中小企業サイバー攻撃被害事例収集等業務
実施報告書（概要版）

2024年3月29日

独立行政法人情報処理推進機構
セキュリティセンター

IPA Better Life with IT

背景・目的

● 中小企業サイバー攻撃被害事例収集等業務における背景・目的は以下の通り。

● **背景：**

近年、機密情報を狙ったサイバー攻撃が日々発生し、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。このため、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)」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」を計2回実施した。これにより、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。

● **目的：**

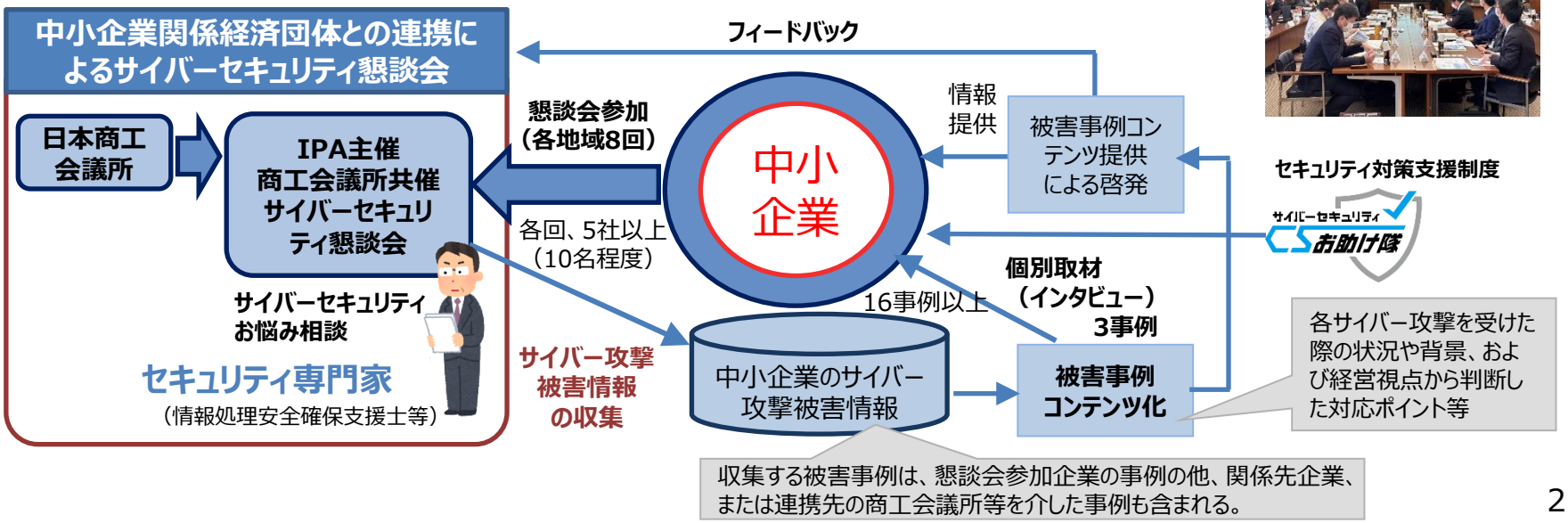
そこで本業務では、令和 4年度に実施した中小企業の経営者を対象とした「サイバーセキュリティ懇談会」 を拡充する方向で開催し、懇談会で収集した中小企業の取り組みや被害事例をもとに、個別取材を通じ、中小企業経営者のセキュリティ意識の啓発に役立つ事例のコンテンツ化を行うこととした。

中小企業サイバー攻撃被害事例収集等業務の概要

● 中小企業関係経済団体（商工会議所等）との連携によるサイバーセキュリティ懇談会を開催。地域のセキュリティ専門家によるお悩み相談の中から、中小企業のサイバー攻撃被害事例等を収集し、個別取材により被害事例のコンテンツ化を行った。

- 令和4年度に実施した、商工会議所協力による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、令和5年度はこれを拡充する方向で各地域で8回開催した（各回、経営者＋随行者各社1名まで、10名程度）。
- サイバーセキュリティ懇談会は、**ゲストスピーカーによる取り組み事例等の情報提供**を行うと共に、ファシリテーターとして**地域のセキュリティ専門家**を起用し、**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等**を収集した（各回2事例×8か所→16事例）。
- 収集した中小企業のサイバー攻撃被害等の情報の中から、今後の中小企業向け**セキュリティ対策の啓発**に供することを目的に、個別取材（インタビュー）による**被害事例のコンテンツ化を3事例**行った。

中小企業サイバー攻撃被害事例収集等業務



サイバーセキュリティ懇談会の実施

● 各地の商工会議所と連携し、サイバー攻撃被害に遭遇した経験を持つ経営者やサイバーセキュリティに関心の高い経営者に集まっていただき、対話形式の「サイバーセキュリティ懇談会」を7か所、計8回開催、40社（53名）が参加した。

➢ サイバーセキュリティ懇談会では、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紹介の後、地域のセキュリティ専門家がファシリテーターを務めたお悩み相談コーナーで、参加者のサイバー攻撃被害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、関心を持っているサイバーセキュリティに関するテーマなどについてヒアリングを行った。

《懇談会案内チラシ例》

《懇談会開催日程と参加人数》

回	地域	共催商工会議所	開催日程	参加企業数（人数）
1	千葉	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	大阪商工会議所	2023年11月14日(火) 13:00～15:00	6社(7名)
3※	大阪	北大阪商工会議所	2023年11月14日(火) 16:00～18:00	5社(8名)
4	熊本	熊本商工会議所	2023年11月15日(水) 14:00～16:00	7社(7名)
5	神奈川	横須賀商工会議所	2023年11月21日(火) 13:00～15:00	6社(10名)
6	群馬	高崎商工会議所	2023年11月24日(金) 13:00～15:00	5社(7名)
7	長野	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	新潟商工会議所	2023年12月4日(月) 10:00～12:00	3社(4名)
	※大阪は同日2回の開催		合計:	40社(53名)

【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（セキュリティ専門家）】
米澤 國雄氏(佐倉)、田中 基貴氏(大阪)、森本 宗聡氏(熊本)、田中 孝典氏(横須賀)、山本 哲也氏(高崎)、北嶋 崇氏(松本)、武内 正一郎氏(新潟)

サイバー攻撃被害事例まとめ

● 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事例も確認された。

◇サイバー攻撃被害事例

No.	インシデントタイプ	件数	主な被害事例
1	メール被害	18件	• 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。被害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(システム事業)I.H氏) • 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) • 行政機関に**なりすましたメールを受信**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)
2	ホームページ改ざん被害	3件	• 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事業)T.S氏)
3	その他	1件	• 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。カード確認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(ホームページ制作業)N.Y氏)
	合計：	22件	

有益なセキュリティ対策の取組みやインシデント対処方法

● サイバーセキュリティ懇談会のヒアリング内容から、他の中小企業経営者に有益なセキュリティ対策の取組みやインシデント対処方法について、開催回毎2事例、計16事例をまとめた。

◇サイバーセキュリティ懇談会　開催回別事例概要

「サイバーセキュリティ懇談会 開催回別事例集」掲載順

開催回	対象者	見出し
佐倉	E社（社会保険労務士事務所）代表　Y.H氏	～個人事務所を経営しながら、社労士会のセキュリティ活動にも貢献～
	B社（空調設備製造・施工業）代表取締役　K.T氏	～不安の増すシステム投資判断：公平な立場の相談相手が欲しい～
大阪①	B社（樹脂成型品製造業）専務取締役　H.K氏	～組織全体のセキュリティ意識を強化、より安全なものづくりの現場を構築～
	D社（ソフトウエア開発業）代表取締役　M.N氏	～サイバー被害における平均的な被害額を知り、顧客対応に活用する～
大阪②	A社（システム構築・販売業）取締役　I.H氏	～サイバー攻撃対策は、技術と教育の両輪で～
	C社（電気器具製造業）常務取締役総務部長N.Y氏	～セキュリティ対策を一任され、奮闘する総務部長～
熊本	G社（広告代理店業）社長　H.H氏	～海外からのサイバー攻撃の被害を受けて～
	B社（レジャー施設業）DX担当　K.S氏	～IT投資のスタンダードとは？～
横須賀	A社（自動車部品製造業）代表取締役　O.H氏	～サプライチェーンインシデントを発生させないためにできること～
	B社（建築物修繕業）代表取締役　S.M氏	～最新エンドポイントセキュリティの導入でエモテット被害を最小限に抑える～
高崎	C社（建材卸売・建築業）　代表取締役社長　K.M氏	～リスクに備え、事業継続のためにできることを最優先に取り組む～
	D社（情報処理サービス業）専務取締役　S.J氏	～内部不正を未然に防ぐため、管理体制と社内教育の徹底を～
松本	C社（ウェブサイト制作業）代表取締役　N.Y氏	～社員のセキュリティ意識の均一化を図り、社内外共にリスク対策を万全に～
	B社（ソフトウェア開発業）取締役執行役　T.H氏）	～システムインテグレーター、ホームページ改ざんから学ぶセキュリティ対策～
新潟	C社（住宅用空調機販売業）取締役　相談役　Y.S氏	～経営者も担当者と一緒にセキュリティ意識を高め一丸となって会社を守る～
	A社（パソコン設定・サポート業）代表取締役　S.H氏	～グループ会社のサイバーセキュリティ対策の展開に注力～

個別取材（インタビュー）による事例のコンテンツ化

- 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及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。

◇個別インタビュー事例※

岡田電機工業株式会社

Okada Hideki
Okada Yusaku

岡田英城　岡田祐作

岡田英城（おかだ・ひでき）
岡田電機工業株式会社 代表取締役

横須賀市に本社・工場を置く、プラスチック製品を中心に様々な製品を開発・生産する企業の代表取締役。大学卒業後、大手通信機メーカーで設計を学び、1988 年岡田電機工業㈱へ入社。先代の企業から大きく業態変換をさせ現在に至る。

岡田祐作（おかだ・ゆうさく）
岡田電機工業株式会社 生産本部長、株式会社 FACTORIZE 代表取締役

大学卒業後、大手金融機関にて営業職やデータ関連職として 3 年間従事し、2017 年岡田電機工業株式会社に入社。生産本部長を務める傍ら、岡田電機工業株式会社から新設分割により、株式会社 FACTORIZE を設立。人手不足かつ高齢化している日本の中小製造業に「デジタル化による負担軽減」をコンセプトに、自社開発プロダクト「軽減くん」を拡販中。

独自システム「軽減くん」の販売に向けて
セキュリティ対策を強化

――御社の事業概要と、現在なさっているサイバーセキュリティ対策をお聞かせください。

岡田英城社長●当社では、主に各種プラスチック部品の射出成型、加工、組立を行っています。売上の過半は自動車部品で、そのほか事務用什器の部品や建設の部品などです。従業員は約 60 名。工場はシフトを組み、日曜日を除いて 24 時間稼働しています。成型用の金型は、以前は中国に外注していたこともありましたが、新型コロナの感染が拡大して以降はすべて日本国内に戻しています。また、2 年ほど前に「軽減くん」という自動日報作成・原価管理ツールを独自開発し、分社化した株式会社 FACTORIZE（ファクトライズ）で昨年から販売しています。さらに新規事業として、廃棄物の再利用化にも取り組み始めました。

岡田電機工業株式会社
（横須賀／自動車部品製造業）

株式会社クロスエフェクト

Hatanaka Katsunori

畑中克宣

畑中克宣（はたなか・かつのり）
株式会社クロスエフェクト 専務取締役

大学卒業後、特殊車両製造メーカーで 3DCAD 設計に従事。2001 年にクロスエフェクト、2011 年に医療系画器シミュレーター開発のクロスメディカル、2022 年にデジタルに特化したクロスデザインを設立し、各社の専務取締役に就任。2013 年第 5 回ものづくり日本大賞内閣総理大臣賞を受賞。

「サイバーセキュリティお助け隊」の利用と UTM の導入で、経営陣の安心感が格段に向上

――最初に事業概要をお聞かせいただけませんか。

畑中●当社の事業は大きく分けて 3 つあります。第一の事業は、2001 年の創業当初から手がけている試作品の受託製作です。メーカーの開発段階の図面をお預かりして、樹脂製の試作品を製作するという事業です。もっとも、開発段階の情報は極めて機密性が高いため、当時はほとんどのメーカーは試作品製作の外部委託は行っていませんでした。しかし、創業者であり現社長である竹田は必ず試作品製作をアウトソースする日が来ると見込み、こ

株式会社クロスエフェクト
（京都／樹脂成型品製造業）

株式会社コムテックス

Kobayashi Masaaki

小林正明

小林正明（こばやし・まさあき）
株式会社コムテックス　代表取締役社長

1818 年（文政元年）創業の建設資材・専門工事の総合商社 8 代目社長。1975 年に大学を卒業後、大手総合商社で鋼管輸出を担当し、その間、2 年間メキシコに駐在（研修生）。1984 年（昭和 58 年）に当社に入社し現在に至る。

最重要のデータは、サーバ、クラウド、
オフラインの 3 か所で保管

――御社は建築・土木関係の会社ですが、業界のデジタル化はどのような状況ですか？

小林●当社の創業は 1818 年ですので、200 年近い歴史がありますが、もともとは長い間、鍋、釜、包丁などの金物を町の金物店に卸す商売をしていました。しかし、昭和 30 年代後半から 40 年代にかけてスーパーマーケットやホームセンターが登場し、金物店が淘汰されはじめましたので、このまま商売を続けていては会社が存続できないと、建設分野にシフトしました。それ以来、形鋼・鋼板といった鋼材をはじめ建築金物、屋根・外壁材、土木鉄構製品など各種建材を販売しています。また、その後、販売だけでなく工事業にも参入し、屋根・外壁、サッシ、ガードレール、基礎建設工事など建築・土木工事も手がける

株式会社コムテックス
（高崎／建材卸売・建築業）

本業務における考察

- 本業務において実施した、サイバーセキュリティ懇談会および個別取材（インタビュー）における経営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

- 従業員に、“会社の安全が自身の行動にかかっている”ことをいかに理解してもらえるかが重要。中小企業の経営者自身によるメッセージの発信が最も効果的と考える。
- 経営者が、“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り、中小企業サイバーセキュリティ対策における最大の要。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が「かかわり」を持つ機会を、戦略的に創出する必要がある。

2.セキュリティ全般に関する相談先の不足

- 多くの中小企業において、セキュリティ全般に関する客観的なアドバイスを提供する専門家が求められている。中小企業におけるシステム関連の相談先の多くは、OA商社やITベンダーの様子であるが、「ITベンダーから提案されるセキュリティ対策費用が高額である」「セキュリティ対策製品の導入後、状況を把握していない」などの状況が聞かれた。
- 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聞かれ、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。

3.懇談会形式の情報共有の機会の重要性

- 今回聞かれた悩みの多くが、社内の「運用」に依拠するものであり、運用の構築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、参考になると思われる。
- 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。

本業務における考察（つづき）

- 本業務において実施した、サイバーセキュリティ懇談会および個別取材（インタビュー）における経営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主要な観点５つが明らかになった。

4.サプライチェーンリスク対策

- 増加するサプライチェーンリスクに対処するためには、”企業規模にかかわらず、同じ傘の下の企業は同じレベルのセキュリティ対策を実施すること”がインシデント防止に役立つが、一方で、懇談会の参加者による発言から、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、統一した基準を設けることは困難が多いことも浮き彫りとなった。
- 「発注先の小規模事業者にセキュリティチェックを実施した場合、対策の費用を先方に負担させてしまう場合がある」と懸念を示す声も参加者からあがった。サプライチェーンリスク対策を推進するにあたり、中小企業だけでなく、その外注先の小規模模事業者に対する何らかの支援を講じる必要があると考えられる。

5.セキュリティ対策資金不足を克服する工夫

- 中小企業においてはセキュリティ対策充てる資金が不足するという声が多く聞かれたが、当該課題について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サービスなど、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。
- サイバーセキュリティリスク対策においては、守るべき対象を “事業継続のために、最低限必要なデータ”に絞り込むなど、工夫によって無理のない範囲で目的にかなう対策を講じることも可能と考えられる。