図 2-6　大阪①_写真 2

3.大阪②

・日時：2023 年 11 月 14 日(火)16:00～18:00

・会場：大阪商工会議所　会議室(大阪府大阪市中央区本町橋 2-8)

・参加企業(人数)：5 社(8 名)

参加企業	A 社(システム構築・販売業)　取締役(I.H 氏)、維持管理グループ　課長代理(U.R 氏) B 社(保険代理店業)　南大阪支店長(N.K 氏)、(H.S 氏) C 社(電気器具製造業)　常務取締役総務部長(N.Y 氏) D 社(産学連携支援サービス業)　ゼネラルマネージャー(N.M 氏)、アシスタントゼネラルマネージャー(N.H 氏) E 社(特殊塗装業)　営業部(M.M 氏)
ゲストスピーカー	創ネット株式会社　代表取締役社長　小口　幸士氏
ファシリテーター	コンサルティング・リンクスル　代表　田中　基貴氏
主催者	独立行政法人情報処理推進機構(IPA)　セキュリティセンター セキュリティ普及啓発・振興部普及啓発グループ　芳賀　政伸氏、伊藤　由佳氏
共催者	大阪商工会議所　経営情報センター　課長　野田　幹稀氏、登坂　文香氏 北大阪商工会議所　情報センター　森下　健太郎氏 豊中商工会議所 事務局長　吉田　哲平氏、IT 推進室専任アドバイザー　中元　一廣氏
オブザーバー	経済産業省　近畿経済産業局 地域経済部　次世代産業・情報政策課　情報化推進係長　中村　憲司氏 (以下、オンライン参加) 経済産業省　商務情報政策局　サイバーセキュリティ課　課長補佐　三田　真史氏 日本商工会議所　情報化推進部　部長　原　伸一氏、主席調査役　和田　昌昭氏

図 2-7　大阪②_写真 1

図 2-8　大阪②_写真 2

4.熊本

・日時：2023 年 11 月 15 日(水)14:00～16:00

・会場：熊本商工会議所　会議室(熊本県熊本市中央区横紺屋町 10)

・参加企業(人数)：7 社(7 名)

参加企業	A 社(食品加工業)　総務部部長(I.Y 氏) B 社(レジャー施設業)　DX 担当(K.S 氏) C 社(害虫駆除サービス業)　IT 管理担当(S.I 氏) D 社(農業コンサルティング業)　IT 管理部　技術開発チーフ(N.K 氏) E 社(観光振興業)　NW 担当(N.K 氏) F 社(法律事務所)　所長(H.M 氏) G 社(広告代理店業)　社長(H.H 氏)
ゲストスピーカー	創ネット株式会社　代表取締役社長　小口　幸士氏
ファシリテーター	特定非営利活動法人　熊本県 IT コーディネーター協会　理事　森本　宗聡氏
主催者	独立行政法人情報処理推進機構(IPA)　セキュリティセンター セキュリティ普及啓発・振興部普及啓発グループ　芳賀　政伸氏、伊藤　由佳氏
共催者	熊本商工会議所 会員サービス部　部長　坂井　一文氏、　課長補佐　岸田　慎吾氏
オブザーバー	一般社団法人熊本県サイバーセキュリティ推進協議会　橘　弘氏 (西日本電信電話株式会社　熊本支店　熊本ビジネス営業部　課長) 経済産業省　九州経済産業局　地域経済部　情報政策課 デジタル経済室　室長　春口　浩子氏、情報化推進　小幡　拓也氏 (以下、オンライン参加) 東京都産業労働局商工部　経営支援課　事業調整担当 課長代理　菅澤　美佳氏、課長代理　枝　昭徳氏、主事　小瀬　光裕氏

図 2-9　熊本_写真 1

図 2-10　熊本_写真 2

5.横須賀

・日時：2023 年 11 月 21 日(火)13:00～15:00

・会場：横須賀商工会議所　会議室(神奈川県横須賀市平成町 2 丁目 14-4)

・参加企業(人数)：6 社(10 名)

参加企業	A 社(自動車部品製造業)　代表取締役(O.H 氏)、生産本部長(O.Y 氏) B 社(建築物修繕業)　代表取締役(S.M 氏)、情報システム課　サブマネージャー(S.H 氏) C 社(衣料洋品販売業)　代表取締役社長(T.I 氏)、(F.M 氏) D 社(NPO 法人)　理事 情報セキュリティグループ長(T.Y 氏)、理事 情報セキュリティ管理責任(I.T 氏) E 社(金属プレス業)　代表取締役(M.A 氏) F 社(調剤薬局チェーン業)　専務取締役(M.Y 氏)
ゲストスピーカー	創ネット株式会社 代表取締役社長　小口　幸士氏
ファシリテーター	株式会社クロスウィズユー　代表取締役　　田中　孝典氏
主催者	独立行政法人情報処理推進機構(IPA) セキュリティセンター セキュリティ普及啓発・振興部普及啓発グループ　芳賀　政伸氏、伊藤　由佳氏
共催者	横須賀商工会議所 専務理事　菊池　匡文氏、産業地域活性課　参事　大井　康浩氏
オブザーバー	かながわ信用金庫　常務理事　片岡　祐二氏、事務部長　田中　武幸氏 経済産業省　関東経済産業局　地域経済部　デジタル経済課　田中　隆誠氏 (以下、オンライン参加) 経済産業省　関東経済産業局　地域経済部　デジタル経済課　情報企画係長　山田　郁美氏 日本商工会議所　情報化推進部　主席調査役　和田　昌昭氏

図 2-11　横須賀_写真 1

図 2-12　横須賀_写真 2

6.高崎

・日時：2023 年 11 月 24 日(金)13:00～15:00

・会場：高崎商工会議所　会議室(群馬県高崎市問屋町 2 丁目 7-8)

・参加企業(人数)：5 社(7 名)

参加企業	A 社(ソフトウエア開発業)　代表取締役(A.A 氏)、IT アーキテクト リーダー(O.T 氏) B 社(情報処理サービス業)　常務取締役(O.T 氏) C 社(建材卸売・建築業)　代表取締役社長(K.M 氏) D 社(情報処理サービス業)　代表取締役(S.M 氏)、専務取締役(S.J 氏) E 社(情報処理サービス業)　代表取締役(M.K 氏)
ゲストスピーカー	創ネット株式会社　代表取締役社長　小口　幸士氏
ファシリテーター	ミニティ株式会社　代表取締役　　山本　哲也氏
主催者	独立行政法人情報処理推進機構(IPA)　セキュリティセンター 　セキュリティ普及啓発・振興部普及啓発グループ　芳賀　政伸氏、伊藤　由佳氏
共催者	高崎商工会議所 　専務理事　石綿　和夫氏、会員サービス課　課長　櫻井　誠氏、 　係長　中島　宏人氏、主事補　堤　はる香氏
オブザーバー	(以下、オンライン参加) 経済産業省　関東経済産業局　地域経済部 デジタル経済課　情報企画係長　山田　郁美氏、田中　隆誠氏

図 2-13　高崎_写真 1

図 2-14　高崎_写真 2

7.松本

・日時：2023 年 11 月 28 日(金)13:00～15:00

・会場：松本商工会議所　会議室(長野県松本市中央 1 丁目 23-1)

・参加企業(人数)：3 社(5 名)

参加企業	A 社(ICT 導入サポート業)　代表取締役(K.K 氏) B 社(ソフトウェア開発業)　取締役執行役員(T.H 氏)、技術統括部　フェロー(M.F 氏) C 社(ウェブサイト制作業)　代表取締役(N.Y 氏)、(K.H 氏)
ゲストスピーカー	創ネット株式会社　代表取締役社長　小口　幸士氏
ファシリテーター	TakTools　代表　　北嶋　崇氏
主催者	独立行政法人情報処理推進機構(IPA)　セキュリティセンター セキュリティ普及啓発・振興部普及啓発グループ　芳賀　政伸氏、伊藤　由佳氏
共催者	松本商工会議所 DX 推進部長　林　祐一郎氏、情報事業部　主事　梶原　悠氏
オブザーバー	(以下、オンライン参加) 経済産業省　関東経済産業局　地域経済部　デジタル経済課　総括　近藤　裕貴氏 日本商工会議所　情報化推進部　主席調査役　和田　昌昭氏

図 2-15　松本_写真 1

図 2-16　松本_写真 2

8.新潟

・日時：2023 年 12 月 4 日(月)10:00～12:00

・会場：新潟商工会議所　会議室(新潟県新潟市中央区万代島 5)

・参加企業(人数)：3 社(4 名)

参加企業	A 社(パソコン設定・サポート業)　代表取締役(S.H 氏) B 社(食品販売業)　新潟本社　DX マーケティング部　課長(N.S 氏) C 社(住宅用空調機販売業)　取締役　相談役(Y.S 氏)、所長(S.A 氏)
ゲストスピーカー	太田油脂株式会社　代表取締役社長　太田　健介氏
ファシリテーター	株式会社ビックリマーク　代表取締役　班長　武内　正一郎氏
主催者	独立行政法人情報処理推進機構(IPA)　セキュリティセンター セキュリティ普及啓発・振興部普及啓発グループ　芳賀　政伸氏、伊藤　由佳氏
共催者	新潟商工会議所 事業部　次長　山口　泰博氏、会員サービス課　主事　相馬　七海氏
オブザーバー	(以下、オンライン参加) 経済産業省　関東経済産業局　地域経済部 デジタル経済課　情報企画係長　山田　郁美氏、田中　隆誠氏 日本商工会議所　情報化推進部　部長　原　伸一氏

図 2-17　新潟_写真 1

図 2-18　新潟_写真 2

第4項 インシデント事例

懇談会で得られた議論の内容から、参加企業におけるサイバーインシデント等の状況について情報を抽出した。

4-1.まとめ

インシデント[1] 件数		22 件
[内訳]	①メール被害	18 件(約 82%)
	②ホームページ改ざん被害	3 件
	③その他	1 件

【ポイント】

・ウイルス感染等による被害

今回のサイバーセキュリティ懇談会では、参加企業等から 22 件のサイバーインシデント事例を収集した。主にメール等によるウイルス攻撃による被害が発生しており、企業内で注意喚起や社員教育をしているにもかかわらず、ウイルスメールを開くことにより感染をしていた。その中で、不審メールについて、発送元であると取引先に電話確認することにより未遂となった事例も報告され、アナログな手法であるが簡単にできる予防対策の 1 つになると思われる。

4-2. 被害事例

(1) メール被害 [17 件]

①過去、官公庁からの連絡を装ったウイルス付きメールを開封し感染した。(【佐倉】A 社(化学品製造業)K.A 氏)

②約 1 年前、UTM[2]を導入する前に迷惑メールを開いてしまった。今も感染状態が継続しているかが心配であるが、専門家に相談したところ、たとえ過去に社内ネットワークに侵入したウイルスが、社外に不正送信されたとしても、UTM が検知し、送信を防御するとの説明があり、安心した。(【佐倉】E 社(社会保険労務士事務所)Y.H 氏)

③約 10 年前、社員がウイルスに感染していた私物パソコンを、社内ネットワークに接続し、社内システムにウイルスが拡散された。ファイルサーバーにおいて、復旧に必要な調査範囲が明確でなかったため全システムの復旧まで 3 日を要した。インシデント発生の要因として、当時のセキュリティ対策の不十分さがあり、私物パソコンの社内接続を禁止していたものの、社員教育や不許可端末の検知機能が十分ではなかった。(【大阪①】D 社(ソフトウエア開発業)M.N 氏)

---

[1] インシデント：何らかの問題が発生してアクシデント（事件・事故）になる一歩手前の状況を指す。発見が遅れたり気付かずに見過ごされたりした場合に重大な事件や事故・危機的な状況に発展する可能性やリスクを持つ出来事・事案・事象・事例のこと。

[2] UTM: Unified Threat Management ネットワークにおけるセキュリティ監視装置

④⑤当社が対処した顧客先におけるランサムウェア被害事例は 2 件あり、1 例目はサーバー1 台の被害で済んだが、2 例目は複数台のサーバーが感染し、復旧に 1 週間以上を要した。(【大阪①】D 社(ソフトウエア開発業)M.N 氏)
⑥取締役がなりすましメールを開き、エモテットに感染したことを契機にセキュリティ対策を強化したにもかかわらず、その後、社員がメールに記載されたマルウェアへのリンクをクリックし、ウイルスが社内に拡散される 2 度目の被害が発生した。発生源のメールはウイルス対策ソフトの検知をすり抜けていた。(【大阪②】A 社(システム構築・販売業)I.H 氏)
⑦エモテットによる攻撃メール被害に遭遇した。不審なメールが一定の時期に集中して社内に送られて発覚。協力会社からの情報漏洩が原因と見られる。IPA の攻撃関連サイトから提供されていた感染チェックツールを使用し、メールを受信したパソコンの感染の有無の確認をした。メールを開いてしまった社員もいたが、最新のエンドポイントセキュリティが導入されていたため、実害は出なかった。(【横須賀】B 社(建築物修繕業)S.M 氏)
⑧行政機関になりすましたメールを過去に受信した。普段受信するメールにはない行政機関のホームページへのリンクが貼られていた。システムに一番詳しい社長が最初にメールを見たおかげで、不審な点に気づき、社内の感染を防げた。(【横須賀】F 社(調剤薬局チェーン業)M.Y 氏)
⑨普段使用しているクレジットカードの請求日を狙ってメールが送られた。ID とパスワードを要求され、入力すると次にクレジットカードの番号も求められた。メールを見直すと、URL があきらかにクレジットカード会社のものではなかった。翌日には本物のクレジットカードの請求書が届き、フィッシング URL も UTM でブロックされた。(【松本】A 社(ICT 導入サポート業)K.K 氏)
⑩個人の経験だが、1 台の端末から突然異常な数のメールが発信される被害に遭遇した。当該端末をクリーンアップ後も、別の端末から同様の現象が連鎖的に発生した。最終的には全社のネットワークを遮断し、一斉クリーンアップを実施した。(【新潟】A 社(パソコン設定・サポート業)S.H 氏)
⑪アドミニストレーター(admini@xxx)宛にウイルス付きのメールが送信され、誤ってメールを開いた端末のデータが一気に消去された。攻撃されたメールアドレスのドメインが大手製薬会社の社名と酷似していたため、誤って攻撃されたものとみている。(【新潟】A 社(パソコン設定・サポート業)S.H 氏)
⑫相談窓口として、ホームページにアドレスを載せているが、そのアドレスに毎日かなりの数のなりすましメールが届く。対策を講じても、イタチごっこで、すぐに別のメールが送られてくる。(【高崎】D 社(情報処理サービス業)S.J 氏)
⑬⑭弊社になりすましたメールが送信されたケースが 2 件あった。1 件目は、お客様宛に過去に送信した文面を利用された。2 件目は社員のメールアドレスを送信者としたウイルス付きメールが、お客様に送信された。(【佐倉】A 社(化学品製造業)K.A 氏)
⑮グループ内事業部がランサムウェアの被害に遭遇し、結果、取引先の医療機関にまで被害が及んだ。(【大阪①】E 社(医薬品卸売業)M.H 氏)
⑯過去にエモテット被害に遭遇した。自社の管理職の名前で関連会社にメールが送信された。発覚してすぐに、全ての関連先に電話でメールを開かないように注意喚起したが、開けてしまったところがあった。対策するパソコンの特定が難しく、本インシデントが発生した事業部のパソコン 30 台をクリーンア

ップして様子見としたが、どこまで広がっているかを追いかけられる形にしておく必要がある。(【熊本】B 社(レジャー施設業)K.S 氏)

⑰取引先から不審なメールを受信した際、発送元である取引先に電話で確認をしたところ、被害を免れることができた(【大阪②】B 社(保険代理店業)N.K 氏)

⑱リンクや添付ファイル等何もついていない、脅迫文のみのメールを受信した。専門家に確認したところ、メールアドレスが実際使用されているか確認後、次の攻撃がされるケースがある。もしくはメールの半分がウイルス対策ソフトによって消去されている可能性もあるとのことだった。(【新潟】B 社(食品販売業)N.S 氏)

(2)ホームページ改ざん被害 [3 件]

①2020 年 12 月に自社ホームページの管理用 ID とパスワードが漏洩し、ホームページが書き換えられ、ホームページをクリックすると別のサイトにリダイレクトされる事象が発生した。漏洩の原因を調べたかったが、見積もりが高額だったため断念し、書き換えられたコードを元に戻し、UTM とエンドポイントセキュリティを導入するなどの対策を講じて問題を解決した。管理用 ID の漏洩は、担当者が一人で、管理者が十分に社員教育をしていなかったことが要因の 1 つであり、現在は担当者に定期的なパスワード変更を通知し、再発防止に努めている。(【大阪①】F 社(デジタルコンテンツ開発業)T.S 氏)

②自社の偽サイトが立ち上げられ、詐欺の踏み台サイトとされた経験を持つ。海外(韓国)からの仕掛けにより、偽サイトから商品購入すると、海外へと送金される仕組みとなっていた。最後は警察の捜査により解決した。(【熊本】G 社(広告代理店業)H.H 氏)

③1 年ほど前に、CMS*[3]の脆弱性が原因で、ホームページの一部が攻撃され、フィッシングサイトに誘導するような改ざんを受けた。発覚後すぐにホームページを止めたが、サーバーがダウンした。被害直後は、ホームページ上での公表、IPA への報告やお客様への説明などの対応に多く時間を要した。CMS を排除し、新たなホームページを作成した。業務への直接の影響はなかったものの、結果復旧まで 2～3 ヶ月を要した。新しいホームページになった今も、外部からの不審なアクセスは続いている。(【松本】B 社(ソフトウェア開発業)T.H 氏)

(3)その他 [1 件]

①5、6 年ほど前、当社が作成したショッピングサイトで、約 1 万件のカードの使用可能確認が行われた。与信手数料が短時間で数十万円に上がって発覚した。調査の結果、当該事件は中国からのアクセスだった。盗用カードの不正利用ための確認であった可能性が高い。(【松本】C 社(ウェブサイト制作業)N.Y 氏)

第5項 懇談会サマリー

懇談会にてヒアリングした内容に基づき、開催回毎 2 事例、計 16 の事例を、ピックアップした。各地に

[3] CMS：「Contents Management System：コンテンツ・マネジメント・システム」の略で、Web サイトのコンテンツを構成するテキストや画像、デザイン・レイアウト情報（テンプレート）などを一元的に保存・管理するシステムのこと。

おける 2 事例のサマリーを以下に示す。

【佐倉】

千葉県佐倉市の【佐倉】E 社(社会保険労務士事務所)Y.H 氏は、商工会議所や IPA などの専門家の手を借りながら、個人事務所のセキュリティ対策や、千葉県社会保険労務士会のデジタル化推進に取り組んでいる。千葉県社会保険労務士会においては参加者のニーズやスキルに応じた研修の実施が困難であることを課題として挙げている。 一方、【佐倉】B 社(空調設備製造・施工業)K.T 氏は、大手 OA 商社の提案について、相談する相手がいないため、疑問を抱いたままのシステム投資を続けている。K.T 氏は、投資額の膨らみに不安を抱いており、自身でシステムの現状やリスクを正確に把握できていないため、公平な立場で評価してもらえる相談相手を探している。

まとめ：両社ともに、セキュリティ対策やデジタル化の推進、システム投資判断など、専門的な知識やスキルが求められる場面において、専門家への相談を求めていることが示唆される。

【大阪①】

【大阪①】B 社(樹脂成型品製造業)では、在宅勤務者の増加に伴い、在宅インターネット環境からのウイルス侵入を懸念。社員のセキュリティ教育の強化や、迷惑メールによるウイルス感染リスクの管理対策を第三者に相談することを検討している。【大阪①】D 社(ソフトウエア開発業)では、自社と顧客先でランサムウェア被害を経験。顧客対応時のランサムウェア被害防止のために、リモート接続時のリスクの軽減を図りたいと考えおり、社内負荷軽減のために、外部サービスの利用も検討している。また、ランサムウェア被害額の実態を把握し、今後の顧客対応に活かしたいとも考えている。

まとめ：両社では、在宅勤務やリモートメンテナンスなど、リモート接続の際のリスク対策強化が共通の課題である。また、対策を強化するにあたり、両者ともに自社内での解決が困難であると認識しており、外部サービスの利用や専門家への相談を検討している。

【大阪②】

【大阪②】A 社(システム構築・販売業)は、技術的な対策に加え、セキュリティ教育の強化などの人的な対策を実施したにもかかわらず、2 度目のサイバー被害に遭遇した経験がある。社員の意識が十分に高まっていなかったことが原因とみられ、社員一人ひとりにセキュリティの重要性を理解してもらうための方法を模索している。【大阪②】C 社(電気器具製造業)は、社長からセキュリティ対策を任された総務部長が、社員へのセキュリティ教育や UTM の導入などの対策を実施している。しかし、経営者自身がセキュリティ対策のかじ取りを担うことが本来のあるべき姿で、そのためには、専門知識が必要となる。社内に専門家が置けない状況ではあるが、今後は、経営者と専門家が連携して、セキュリティ対策を推進していく必要がある。

まとめ：両社ではいずれも「社内全体のセキュリティ啓発」が課題であり、専門家と共に、経営者を含めた全社的なセキュリティ意識の向上のための方策を検討する必要があると示唆される。

【熊本】

【熊本】G 社(広告代理店業)H.H 氏は、著作権侵害を目的とした偽サイトの立ち上げという被害を受けた経験から、サイバーセキュリティの重要性を認識している。日々の通常業務においても迷惑メールによるサイバー攻撃の脅威に常にさらされており、海外企業との取引においても、セキュリティの甘さを感じており、リスクを回避するためには、さらなる対策が必要であると考えている。【熊本】B 社(レジャー施設業)では、過去にエモテットによる被害を受けた経験から、被害を最小限に抑えるためには、被害の拡大を早期に把握することが重要であると考えている。また、IT 監査の厳格化により、IT 予算の確保がしやすくなった一方で、サイバーセキュリティ対策の「どこまでやれば良いのか」という悩みを抱えている。様々な IT ベンダーから提案を受けるが、どれも高額な費用がかかるため、自社にとって最適な対策を見極めるのが難しいという。懇談会に参加し、判断の参考になるような情報収集に努めているとのこと。

まとめ：両社ともにサイバー攻撃の被害経験から、今後の対策について、また、【熊本】B 社（レジャー施設業）においては IT ベンダーからの提案の「見極め」についての課題も抱えており、懇談会などに積極的に参加し、参考情報の収集に努めている。

【横須賀】

【横須賀】A 社(自動車部品製造業)は、大手自動車会社関連会社のサイバーインシデント事件を教訓に、UTM の導入や社員への注意喚起など、セキュリティ対策を強化している。しかし、UTM の運用についてはレポートの活用など未着手な部分が多く、また、社内に情報システムの専門担当がいないため、課題も多い。また、上流取引先からのセキュリティ調査の強化も見据え、より一層の対策強化が求められている。【横須賀】B 社(建築物修繕業)は、エモテット被害に遭遇したものの、最新のエンドポイントセキュリティの導入により、実害を最小限に抑えることができた。被害後は、セキュリティソフトウエアの更新タイミング、インシデント発生時の対応の見直しなどの対策を講じている。しかし、社内に 200 台の使われていないパソコンが存在し、定期的なセキュリティ更新が実施されていないという課題もある。

まとめ：両社は、いずれもサイバー攻撃の脅威を認識し、セキュリティ対策の強化に取り組んでいるが、その一方で一部運用が不足している現状があり、適切な対策を講じる必要がある。

【高崎】

【高崎】C 社(建材卸売・建築業)は、創業 200 年の老舗企業であり、重要な売掛金データについて

独自のバックアップ運用を実施している。インターネット回線や電源の途絶など、予期せぬ事態が発生した場合のリスクを考慮した対策であり、また、自身についても、いざというときのためにマニュアルを用意し、経営を継続するための対策を取っている。【高崎】D 社(情報処理サービス業)は、データ入力やコールセンター事業など、多くの個人情報を扱う企業である。そのため、内部不正対策を最優先課題と位置づけ、管理体制の強化と社内教育の徹底に取り組んでいる。パソコン PC の USB ポートを制限するなど、技術的な対策も講じているが、それだけでは内部不正を防ぐことは難しいと考えている。そのため、社員に対して、内部不正のリスクや、不正を防止するための行動について、定期的に教育を行っている。

まとめ：両社はいずれもサイバー攻撃のリスクを認識し、それぞれの事業内容にあった方法で対策に取り組んでいるが、技術的な対策のみならず、非常時マニュアルの整備や社員の意識改革など、人的な対策も重要であるという意識を共通して持っている。

【松本】

【松本】C 社(ウェブサイト制作業)はウェブサイト制作会社であるが、セキュリティ対策として、最新のセキュリティ情報の収集と社内共有を進めることと、社内外でセキュリティ知識の均一化を図ることを課題としている。【松本】B 社(ソフトウェア開発業)は、自社のホームページ改ざん被害を経験後、専門家によるリスクアセスメントを実施し、セキュリティ対策の強化を目指している。アセスメント結果を社員に共有し、全社の意識向上につなげることができたが、提案事項を全て実施すると費用と対応の負荷が多くなり悩んでいる。また、近年、複数のシステム連携が進む中、セキュリティの責任範囲を明確にするために、開発標準プロセスや契約書の見直しなどにも取り組んでいる。

まとめ:両社はいずれも社員のセキュリティ意識の向上と知識の共通化、そしてインシデント発生時の運用体制の確立を課題として挙げている。また、共にデジタル製品をサービスとして提供する立場であるため、顧客のセキュリティ意識の向上も重要であるとの認識も持っている。【松本】B 社（ソフトウェア開発業）においては、セキュリティ対策の費用および運用負荷とのバランスについて課題を抱えている。

【新潟】

【新潟】C 社(住宅用空調機販売業)では、6 か所ある営業所等の拠点間のセキュリティ対策が課題である。対策の推進にあたり、経営者が情報セキュリティの重要性を正しく認識し、また、社内で、守るべき情報とそのリスク、対策の程度や費用についても話し合うことが重要と考えている。【新潟】A 社(パソコン設定・サポート業)では 33 のグループ会社全体のセキュリティ対策を開始する予定である。各社にある最も重要なデータを整理しており、また、第一歩目として、まずはセキュリティアクションの実行から取り組む予定である。セキュリティ対策製品の導入よりも、その後の運用の継続が重要と考えている。

まとめ：両社ともに、セキュリティ対策推進の第一歩として、「会社として守るべき情報を整理する」ことが重要と考えている。セキュリティ対策の運用においても、人的要素を重視しており、経営者を含め社員全員で運用体制を構築し、会社を守っていく姿勢が大切との認識を持っている。

第2節 サイバー攻撃被害事例のコンテンツ化

第1項 コンテンツ化の概要

サイバーセキュリティ懇談会で収集した中小企業のサイバーセキュリティ被害および対策事例の中から、中小企業のセキュリティ対策の啓発に資する 3 事例を選択し、インタビュー形式による個別取材を行い、取材結果を取りまとめたコンテンツを作成した。

第2項 インタビュー方法

インタビューの実施方法は、インタビュアーがインタビュー対象者に質問をして回答を得る対話形式とした。インタビュー実施場所はインタビュー対象者の所属する企業内とし、インタビュー日程はインタビュー対象者の指定する日時とした。所要時間は撮影にかかる時間を含め、1 時間半程度とした。

インタビュアーには、先に開催したサイバーセキュリティ懇談会のファシリテーターを務めた地域のセキュリティ専門家を起用した。

また、カメラマンとライターを事前に手配し、インタビュー開催時に同行した。インタビュー実施中に、インタビュー対象者の許可を得て、インタビュー対象者の近景、ならびにインタビュー風景の写真を撮影した。

インタビューは、全て IC レコーダーで音声記録し、文字起こし原稿を作成した。発言内容のデータを収集し、その内容を基にコンテンツを作成した。作成したコンテンツは、インタビュー対象者、インタビュアーおよび IPA と内容確認を実施した。

インタビュー実施方法について、以下のとおりに示す。

【実施期間】

・ 2023 年 12 月～2024 年 1 月

【スケジュール】

・ 開始 10 分前　スタッフ現地入り
　　*スタッフ内訳：IPA　1～2 名,インタビュアー　1 名,
　　カメラマン　1 名,ライター　1 名,事務局　2 名
・ 開始～1 時間半　撮影準備、挨拶、インタビュー開始、インタビュー終了後撮影
・ 撮影終了後　撤収

【実施場所】

・ インタビュー対象者所属企業内

第3項 インタビュー対象

初めにインタビュー対象となる候補者 4 名を懇談会 2 事例より選出した。選出にあたり、「事業継続」という経営者的視点からのセキュリティ対策を重要な事項と判断し、実際に対策を講じていることを基準とした。候補者 4 名の概要資料を作成し、IPA と協議後、インタビュー対象者 3 名を決定した。

インタビュー対象者 3 名およびその選定理由について、以下の表に示す。

No	懇談会開催地	企業名	インタビュー対象者	選定理由
1	横須賀	岡田電機工業株式会社	代表取締役 岡田　英城　氏 生産本部長 岡田　祐作　氏	UTM の設置など、基本的なセキュリティ対策を実施している。社内のシステム環境の整備を社長のご子息が担当し、親子で懇談会に出席するなど、二人三脚で事業を引導する姿勢を有す。また、主な取引先が自動車業界であるため、サプライチェーンセキュリティの現状および課題についてのヒアリングも可能である。
2	大阪	株式会社クロスエフェクト	専務取締役 畑中　克宣　氏	お助け隊サービスを利用し、UTM を導入するなど基本的なセキュリティ対策を実施している。また、在宅勤務時の自宅インターネット回線からのウイルスの侵入や、社員のセキュリティ意識を懸念するなど、セキュリティリスクに対する感度が高い。当事業者は、デジタル技術を使用した医療用臓器モデル開発事業の拡大にむけて、守秘性の高い医療データを安全に取り扱うべく、今後も高度なリスク対策が求められる事業者でもある。
3	高崎	株式会社コムテックス	代表取締役 小林　正明　氏	UTM、サイバー保険への加入など、基本的なセキュリティ対策を実施している。また、有事に備え、経営者自らが重要データの選別とバックアップを運用している。「事業の継続」を起点に「リスク対策」が正しい順序で考察され、実行されている。また、経営者は高崎商工会議所の副会頭として、地域社会のネットワークに幅広い人脈と知見を有する。

対象者への事前説明は、オンラインにて「個別インタビュー主旨説明」資料を提示し行った。主旨説明資料には、インタビュー実施方法、インタビュー項目、アウトプットイメージ等を掲載した。経営者インタビューで引き出したいポイントや、コンテンツでの実写真および実名公表の合意を得た後、日程調整などの準備を進めた。

個別インタビュー主旨説明資料の内容例を以下に示す。

(1)目的・取材概要

【目的】

・本業務では、先日実施したサイバーセキュリティ懇談会でお伺いした事例の中から、3 つの事例を個別に取材（インタビュー）し、コンテンツ化します。

・中小企業経営者のサイバーセキュリティ対策および事業継続の啓発に役立つコンテンツの作成を目指します。

【取材内容】

・サイバーセキュリティ懇談にてヒアリングした結果を基に、下記 3 つのポイントについて詳しくお聞かせいただきます。

・経営視点から判断するサイバーセキュリティ対策のポイント

・日ごろの業務を通じてご関心のあるサイバーセキュリティに関するテーマ

・サイバー攻撃被害経験をお持ちの場合、前後の状況や背景および対応

【アウトプット】

本事業にて作成した事例コンテンツは、冊子および Web ページにて公開します。

(2)アウトプット章立てイメージ

【主旨】 経営者による経営者のためのセキュリティ対策の啓発

序章
- a. 事業内容紹介
- b. 自己紹介

1 章. セキュリティ対策の現状
- a. 私のセキュリティ意識
- b. 対策コストとシステム構成、運用について
- c. 人員体制
- d. 取引先におけるセキュリティ対策の動向
- e. 相談先（地域/同業者との横つながり）

2 章. サイバーセキュリティに関する悩みごと （※個々の事例に合わせて設定）
- a. お悩み 1
- b. お悩み 2

3 章. 要望・提言（※個々の事例に合わせて設定）
- a. 対 同業者
- b. 対 商工会議所
- c. 対 IPA
- d. 対 地方自治体

第4項 インタビュー項目

懇談会でヒアリングした内容に基づき、経営者としてのセキュリティ対策の判断とその視点を掘り下げるためのインタビュー項目を、インタビュアー、ライター、IPA と協議の上決定した。協議に際し、インビュー対象者の所属企業の事業概要や経営者の経歴、作成予定コンテンツのキャッチコピーやシナリオなどをまとめた資料集を作成した。

個別インタビュー資料集を、以下のとおり図に示す。

図 2-19 個別取材資料集 1

図 2-20 個別取材資料集 2

インタビュー項目を、以下の表に示す。

No	質問テーマ	質問項目
1	事業内容の紹介	(ア) 事業内容とステークホルダーについて (イ) 取引先間の、情報の授受について(デジタル化の範囲など)
2	サイバー被害時の事業リスクについて	(ア) サイバー被害を受けた場合の、最も大きな事業リスクについて (イ)一番守らなければいけないデータは何について。また、それを守る方法について
3	現在のセキュリティ取り組みについて	(ア) お助け隊 ① サービス加入の経緯について ② セキュリティ対策を考えるようになった、一番始めのきっかけについて (問い合わせのきっかけとなった事柄や背景、最初に声をあげた社員など) ③ 他サービスの中から、お助け隊を選択した理由について ④ お助け隊に対する満足度や課題感について サービスを導入後の変化など
		(イ) その他のセキュリティ対策 ① 図面データ等、重要なデータの取引先への受け渡し方法、暗号化等のセキュリティ対策について ② 外注管理について(セキュリティ対策関連事項) ③ クラウド等外部サービスの利用について サービスの利用を決めたポイントなど ④ BCP 対策(南海トラフ)の状況について ⑤ 保険の加入状況について 付帯サービスの利用状況も含めて
		(ウ) 運用について

		① 社内のセキュリティ担当者について ② セキュリティに関する相談相手の有無や、相談方法について ③ 業界団体や商工会議所などのネットワーク内におけるセキュリティ対策(意見交換会など)の現状について
		(エ) 費用について ① セキュリティ対策費用の支出についての考え方 (コストか投資か・他の支出と比較しながら) ② セキュリティ費用の割合について ③ セキュリティ対策予算を立てることが難しい、他の経営者へのアドバイス等
4	課題	(ア)社員教育について ① 社内におけるセキュリティ教育の実施状況について、デジタル人材の育成予定等 ② 社員の教育不足の最大のリスクは何かについて ③ インシデント発生時に備えた、連絡網や運用手順書の準備状況について ④ 事故防止策について i. 人的要因に基づく情報漏洩リスクについて、会社の考え方、課題 ii. セキュリティポリシー設定の有無と、社員への教育について iii. 迷惑メール対策について、現状の取り組み(訓練等) iv. 迷惑メール対策の課題点 v. 取り組みを予定する対策等
5	未来への提言	① 地域の同業者に向けたセキュリティ対策やデジタル化等のアドバイス ② 業界団体や商工会議所等、コミュニティ関係者への要望や提言等、 ③ IPA、自治体、行政等に対する要望や提言 ④ 今後の事業展開について

第5項 インタビュー実施日程

インタビュー実施日程を以下の表に示す。

No	実施日程	実施場所	インタビュー対象者	懇談会開催地
1	12 月 27 日(水) 10:30 - 12:00	神奈川県　横須賀市 岡田電機工業株式会社 会議室	代表取締役 岡田　英城　氏 生産本部長 岡田　祐作　氏	横須賀
2	1 月 12 日(金) 13:00 - 14:30	京都府　京都市 株式会社クロスエフェクト 会議室	専務取締役 畑中　克宣　氏	大阪
3	1 月 18 日(木) 13:30 - 15:00	群馬県　高崎市 株式会社コムテックス 会議室	代表取締役 小林　正明　氏	高崎

第6項 インタビューコンテンツの作成

個別インタビューの結果を、経営者のサイバー対策事例コンテンツとして取りまとめた。コンテンツはインタビュアーとインタビュー対象者との対話形式とし、1 事例 5,000 文字以上で、インタビュー写真および関連する図表やイメージ図等を挿入して作成した。取りまとめたコンテンツは、インタビュー対象者、インタビュアーおよび IPA に内容確認を行った。コンテンツは冊子用の Microsoft Word2016 以上の形式と、ホームページ用の HTML 形式の 2 種類を作成した。なお、該当コンテンツについては、別添 2 にて報告するものとする。

第7項 インタビューサマリー

個別インタビューサマリーを以下に示す。

No.1)岡田電機工業株式会社　代表取締役　岡田　英城氏　/　生産本部長　岡田　祐作氏

岡田電機工業株式会社は、顧客情報の取り扱いを含むクラウドサービス事業を開始したことを 1 つのきっかけとし、全社的なセキュリティ強化を実施した。システム専門家の不在のなか、長年付き合いのある OA 商社に相談し、UTM やクラウドへのデータバックアップなどの最新セキュリティツールを導入した。しかしヒアリングの結果、レポーティングや保守サービスなどの機能を活用できていないことが判明した。ツールの正しい運用方法を理解せずに「安心」していたということである。また、自動車業界を主な取引先とするため、サプライチェーンにおけるセキュリティリスクを懸念している。現在、上流の企業からはセキュリティチェックリストを受け取っているが、金型メーカーなどの外注先へのチェックは行っていない。外注先は小規模事業者が多く、セキュリティ対策の要求は、費用の負担が発生するため、現実的でないとのことだった。

サプライチェーンリスクが増加するなか、チェーン全体のセキュリティ対策が必要不可欠であるが、推進に

あたり、小規模事業者への支援も考慮する必要があると思われる。

ポイント：セキュリティツール機能の不十分な活用、専門家の不在、サプライチェーンリスク対策における小規模事業者の支援

No.2)株式会社クロスエフェクト　専務取締役　畑中　克宣氏

株式会社クロスエフェクトは、畑中専務自らの積極的な情報収集により、サイバーセキュリティお助け隊サービスに加入し、UTM を導入した。結果、経営陣の安心感向上や、セキュリティ最新情報の入手による社員教育の機会増加と情報収集コスト削減という効果を得ている。取引先の信頼を重視する社長は、機密情報データの取り扱いに極めて慎重な姿勢を取り、毎週の朝礼で、社員の意識が向上するような話をしている。事業継続の本質的なセキュリティ意識を社員に醸成すべく、社長自らが対応している。今後は、医療系データの受け渡しを効率化し、社内にシステム運用体制を構築することを目標とする。引き続き、懇談会などから情報収集し、会社の成長に対応できる仕組みを構築するとのことである。

ポイント：経営者自らの積極的な情報収集(懇談会への参加)、経営者による社員教育、機密性の高い医療データの受け渡しの効率化、社内運用性の構築を目標

No. 3)株式会社コムテックス　代表取締役　小林　正明氏

株式会社コムテックスの大きな特徴は、事業継続を目的とするリスクヘッジ対策を社長自らが 30 年前から実施していること。社内の最重要データとする売掛金データを、現在は 3 つの場所に保存しており、そのうちの 1 つはインターネットが使用できくなるリスクを想定し、会社ではない場所に保存している。

往々にして、「セキュリティ対策製品の導入」という手段が、セキュリティ対策の目的に取り違えられるケースも多いなか、コムテックス社は、「事業の継続」をゆるぎない目的とし、セキュリティ対策製品の持つリスクを冷静に分析し、自社に適切な「セキュリティ対策」を画策・実施している。商工会議所に対しては、これまでの取り組みに加えて、セキュリティに関する情報発信やセミナーの継続的な実施を期待しているとのことである。

ポイント：最重要データは 3 か所でバックアップ、事業継続を目的としたセキュリティ対策、対策の工夫、商工会議所による情報収集機会創出への期待

第3章 考察

懇談会および個別インタビュー参加者の発言を分析した結果、中小企業のサイバーセキュリティ対策に関わる以下の主要な観点５つが明らかになった。

① 従業員、経営者のセキュリティ意識の欠如
② セキュリティ全般に関する相談先の不足
③ 懇談会形式での情報共有の機会の重要性
④ サプライチェーンリスク対策
⑤ セキュリティ対策資金不足を克服するための工夫

以下に詳細を示す。

第1項 従業員、経営者のセキュリティ意識の欠如

今回のヒアリングでは、社内において、セキュリティ対策が進まない理由の１つとして、従業員、経営者双方のセキュリティ意識の欠如を指摘する声が多数聞かれた。

A) 従業員のセキュリティ意識の欠如

「エモテット被害後、セキュリティ対策を強化したにもかかわらず、社員の不注意によって、２度目のウイルス感染が発生した」「端末の外部記憶装置の出入口を塞ぐなどの対策をしているにもかかわらず、業務中に従業員がインターネットを閲覧後、エラーサイトが出現した」など、懇談会では、情報セキュリティ対策を強化しているにもかかわらず、人的要因によって被害が発生してしまうことが指摘された。同様に、内部不正による情報漏洩対策の進め方についての悩みも聞かれた。

サイバー攻撃は日々高度化しており、技術的な対策だけでは防御しきれず、現場の従業員の協力が欠かせない。問題は、“会社の安全が自身の行動にかかっている”ことを従業員に理解させられるか、である。インシデントは誰にでも起こり得るものということ、日々脅威にさらされていること、そして、被害を発生させた場合、事業を止めてしまう可能性もあることを一人ひとりが正しく理解しておく必要がある。意識が定着すれば、啓発活動も効果を発揮しやすく、また、社内の運用体制を構築する際に、積極的な協力を得られる可能性が高まる。

ではどのように意識を変えていくか。

会社を守るため、というセキュリティ対策の目的の本質から考えると、やはり会社内部からの働きかけが望ましい。中小企業は経営者と従業員の距離が近いという利点を活かし、経営者自らが発信することが効果的である。ただし、そのためには、経営者自身が危機意識を有していることが前提である。実際、懇談会の出席者からも、朝礼などの機会を利用し、経営者自身が会社全体の意識の醸成に取り組む事例が聞かれた。また、そのような会社は一定のセキュリティ対策を実施済みであった。

B) 経営者のセキュリティ意識の欠如

「経営者がセキュリティ対策に関心がない」「実際に起こっていないことへの対策に、予算を充てられない」 、この 2 点が懇談会で多く聞かれた経営者の意識である。
今回ファシリテーターを依頼したセキュリティ専門家によれば、大手企業のサイバー攻撃被害事例ばかりメディアで報じられるため、“中小企業は攻撃対象ではない”、“中小企業のデータは狙われるほど重要ではない”と受け取られがち、とのことである。

中小企業においても、“自社は大丈夫”という根拠のない思い込みは持たず、中小企業の経営者が自ら“自社も攻撃対象である“と正しく認識することが、セキュリティ対策の出発点であると言える。現に、懇談会の出席者でセキュリティ対策を講じている経営者は、「被害を受けることを前提としている」もしくは「実際に被害に遭った」など、自社を攻撃の対象と、正しく認識していた。

これらのことから、経営者に如何にセキュリティ意識を持ってもらうかが、中小企業のサイバーセキュリティ対策における最大の要であるが、その方法については、いくつか考えられる。商工会議所等支援機関からの懇談会やセミナーの開催、IPA からの情報発信などの啓発活動に加えて、例えば、簡易攻撃メール訓練サービスを活用したテスト攻撃メールを送信する取り組みや、 中小企業が運営する EC サイト向けの脆弱性診断のような取組みが有効と考えられる。支援機関と協力しながら、サイバーセキュリティと中小企業経営者との間に「かかわり」を与える機会を、戦略的に創出していく必要があると考える。

第2項 セキュリティ全般に関する相談先の不足

懇談会で一番多く聞かれた要望は「専門家へ相談をしたい」であった。相談の中身は様々で、「社内の教育の展開」「社内のインシデント体制の構築」に関するアドバイスから、「IT ベンダーからの高額提案の目利き」を求める声も複数あった。

また、現在、中小企業がセキュリティの相談を行う先の多くは、古くから自社に出入りのある OA 商社や IT ベンダーであることも分かった。OA 商社や IT ベンダーは、商材の販売を目的とした営利企業であることから、専門知識のない中小企業に対して、往々にして商談が優先されがちであり、社員教育や体制構築など、商材の販売につながらない相談は後まわしになる懸念がある。実際、懇談会においても、「高額な見積を受け取って判断に悩んでいる」、「セキュリティ対策製品は導入したが運用状況を把握していない」などの声があった。セキュリティ対策製品に限らず、IT 製品は、正しい使い方と運用があって初めて効果を発揮するが、現実は “セキュリティ対策製品だけは導入済みだが適切な運用がされていない”中小企業が多く存在する可能性がある。

これらの問題への対応として、中小企業がセキュリティの教育や体制、セキュリティシステムの運用等について、セキュリティ専門家へ相談する窓口を商工会議所や自治体などの地域単位で設立する考え方もある。セキュリティ専門家は地域内に所在することが望ましいが、オンライン会議システム等を活用してもよい。IPA のセキュリティ相談窓口や、サイバーセキュリティお助け隊サービスの活用、商工会議所などの支援機関、保険会社との連携を考慮に入れるのも一つの方法である。中小企業の「セキュリティ対策に取り組みたい」という気持ちを大事に、セキュリティ全般の相談先の充実が望まれる。

第3項 懇談会形式での情報共有の機会の重要性

今回の懇談会のように、地域内の中小企業同士が意見交換をし、情報収集できる場を設けたことは、参加者にとって意義深く、また、今後の中小企業のセキュリティ対策支援においては、継続して同様の取り組みの実施を望むご意見を多くいただいた。

懇談会が有効である理由の１つは、今回聞かれた経営者の悩みの多くが、社内の「セキュリティ運用」に依拠するものだということである。運用をどう構築するかについては正解が存在せず、個々の企業が必要な対策や予算に応じて最適な解を見つけていくプロセスが必要となる。そのためには多くの情報収集が必要であり、なかでも同じ視座を持ち、類似する環境下にある他者からの情報は、たいへん参考になるものと思われる。また、講義形式のセキュリティセミナーは多数あるが、参加者同士が直接対話する形式での開催は稀である。実際、どの回においても参加者全員が発言をし、活発な意見交換が実現した。他者と直接対話する時間そのものも、一種のこころの支えになれたのではとも考えられる。懇談会をきっかけに新たなコネクションが構築できれば、セキュリティ対策以外の場面でも役に立つ場合もあるだろう。例えば、震災など有事の際は、多くのネットワークに所属することが孤立を防ぐ。つながりづくりは広義のインシデント対策とも言える。

第4項 サプライチェーンリスク対策

自動車業界のサプライチェーンリスク対策について、参加者から、「取引先の自動車業界の上流会社からセキュリティチェックリストを受け取っているが、発注先に対するチェックはまだ行っていない」とのお話しがあった。また、住宅業界や建築業界、旅行業界の参加者からは、「大企業を除き、デジタル化自体の進行が遅れている」ともの話しもあった。

増加の一途をたどるサプライチェーンにおけるサイバーセキュリティリスクにおいて、”企業規模にかかわらず、サプライチェーンに属する企業は、同じレベルのセキュリティ対策を実施すること”がサイバー被害防止に役立つが、懇談会の参加者の発言から、事業者のデジタル化やセキュリティ対策のレベルは様々であり、統一したセキュリティ対策基準を設けることは困難が多いように見受けられた。また、上述の自動車部品製造業者は、「発注先の小規模事業者にセキュリティチェックの実施をお願いした場合、対策の費用を先方に負担させてしまう場合がある」との懸念を示された。

サプライチェーンリスク対策を推進するにあたっては、サプライチェーンに属する中小企業はもとより、外注先の小規模模事業者に対しても、何らかの支援を講じる必要があると考えられる。

第5項 セキュリティ対策資金不足を克服するための工夫

中小企業においては、経営者のセキュリティ意識が高いとしても、資金繰りに余裕がなく、充分なセキュリティ対策を実施できないケースも存在する。この問題については、セキュリティ専門家から、サイバー保険

の加入、或いは既存のシステムの見直しで浮いた資金をセキュリティ対策に充てるなどの提案があった。また、実際の対策においては、サイバーセキュリティお助け隊など、中小企業向けの安価で効果的なサービス利用が推奨される。

一般に、セキュリティ対策は、それ自体が利益を生むものではないため、資金の少ない中小企業にとって、“お金がかかるもの”との印象を持たれている。しかし、今回の個別インタビュー事業者のように、リスク対策の対象を“事業継続のために、最低限必要なデータ”に絞り込むことで、無理のない範囲で目的にかなう対策を講じている例もあった。このように、限られた予算で、効果的な対策を講じることは可能であると考えられ、そのための事例を学ぶためにも、本章第 2 項で述べたようなセキュリティ専門家によるアドバイスや、第 3 項の懇談会での意見交換など、さまざまな情報収集の機会を活用し、自社なりの創意工夫を図っていくことが重要であると言える。

第4章 総括

本業務では、中小企業のサイバーセキュリティ対策の啓発に資するコンテンツの作成を目的とし、以下２つの業務を行った。

・サイバーセキュリティ懇談会の開催
・サイバー攻撃被害事例のコンテンツ化

サイバーセキュリティ懇談会では、7 か所 計 8 回において、地域の中小企業事業者が参加する対話形式の懇談会を開催し、参加者は、地元の専門家からのアドバイスを受けながら、セキュリティインシデントの被害経験およびセキュリティ対策に関わるお悩みについて情報交換を行った。

サイバーセキュリティ懇談会では、参加企業等から 22 件のサイバーインシデント事例を収集したが、そのうちの約８割がメールを利用した攻撃被害であった。発送元に電話確認をすることで未遂となった事例もあり、簡単な予防対策の一つとして有効と考えられる。

サイバー攻撃被害事例のコンテンツ化では、懇談会の参加者の中から、他の中小企業者の啓発に資する事例になり得る３名を IPA と協議の上選定し、個別インタビューを実施した。インタビューでヒアリングした内容に基づいて、個別に記事を作成した。

上記２つの業務を通じ、中小企業のサイバーセキュリティ対策推進における、主要な観点５点があきらかとなった。

５つの観点を以下の図に示す。

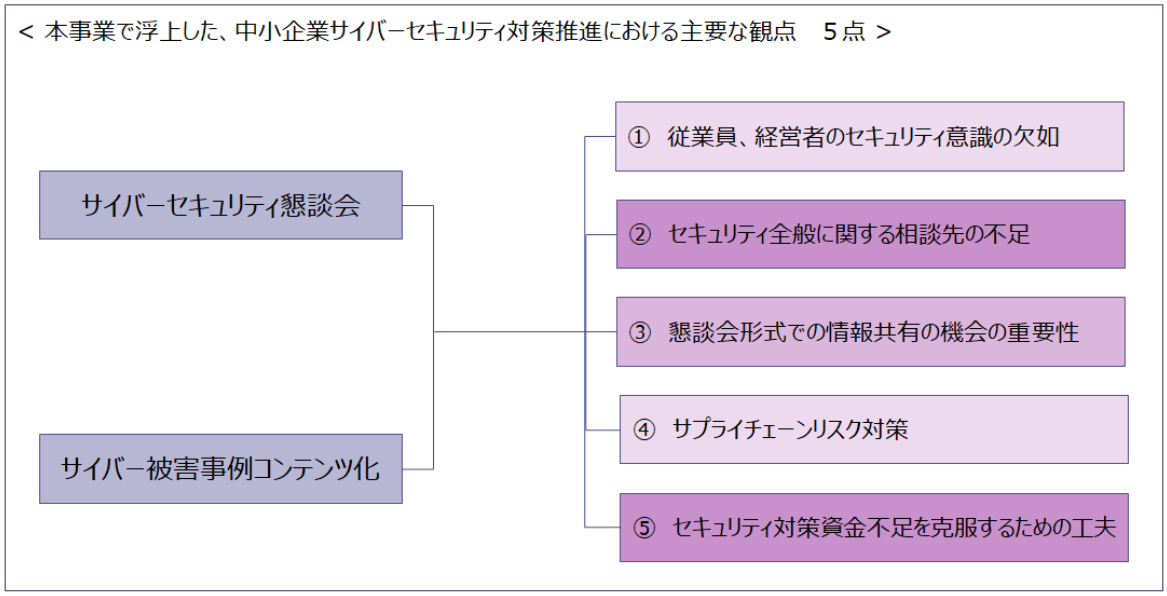

図 4-1 主要観点　５点図

また、上記５つの観点を考察した結果、以下の結論が導き出された。

中小企業におけるサイバーセキュリティ対策は、「事業継続を目的とした経営者のセキュリティ意識が中核となる自発的な取り組み」であることが望ましい。従業員への啓発や予算の割り当てなどの課題が懇談会で提起されたが、経営者の意識が生まれた後は、経営者自らが行動に移し、これらの問題も解決していくと考えられる。

そのためにはまずは“経営者の意識付け”の機会を創出する必要がある。また、懇談会で指摘された、専門家への相談窓口の整備やサプライチェーンに属する小規模事業者への支援などの要望についても、政府、業界団体、支援団体の連携のもとに、効果的な方策を検討していく必要がある。

また、今回の懇談会では、参加者の中小企業経営者による活発な意見交換が行われ、様々な知識、知見、悩み事や工夫のポイントなどの情報が共有された。参加者にとって有効な情報交換の場となったと言えるのではないだろうか。中小企業では、普段抱えている悩みを共有できる機会が少ない。懇談会に出席し、地域のセキュリティ専門家や他の中小企業経営者と悩みを共有することは、たとえ解決に至らなくても、安心感を得られる効果があると考えられる。今後も、中小企業経営者の自発的かつ効果的なセキュリティ対策実施支援のため、商工会議所等の支援機関と連携しながら、情報交換の場を継続して開催することが望ましい。

以上