別紙

サイバーセキュリティお助け隊
実証参加企業事例集

この事例集は、「中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊）」に参加した企業のうち、13社へ訪問ヒアリングを行い、実証参加企業が実施した実証内容、制度・施策に対する意見、これまでの取組みと今後についてまとめたものです。

事例掲載企業一覧

	地域	業種	従業員数	資本金
A社	宮城県	情報通信業	約80名	約7,000万円
B社	宮城県	情報通信業	約20名	約1,000万円
C社	新潟県	電気通信工事業	約20名	約1,600万円
D社	新潟県	保険代理業	約20名	約500万円
E社	埼玉県	製造業	約130名	約1,700万円
F社	神奈川県	サービス業	約100名	約1,000万円
G社	石川県	製造業	約80名	約5,600万円
H社	石川県	製造業	約170名	約6,500万円
I社	愛知県	製造業	約50名	約3,000万円
J社	愛知県	サービス業	約20名	約1,000万円
K社	大阪府	製造業	約90名	約3,000万円
L社	大阪府	製造業	約40名	約3,500万円
M社	広島県	サービス業	約370名	約2,000万円

A社　宮城県		
業種	情報通信業	システム管理室を立上げ、情報セキュリティ対策を組織全体で推進
従業員数	約80名	
資本金	約7,000万円	
回答者	情報セキュリティ管理担当マネージャー	

■ 参加動機

システム管理室を立ち上げ、IT全般の統制を行っているところ、本事業を紹介され、良いタイミングと捉えて参加した。

■ 今回の実証事業で実施した対策と結果

駆け付け対応　無

対策		結果
○	UTM機器	実際に怪しげな通信パケットなどはなく、攻撃らしきものも事前にはじいていたので、侵入を許すことはなかった。ネットワークのセキュリティ監視を適宜行えて、何かあった時の対応も機敏に行うことができると感じた。
	EDRソフト	
	WEB脆弱性診断	
	標的型メール訓練	

■ 感想・意見

- 情報セキュリティ管理する上で、全社を一元的に見ていく必要があると感じた。
- システム管理室を立ち上げて、情報セキュリティ対策を組織全体で進めていくことが適切な方法と分かった。

■ 情報セキュリティ対策支援に関する制度・施策について

- 事故事例の被害金額などを含めた状況が知りたい。
- コンサルティングを含む、セキュリティに関する相談先があると良い。

実証参加企業のこれまでの取り組みと今後について

■ これまで自社で実施したセキュリティ対策

ウイルス対策ソフト導入、VPNルーターによるネットワークセキュリティ監視などを実施している。また、2019年４月からシステム管理室を発足して、IT全般の統制を行っている。

■ 情報セキュリティ対策にかけられる費用

何らかのインシデントが発生してからでないと、なかなか調達することが難しいと感じているが、セキュリティ対策の導入は検討していきたい。

■ セキュリティ対策に関する取引先からの要求

有　ISMSの取得を要求され、限られた部分での取得で対応。

■ 過去に経験したインシデント

有　WannaCry※に感染した事例がある。

※マイクロソフト社のWindowsを標的としたワーム型ランサムウェア

■ SECURITY ACTIONの宣言・活用状況

未　情報セキュリティ対策を組織全体で進めていけるようにするため、宣言を検討。

■ 情報セキュリティ対策を進める上での課題

マクロ機能※の使用を許可すると、EMOTETなどのマクロ機能を対象としたウイルスの被害に遭う可能性があるため、ワード、エクセルなどのマクロの機能を許可するかどうか検討中。

※マイクロソフト社のOffice製品に標準で搭載されている、操作を自動化するプログラム機能

B社　宮城県		
業種	情報通信業	監視装置の導入によりネットワーク監視を常時実施できることに安心感
従業員数	約20名	
資本金	約1,000万円	
回答者	情報セキュリティ管理担当マネージャー	

■ 参加動機

監視装置のようなものは今まで備わっていなかったので、興味があって本事業に参加した。

■ 今回の実証事業で実施した対策と結果

駆け付け対応　無

対策		結果
○	UTM機器	UTMの設置により、ネットワークのセキュリティ監視を常時行えることは、既存のセキュリティ対策の強化につながった。 実際に不審な通信パケットなどはなく、侵入を許すことはなかった。
	EDRソフト	
	WEB脆弱性診断	
	標的型メール訓練	

■ 感想・意見

- 少し前から、クラウドを使用しての接続サービスを始めたところだったので、監視装置の設置の結果、ネットワークのセキュリティ監視を常時行えることに、安心感があった。

■ 情報セキュリティ対策支援に関する制度・施策について

- 従業員の教育に使えるような資料、コンテンツがあると良い。
(ほぼ同じものを毎年使用しており、新しい事項が織り込まれたものなどを提供してもらえると、従来のものに一部追加などをして使えるため)

実証参加企業のこれまでの取り組みと今後について

■ これまで自社で実施したセキュリティ対策

ルーターによるフィルタリング、セキュリティ規定策定、ISMSに準拠したPDCAサイクルの実行などを行っている。

■ 情報セキュリティ対策にかけられる費用

現状はインシデント発生時、SOC※対応にかかる費用程度。セキュリティ対策にかける予算は、その都度、稟議を挙げて確保している。

※「Security Operation Center」の略称で、サイバー攻撃の検出や分析、対応策等のアドバイスを行う組織

■ セキュリティ対策に関する取引先からの要求

有	新規の顧客に、ISMSを取得していることが条件となっている相手先が多かったので取得した。

■ 過去に経験したインシデント

無

■ SECURITY ACTIONの宣言・活用状況

未	ISMSを取得していて、宣言を行う要件は揃っていると思われるので、二つ星宣言を検討。

■ 情報セキュリティ対策を進める上での課題

人的リソースの不足で、セキュリティに専従の担当者を確保することができず、兼務の担当者は通常の就業時間内では業務を完了することができない。

C社　新潟県		
業種	電気通信工事業	実証参加を機に情報セキュリティ対策を組織全体で進めていける体制を検討
従業員数	約20名	
資本金	約1,600万円	
回答者	情報セキュリティ管理担当マネージャー	

■ 参加動機

攻撃を受けていると感じながらも特にチェックできていない状況であり、情報セキュリティ対策を実施していることを、顧客等に示すことの必要性があると感じていたところ、本事業を紹介され参加した。

■ 今回の実証事業で実施した対策と結果

駆け付け対応　無

対策		結果
○	UTM機器	怪しい通信パケットの攻撃などは検知していたが、事前に排除していたので、侵入を防御出来ていた。特に問題が発生していないことを確認した。
	EDRソフト	
	WEB脆弱性診断	
	標的型メール訓練	

■ 感想・意見

- 特に問題が発生していないことを確認できてよかった。
- 参加することで、情報セキュリティ対策に対応実施していることを、外向けにアピールできるのが良いと感じた。
- 今後、Webサイトのフィルタリングも行えるようにしたい。

■ 情報セキュリティ対策支援に関する制度・施策について

- 海外からのメールは、すべて迷惑メールとして処理することが出来るツールがあると良い。

実証参加企業のこれまでの取り組みと今後について

■ これまで自社で実施したセキュリティ対策

ファイアウォールの導入、サイバー見回りの外部サービスを依頼するなどの対策を実施している。

■ 情報セキュリティ対策にかけられる費用

現状は月額10万円以内で、今後かけられる費用も同程度にとどまることになると思われ、増額することは難しい。

■ セキュリティ対策に関する取引先からの要求

有　図面、個人情報(日報)等の管理に加え、工事の予定、日程などの管理を、二要素認証で行ってほしいという要求があった。

■ 過去に経験したインシデント

有　メールサーバー等のサイバー見回りサービスの範囲外で、アタックを受けたことがある。

■ SECURITY ACTIONの宣言・活用状況

未　今回の実証参加を機に、情報セキュリティ対策を組織全体で進めていけるように、体制を検討していく。

■ 情報セキュリティ対策を進める上での課題

図面、個人情報(日報)等の管理、その他定常的に発生するデータの管理をどのようにしていけば良いか。

D社　新潟県		
業種	保険代理業	体制構築、ツールの導入など、必要な費用をかけて対策実施を検討
従業員数	約20名	
資本金	約500万円	
回答者	経営者、情報セキュリティ管理担当マネージャー	

■ 参加動機

情報セキュリティ管理担当責任者を決めてセキュリティ体制の構築を始めたところ、本事業を紹介され良い機会と考え参加した。

■ 今回の実証事業で実施した対策と結果

駆け付け対応　無

対策		結果
○	UTM機器	不審な受信パケットの検知、フィルタリングなどの対処により、特に問題の発生は見受けられなかった。
	EDRソフト	
	WEB脆弱性診断	
	標的型メール訓練	

■ 感想・意見

- 不審な受信パケットがあることなどに気付くことが出来た。(フィルタリングされているので問題なし)
- サイバーセキュリティ対策の進め方の教示が得られた。

■ 情報セキュリティ対策支援に関する制度・施策について

- 社内の従業員教育等に使える資料があると良い。
- 他者で発生しているインシデントの原因や、リテラシーに関することなどを教えてほしい。

実証参加企業のこれまでの取り組みと今後について

■ これまで自社で実施したセキュリティ対策

セキュリティ機能を有したオンラインストレージを利用することで情報取扱いの制限を設けている。PC持ち出しやUSBメモリ持ち込み不可などのルールを決めて、従業員には誓約書を提出させている。

■ 情報セキュリティ対策にかけられる費用

今後は体制の構築、ツールの導入など、ある程度のセキュリティを構築するために必要な費用はかけていく。現在月額1万円程度の費用でUTM導入を検討している。

■ セキュリティ対策に関する取引先からの要求

有　エンドポイント対策の仕組みを導入するようにとの要請があった。

■ 過去に経験したインシデント

無

■ SECURITY ACTIONの宣言・活用状況

未　情報セキュリティ管理担当責任者を決めて、セキュリティ体制の構築を始めたため、積極的に取り組む。

■ 情報セキュリティ対策を進める上での課題

現状利用しているサービスについて、クラウド上の問題が散見していることを聞いて、より安全な同等のサービスに移行していく計画であるが、現状のサービスには、既に加入している保険との関係もあり、移行にあたってそれら保険についてどのようにするか検討を要する。

E社　埼玉県		
業種	製造業	情報セキュリティはお客様の信頼を得る差別化要素と考え、取り組みを強化
従業員数	約130名	
資本金	約1,700万円	
回答者	経営者、情報セキュリティ管理担当マネージャー	

■ 参加動機

中小企業基盤整備機構から紹介された情報アドバイザーと社内若手社員3名でチームを立ち上げ、情報セキュリティに取り組んできたところ、本事業を知り参加した。

■ 今回の実証事業で実施した対策と結果

駆け付け対応　無

対策		結果
○	UTM機器	※訪問時点では、PCのWindows7からWindows10への入れ替えの関係で、IPアドレスの変更が必要のため、UTM機器が未稼働
	EDRソフト	
	WEB脆弱性診断	
	標的型メール訓練	

■ 感想・意見

- 情報セキュリティは「空気みたいなもの」で、あって当たり前だが、無くなると困る存在と考えている。
- 「出る杭は打たれる」というが、当社は「出る以上は備える」という心構えで、セキュリティに率先して取り組みたいと考えている。

■ 情報セキュリティ対策支援に関する制度・施策について

- 社内に人材がいないため、月1回程度でも、セキュリティの専門家を派遣する支援を行って欲しい。
- 社内のセキュリティ担当者を育成するプログラムを作って欲しい。

実証参加企業のこれまでの取り組みと今後について

■ これまで自社で実施したセキュリティ対策

情報セキュリティポリシーの策定、ファイアウォール導入、ウイルス対策ソフト導入などを実施している。

■ 情報セキュリティ対策にかけられる費用

情報セキュリティへの投資は必要と考えるが、効果が見えづらく費用を出しづらい面がある。業務効率化や従業員の管理負担軽減につながるIT投資は数百万円規模で実施している。

■ セキュリティ対策に関する取引先からの要求

無

■ 過去に経験したインシデント

無

■ SECURITY ACTIONの宣言・活用状況

★　情報セキュリティ規定は策定したが社内に展開していない。社内展開後に、二つ星の宣言予定。

■ 情報セキュリティ対策を進める上での課題

情報セキュリティのチーム3名は他業務と兼務のため、今回の取り組み後は解散する。継続して社内のIT全般を担当する人材を探しているが、なかなか見つからない。

F社　神奈川県		
業種	サービス業	**実証事業でインシデントを検知し、従業員のセキュリティに関する知識不足を再認識**
従業員数	約100名	
資本金	約1,000万円	
回答者	情報セキュリティ管理担当マネージャー、他1名	

■ 参加動機

当社は損害保険代理店であり、お客様の個人情報を取り扱うことも多いため、自社セキュリティに問題意識を持ったことから、本事業に参加した。

■ 今回の実証事業で実施した対策と結果

駆け付け対応　**有**

対策		結果
○	UTM機器	ハイアラートを検知したため、駆け付け対応を受けた。アラートの原因は、古い会計ソフト搭載したPC（WindowsXP）をデータ照会用に保管していたが、ネットワークに接続してプリンタ出力した際に発生。駆け付け対応で、ワームやトロイの木馬系20ファイルを駆除した。
	EDRソフト	
	WEB脆弱性診断	
	標的型メール訓練	

■ 感想・意見

- セキュリティに関する知識が無かったことから分からないことが多かったが、実証に参加して分かるようになって安心した。
- UTM導入時、IP設定の件でネットワーク業者に確認連絡をしたが、当社に専門知識が無いため、話がかみ合わず、導入に手間取った。

■ 情報セキュリティ対策支援に関する制度・施策について

- 当社が加入する県の業種団体は小さい企業が多いため、セキュリティに関する注意喚起は業種団体から実施すると良い。

実証参加企業のこれまでの取り組みと今後について

■ これまで自社で実施したセキュリティ対策

Windows10のPCについては、OS付属のセキュリティ対策ソフトを利用している。

■ 情報セキュリティ対策にかけられる費用

損害保険は取次手数料が限られているので、その中からセキュリティに関する費用を捻出することは難しい。担当者としてセキュリティ対策の重要性を感じながらも、社長に対して費用の妥当性が説明できない。

■ セキュリティ対策に関する取引先からの要求

無

■ 過去に経験したインシデント

無

■ SECURITY ACTIONの宣言・活用状況

未　損害保険の営業の際にマークがあると信用につながると考えるため、宣言を検討する。

■ 情報セキュリティ対策を進める上での課題

拠点のPCの台数が多く、Windows7のサポート終了に伴う更新など費用面が課題である。また、中小企業はセキュリティに対する知識が不足しているため、従業員の教育が課題である。

G社　石川県		
業種	製造業	**組織全体の脆弱性や脅威を監視するサービスの有効性を実感**
従業員数	約80名	
資本金	約5,600万円	
回答者	情報セキュリティ管理担当者	

■ 参加動機

自社のセキュリティ対策状況と自社に対するサイバー攻撃の状況を知りたかったため、本事業に参加した。

■ 今回の実証事業で実施した対策と結果

駆け付け対応　**無**

対策		結果
	UTM機器	OSアップグレード及びオフィスパッチに関する脆弱性を検知し、対象の３台に対して対策を実施した。
○	EDRソフト	
○	WEB脆弱性診断	
	標的型メール訓練	

■ 感想・意見

- 当社は「１人情シス」のため、月次レポートにより全体の脆弱性や脅威を見てくれるサービスは非常に助かる。
- レポートについては、専門用語が多く、また細かいため、もう少し中小企業向けに分かりやすくフィードバックしていただきたい。

■ 情報セキュリティ対策支援に関する制度・施策について

- WEBの定期的なチェックが大変なため、手間がかからず分かりやすい情報発信をお願いしたい。
- IPAの施策や支援ツールについての認知度がより向上すると、社内での説明し易さの観点から対策推進の原動力になる。

実証参加企業のこれまでの取り組みと今後について

■ これまで自社で実施したセキュリティ対策

ウイルス対策ソフトの導入、ファイアウォールの設置、物理的な遮断、定期的なバックアップなどを実施している。また、メールでの情報共有を定期的に実施している。

■ 情報セキュリティ対策にかけられる費用

年間10万円以下。目に見えない対策のため経営者に対して説明しづらく、セキュリティ対策以外の操作性向上のための投資などが優先される。

■ セキュリティ対策に関する取引先からの要求

無　セキュリティ対策を契約上明記されることはあまりない（メール誤送信防止くらい）。

■ 過去に経験したインシデント

有　ヒューマンエラーに起因するメール誤送信の経験はあるが、周囲を含めてウイルス感染や情報漏えいは発生していない。

■ SECURITY ACTIONの宣言・活用状況

未　「5分でできる！情報セキュリティ自社診断」を実施済みのため、宣言を検討する。

■ 情報セキュリティ対策を進める上での課題

個人顧客の情報も多く取り扱っているため、個人情報の管理徹底をどのようにするかが課題である。また、セキュリティリスクに対する経営者の意識は高い方だと感じているが、さらなる啓発が必要。

H社　石川県		
業種	製造業	取引先からの要求が高まるなか、業界平均を踏まえたセキュリティ対策を推進
従業員数	約170名	
資本金	約6,500万円	
回答者	経営者、情報セキュリティ管理担当者	

■ 参加動機

同業他社（特に同業種同規模の企業）における取組状況を知りたかったため、本事業に参加した。

■ 今回の実証事業で実施した対策と結果

駆け付け対応　無

対策		結果
	UTM機器	Windows7に対するアップグレードの通知、またアップグレードに伴いインストール済みの特殊ソフトの交換対応など レポート及び助言を提供してもらったことで、対策を進めることができた。
○	EDRソフト	
	WEB脆弱性診断	
	標的型メール訓練	

■ 感想・意見

- 有意義なサービスと思うが、継続するかは料金との兼ね合いとなる。
- 最低限のサービスとオプションで必要な機能を選べるようになると良い。ただし、当社だと総務の担当がセキュリティを兼務していることもあり、ワンパッケージでなんでもやってくれると非常に助かる。

■ 情報セキュリティ対策支援に関する制度・施策について

- 個社の取組を進めるためには、業界団体が旗振り役となって何らかの支援ができると良いのではないか。
- 政府の動き、支援策についての情報をタイムリーにもらいたい。

実証参加企業のこれまでの取り組みと今後について

■ これまで自社で実施したセキュリティ対策

ウイルス対策ソフト、OS対策（定期的なパッチ対応）、UTM設置などを実施している。また、ベンダーを講師に招き、全社員を対象とする社内研修を不定期で開催している。

■ 情報セキュリティ対策にかけられる費用

現時点、UTMで年間100万円（5年契約500万円）、ウイルス対策は年間30万円（社内PC100台）など費用がかかっているため、これ以上の対策費は厳しい。

■ セキュリティ対策に関する取引先からの要求

有　大企業から機密保持契約を求められることが多くなってきている。セキュリティ対策に関する調査アンケートを取られることがある。

■ 過去に経験したインシデント

有　2～3年前に、ウイルス感染の疑いから全システムを停止し、ウイルスチェックを全数に対して行った。（ウイルス検出はなかった）

■ SECURITY ACTIONの宣言・活用状況

未　宣言事業者向けのメルマガは非常に関心があるため、宣言を検討する。

■ 情報セキュリティ対策を進める上での課題

昨今は企画の段階から客先に入りこんで仕事を行うため、機微な情報を得ることがこれまでに比べて多くなってきており、現状の管理で問題ないかが不安な状況。その他、当社の規模でPC100台は多い方であると認識しており、モバイル活用も検討しているが安全性が懸念され進んでいない。

I社　愛知県		
業種	製造業	**実証参加を通じて監視装置の有効性を認識**
従業員数	約50名	
資本金	約3,000万円	
回答者	経営者、情報セキュリティ管理担当マネージャー	

■ 参加動機

取引先から要求されたアンケートについて、質問内容の大半が対応できていなかったため、セキュリティへの取り組みを検討するために本事業に参加した。

■ 今回の実証事業で実施した対策と結果

駆け付け対応　無

対策		結果
○	UTM機器	怪しげな通信パケット(ポートスキャン含む)などの攻撃らしきものを検知したが、排除することができ、特に問題の発生等はなかった。 サイバーセキュリティ演習に参加した。
	EDRソフト	
	WEB脆弱性診断	
	標的型メール訓練	

■ 感想・意見

- UTMを使ってみて、入れておくことにより安心感がある。
- 参加した演習はたいへん役にたったと感じている。

■ 情報セキュリティ対策支援に関する制度・施策について

- 研修、演習などの実施は必要と考えており、特に経営者向けのセミナーなどがあると良い。
- コンサルティングをお願いできる先を知りたい。

実証参加企業のこれまでの取り組みと今後について

■ これまで自社で実施したセキュリティ対策

ウイルス対策ソフトを導入している。また、簡単な図面などはそのまま送信しているが、重要な情報はパスワードロックで送信している。

■ 情報セキュリティ対策にかけられる費用

UTM設置で、月間1万円（年間12万円）程度のサービスがあれば導入したい。

■ セキュリティ対策に関する取引先からの要求

有	ウイルス対策ソフトの導入を要求された。また、過去に取引先から訓練メールを送信されたことがある。

■ 過去に経験したインシデント

無	

■ SECURITY ACTIONの宣言・活用状況

未	今後、宣言を含めて、体制を構築していく必要があると認識している。

■ 情報セキュリティ対策を進める上での課題

セキュリティ対策を進めるにあたって、どのようなところから始めていけば良いか、どのように従業員等に伝えていけば良いか。

J社　愛知県		
業種	サービス業	**監視装置の導入により不審な通信の検知の重要性を認識**
従業員数	約20名	
資本金	約1,000万円	
回答者	情報セキュリティ管理担当マネージャー	

■ 参加動機

付き合いのあるベンダーからウイルス対策ソフト更新のたびにUTM設置の提案をされていたところ、本事業を紹介され参加した。

■ 今回の実証事業で実施した対策と結果

駆け付け対応　**無**

対策		結果
○	UTM機器	出入り外注業者が、社内LANに接続していたところ外国(米国)のサーバーと通信していたものを不正な接続とみなして検出したため、許可した端末だけ接続できるようにした。 サイバーセキュリティ演習に参加した。
	EDRソフト	
	WEB脆弱性診断	
	標的型メール訓練	

■ 感想・意見

- 参加した演習はためになったと感じている。
- 現在使っているウイルス対策ソフトのベンダーだけでなく、他社の考えも聞くことができてよかった。

■ 情報セキュリティ対策支援に関する制度・施策について

- 演習形式のものは役に立つと考える。
- 自動車業界のJAFのような情報共有のしくみがあると良い。
- コンサルティングの相談先があれば良い。

実証参加企業のこれまでの取り組みと今後について

■ これまで自社で実施したセキュリティ対策

ウイルス対策ソフトを導入している。

■ 情報セキュリティ対策にかけられる費用

月額１万円から３万円程度。UTM及び遠隔監視で月額3万円程度で提案されたが、導入していない。

■ セキュリティ対策に関する取引先からの要求

無

■ 過去に経験したインシデント

無

■ SECURITY ACTIONの宣言・活用状況

未　少人数で対応できる宣言の手引きなどがあると良いが、取り組み実施に向けて検討する。

■ 情報セキュリティ対策を進める上での課題

UTMの設置などはしっかりしたサポートがないと中小企業は導入できず、対策を諦めてしまう。

K社　大阪府		
業種	製造業	本事業と並行して情報セキュリティポリシーの策定も実施
従業員数	約90名	
資本金	約3,000万円	
回答者	情報セキュリティ管理担当マネージャー/担当者	

■ 参加動機

セキュリティに関しては、中小企業では大企業と同じような管理はできないと感じる一方で、情報流出したときの影響は中小企業の方が大きいことを心配していたところ、本事業を紹介され参加した。

■ 今回の実証事業で実施した対策と結果

駆け付け対応　有

対策		結果
○	UTM機器	業務用PC数台から、HTTPベーシック認証のアラートが検出されたため、駆け付け対応になった。当該PCに対してウイルススキャンを実施したが、マルウェア等は検知されなかった（過検知）。
	EDRソフト	
	WEB脆弱性診断	
	標的型メール訓練	

■ 感想・意見

- UTMのアラート文がメールで届いて、コールセンターとやり取りをしたが、意味が良く理解できなかった。
- 本事業の内容が良かったため、「情報セキュリティマネジメント指導」事業にも参加して、情報セキュリティポリシーの策定を行った。

■ 情報セキュリティ対策支援に関する制度・施策について

- 中小企業同士、業界とか地域での横のネットワークで、情報セキュリティに関する情報共有ができたら良い。
- 当社所在の工業団地は横のつながりが薄いが、業界団体では情報共有はできると思う。

実証参加企業のこれまでの取り組みと今後について

■ これまで自社で実施したセキュリティ対策

ウイルス対策ソフトを導入している。また、メールでの図面のやり取りが多いため、メール誤送信対策オプションを契約して添付ファイルの暗号化を行っている。

■ 情報セキュリティ対策にかけられる費用

月額数千円から1万円程度。セキュリティ対策をきちんと行うと、企業価値が上がると感じているため、取り組みは継続したい。

■ セキュリティ対策に関する取引先からの要求

有　図面の取扱いがあり、取引先からセキュリティ管理の要請がある

■ 過去に経験したインシデント

無

■ SECURITY ACTIONの宣言・活用状況

★★　「情報セキュリティマネジメント指導」を受けて二つ星を宣言。

■ 情報セキュリティ対策を進める上での課題

経営者に対してセキュリティ対策の必要性とかかる費用の妥当性を説明留することが難しい。そのため、UTMのレポートはテクニカルなので、経営者が見て分かるレポートがあるとありがたい。

L社　大阪府		
業種	製造業	**実証参加を通じて社内ネットワークの可視化を実現**
従業員数	約40名	
資本金	約3,500万円	
回答者	経営者、情報セキュリティ管理担当マネージャー	

■ 参加動機

日頃から中小企業のワキは甘いと感じていたところ、本事業を紹介され参加した。

■ 今回の実証事業で実施した対策と結果

駆け付け対応　有

対策		結果
○	UTM機器	不審な通信を検知し、駆け付け対応を実施したが、該当の端末を発見できなかった。その後の確認で、会社管理外のPCがあることが分かり、マルウェア感染の可能性があるため2回目の駆け付け対応を実施し、定期的に外部通信を行っているソフトのアンインストールを実施。
	EDRソフト	
	WEB脆弱性診断	
	標的型メール訓練	

■ 感想・意見

- UTM設置でネットワークの見える化ができた。
- 従業者にサイバーセキュリティの意識が芽生え、気を付けるようになった。

■ 情報セキュリティ対策支援に関する制度・施策について

- 地域産業でのセキュリティに関する情報共有はあった方が良い。
- PCのOSバージョンアップ対応等、公的な費用援助があると良い。

実証参加企業のこれまでの取り組みと今後について

■ これまで自社で実施したセキュリティ対策

インターネット接続、メール送受信は１台のPC（Win10／ウイルスバスターをインストール）のみに限定している。取引先との受発注は、専用回線（INS64）で行っている。

■ 情報セキュリティ対策にかけられる費用

中小企業は生産性をあげてコストを下げないと生き残れないので、なかなかセキュリティにかける費用が確保できない。

■ セキュリティ対策に関する取引先からの要求

無

■ 過去に経験したインシデント

無

■ SECURITY ACTIONの宣言・活用状況

未　一つ星宣言を検討。

■ 情報セキュリティ対策を進める上での課題

メール受信できる１台のPC（Win10）以外は、すべてWinXPのPCだが、使用している受発注パッケージソフトがWin10にバージョンアップできるか不明。今後、インターネットEDIが必要になる場合、PCを買い換える必要があり、対応に困っている。

M社　広島県		
業種	サービス業	**監視装置の導入により正常な運用を確認でき安心感**
従業員数	約370名	
資本金	約2,000万円	
回答者	経営者	

■ 参加動機

セミナーで本事業を知り、営業所について、情報セキュリティ対策の必要性を感じたため参加した。
※本社では体制の構築がなされていて、ISMSを取得している。

■ 今回の実証事業で実施した対策と結果

駆け付け対応　無

対策		結果
○	UTM機器	ファームウェアの更新がなされていないことや脆弱性があることが検知でき、対策を実施することができた。
○	EDRソフト	
	WEB脆弱性診断	
	標的型メール訓練	

■ 感想・意見

- UTMを導入したが、ネットワークなどのシステムへの負荷がかかるわけでなく、継続できそうである。
- 本社から離れているため、営業所近くの業者がインシデント対応、管理を行っている。

■ 情報セキュリティ対策支援に関する制度・施策について

- 情報セキュリティに関するリスクアセスメントを行える資料、ツールなどがあると良い。

実証参加企業のこれまでの取り組みと今後について

■ これまで自社で実施したセキュリティ対策

ウイルス対策ソフトを導入している。また、情報セキュリティポリシーは策定済で、社内報で従業員へのセキュリティ啓発を行って、現場サイドの端末の対応を各自にさせている。

■ 情報セキュリティ対策にかけられる費用

費用がかからなければ現在の実証事業の導入のものを継続できる。

■ セキュリティ対策に関する取引先からの要求

有	自己チェックを促すような機会が年に２回ほどある。また、秘密保持契約をグループ会社の親会社にするようにとの指示があった。

■ 過去に経験したインシデント

有	メールの誤送信、なりすましメールでアドレスが不正利用された。

■ SECURITY ACTIONの宣言・活用状況

未	一つ星宣言を検討。（本社は二つ星を宣言できるレベル）

■ 情報セキュリティ対策を進める上での課題

従業員の教育の観点がもっとも重要と考えているが、どのように従業員等に伝えていけば良いかが課題である。その他、スマートフォンのセキュリティに必要性を感じている。