東京都

令和5年度

中小企業サイバーセキュリティ対策継続支援事業

事例集

はじめに

東京都では、中小企業のサイバーセキュリティ対策強化のため、サイバーセキュリティに関する普及啓発やセキュリティ機器・ソフトの導入、情報セキュリティポリシーの策定を支援してまいりました。加えて、各社がサイバーセキュリティ対策を継続的に進める上で、人材面やノウハウ面でのリソース不足が課題となっていると認識し、令和4年度より、継続的なサイバーセキュリティ対策の実現に向けて、サイバーセキュリティ人材の育成等を目的とした「中小企業サイバーセキュリティ対策継続支援事業」を実施しております。

本事業では、企業のセキュリティ担当者等を対象に、自社の状況に応じて必要なセキュリティ対策を選択・検討し、実践することを目指して、サイバーセキュリティを取り巻く社会背景や企業経営におけるセキュリティ対策の必要性から、セキュリティ対策を実践するためのフレームワーク、具体的な対応事項・手順まで、セキュリティ対策の全容を体系的に解説するセミナーを開催しました。また、セミナーと同日に開催するワークショップにて、セキュリティに関するディスカッションやグループワークを行い、セミナーで培った知識・ノウハウのアウトプットを実践し、参加企業間で各社の取組の共有や自社のセキュリティ対策の振り返りを行いました。更に、セミナー・ワークショップで洗い出された各社のセキュリティ上の課題については、専門家を企業に派遣し、個社の課題解決に向けて伴走支援を実施しました。

この事例集では、令和5年度の本事業の参加企業30社における具体的な支援・取組などについて紹介しております。業種や人数規模、事業内容といった企業の状況によって、セキュリティの課題やとり得る対策・手法は多種多様にあり、サイバー攻撃のトレンドやその対策・手法も日々変化しております。そうした中、自社に適したセキュリティ対策が何かを検討し、実行することは、企業経営に欠かせない取組であり、その中核を担うサイバーセキュリティ人材がいかに企業にとって重要な存在かを事例集を通じて感じていただけますと幸いです。

新型コロナウイルス感染症等の影響により、社会におけるDXは急速に進行しましたが、本来、DXと車輪の両輪であるサイバーセキュリティ対策は後手になりがちです。ぜひ事例集を手に取って、様々な事例からヒントを見つけていただき、自社でのセキュリティ対策の実践にお役立ていただけますと幸いです。

最後に、本事例集の作成にあたり、取材や原稿作成に多大なご協力をいただきました企業の皆様に厚くお礼申し上げます。

令和5年度

中小企業サイバーセキュリティ対策継続支援事業

事例集

目次

事業概要

中小企業サイバーセキュリティ対策継続支援事業について

新型コロナウイルス感染症の影響により、社会におけるDX化が急速に進行していますが、多くの中小企業において、DXと車輪の両輪であるべきサイバーセキュリティ対策を継続的に実施していくための体制整備が喫緊の課題となっています。

この状況を踏まえ、東京都では、セキュリティ対策の普及啓発に加え、セキュリティ機器の導入支援等のハード面の整備を進めていますが、こうした整備を実施した後も、各中小企業のリソース不足（人材面・ノウハウ面）が、継続的なセキュリティ対策の実施に向けて大きな障害になると予想されます。

そこで本事業では、基本的なセキュリティ機器を備え、セキュリティに関する方針、ルール、対策を決めるところまでは実施したものの、その先どうしたらいいのか分からない、自社だけでは対策ができないという不安を抱える中小企業の皆様を対象に、セキュリティ対策の基本を再確認し、課題解決などの手法を学ぶことで、社内にて継続的なサイバーセキュリティ対策ができる人材を育成します。

また、支援実施過程で使用するテキストや事例集など、本事業の取組を広く社会へ公開し、中小企業の皆様が自社でセキュリティ対策を実行する際、困った時に使うことができるツールとして活用していただくことで、中小企業全体の体制強化を目指します。

支援全体像

取組実行
専門家と決めた取組内容やセミナーで得た知見、ワークショップの事例を参考に取組を実行します。

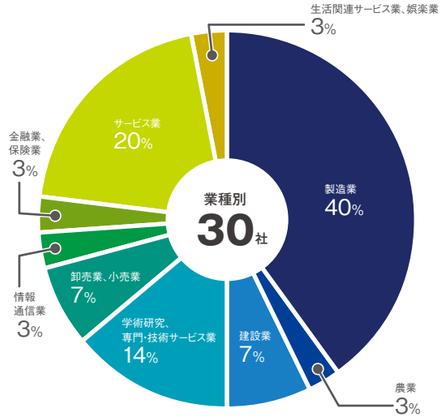
セミナー
導入済のセキュリティ機器の日常的な運用方法や業務内容に沿ったセキュリティルールの策定方法など、中小企業の皆様が自主的にセキュリティ対策業務を運営する上で生じる疑問点の解決に直接役立つ、実践的な知識・ノウハウを講義形式でお伝えします。

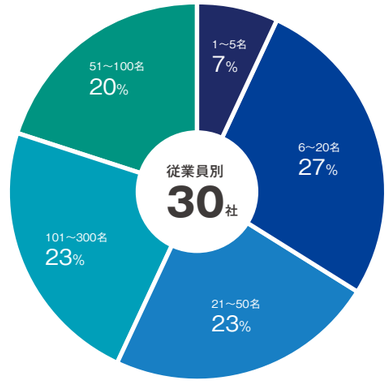
ワークショップ
中小企業の皆様が直面しているセキュリティ対策上の困難について、参加企業の皆様同士で、それぞれの課題に一緒に取り組み、解決策を考えます。自社の問題だけでなく、他社の事例に触れることで、様々な課題の解決に向けた引き出しとなる知識を得られます。

専門家派遣
ワークショップで洗い出した課題を中心に、企業が直面しているセキュリティ上の問題点解決や、社内体制構築へ向けて専門家が支援を行います。

支援対象企業の属性

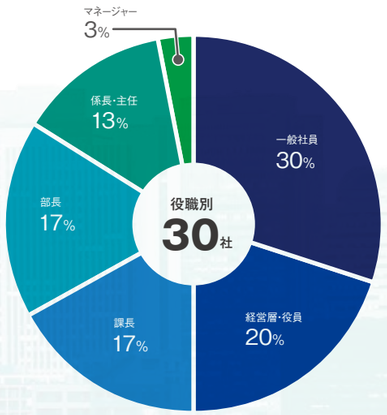
様々な業種や規模の都内中小企業30社にご参加いただきました。





参加者の属性

経営層やセキュリティ担当者など、多様な階層、部門の方30名の方にご参加いただきました。



事業での取組

1 セミナー 全10回

セキュリティ対策の知識だけでなく、役割の違いやDXの推進といった、今後の中小企業のセキュリティを担う中心人物の育成を目指し、「セキュリティ担当の役割理解」、「セキュリティ関係の知識強化」、「今後のアクション」とステップを分けて全10回のセミナーを行いました。

2 ワークショップ 全10回

ワークショップはセミナーと同日開催で全10回、5～6名のグループ形式で行いました。多様なセキュリティ課題を疑似体験することで、未知の課題にも対応できるようになることを目指し、セミナーで得た知識をもとに、グループメンバーで課題や取組事例、問題点を共有し、他社の事例に対して全員で対策を検討・議論しました。

	1	2	3	4	5	6	7	8	9	10
	● 第1回	● 第2回	● 第3回	● 第4回	● 第5回	● 第6回	● 第7回	● 第8回	● 第9回	● 第10回
	サイバーセキュリティを取り巻く環境、および中小企業に求められるセキュリティ対策	これからの企業経営で必要な守りのIT投資と攻めのIT投資 経営投資としてのサイバーセキュリティ対策	サイバーセキュリティに関する国の方針、施策およびサイバー脅威の動向	サイバーセキュリティ対策を進めるうえで活用できるフレームワーク	セキュリティ対策基準の策定 脅威、脆弱性、リスクの定義および関係性	リスクの特定、評価について理解し、対策案を立てる	インシデント対応計画の策定をしようクイックアプローチ/ベースラインアプローチ	インシデントレスポンスの対応について理解する 実施手順・実施者マニュアル	インシデントレスポンスの事後活動について理解する	全体総括 振り返りと今後のアクションについて
	自社で活用しているIT及び実施できているセキュリティ対策やセキュリティ課題と対策について整理する	仮想会社の取組に対するリスクを明確化し、具体的な対応策として攻めと守りのIT戦略を議論し、具体的な提案を整理する	10大脅威の脆弱性がどのようなものかを理解し、対応策を講じる	ISMSの管理手順の作り方の1つを理解する	情報資産台帳の作り方を理解する	リスクの特定、評価について理解し、対策案を立てられるようになる	インシデント対応計画の策定ができるようになる	インシデントレスポンスの対応について理解する	インシデントハンドリングの対応を理解する	今後の改善点やワークショップ内でのメリット・デメリットを共有し、今後の情報セキュリティ対策に活かす

3 専門家派遣 1社につき全4回

参加企業の皆様がワークショップで洗い出した課題や、企業が直面しているセキュリティ上の問題点解決へ向け、多様な得意分野を持つ専門家（ネットワーク設計・構築などの技術分野での経験、リスク分析、セキュリティ事故対応や再発防止策の検証、監査、セキュリティ教育、各種セミナー・支援の講師経験など）が、セミナー・ワークショップで得た気づきや知識を活かし、参加企業の皆様が自ら対策を立案できるようサポートしました。

第１回

専門家が6セクション、23項目からなる調査表を使用して、自社のセキュリティ状況を網羅的にヒアリングを実施。

第２回

第1回のヒアリング結果を元に企業の現状のセキュリティ課題をセクション毎に0～5ポイントで評価して企業にフィードバック。企業の改善計画立案をサポート。

第３回

第2回で立案した計画の進捗状況をチェック。個別課題を進めるにあたっての参考資料の把握と対応方針の検討、改善計画着手後に表出した課題や疑問点にも丁寧に対応します。

第４回

専門家派遣実施後の取組成果を確認。また次年度に向けた課題の洗い出しと目標設定、計画書作成の提案、継続的なセキュリティ改善を行う上で必要な活動の紹介・課題化など、各企業の自立に向けたお手伝いを実施します。

事業での取組

参加企業のセキュリティ体制と支援テーマ

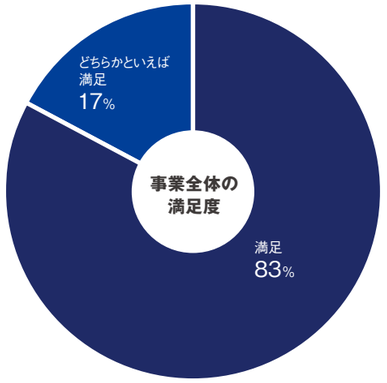
ものづくり企業	従業員数	セキュリティ体制					支援テーマ					
		1名体制	複数	専任	兼務	経営者	ネットワークセキュリティ	エンドポイントセキュリティ	モバイルデバイス	データ保護	セキュリティ意識と教育	外部パートナーとの関係
化粧品原料製造業 A 社	1～5	●			●	●	●				●	●
総合建築業 B 社	1～5	●			●		●				●	●
印刷業 C 社	6～20		●		●	●	●				●	●
産業用機械製造業 D 社	21～50		●		●		●	●				
展示ディスプレイ業 E 社	21～50		●		●					●	●	
計測機械器具製造業 F 社	51～100	●			●		●		●		●	
金属製品製造業 G 社	51～100		●		●		●				●	
医療用機器製造業 H 社	51～100		●		●		●				●	
環境対策コンサルティング業 I 社	51～100		●		●		●				●	●
農業支援サービス業 J 社	101～300	●			●		●			●		
機械工具製造業 K 社	101～300	●			●		●				●	
電子機器製造業 L 社	101～300		●		●		●				●	
オフィス用品製造業 M 社	101～300		●		●		●				●	●
金属建材加工業 N 社	101～300		●		●					●	●	
電子部品製造業 O 社	101～300		●		●						●	●

サービス企業	従業員数	セキュリティ体制					支援テーマ					
		1名体制	複数	専任	兼務	経営者	ネットワークセキュリティ	エンドポイントセキュリティ	モバイルデバイス	データ保護	セキュリティ意識と教育	外部パートナーとの関係
専門技術コンサルティング業 A社	6～20	●			●	●	●				●	●
金融情報サービス業 B 社	6～20	●			●		●	●			●	
葬祭サービス業 C 社	6～20	●			●		●				●	
機械工具関連卸売業 D 社	6～20	●			●			●		●	●	
人材育成支援サービス業 E 社	6～20		●		●	●		●			●	●
公認会計士事務所 F 社	6～20		●		●		●				●	●
電子機械器具卸売業 G 社	6～20		●		●			●		●	●	
労務コンサルタント業 H 社	21～50		●		●	●	●			●	●	
デザイン業 I 社	21～50		●		●		●	●				●
IT ソリューション業 J 社	21～50		●		●		●		●		●	
機械設計技術サービス業 K 社	21～50		●		●		●				●	
インターネットサービス業 L 社	21～50		●		●		●				●	
精密機器輸送業 M 社	51～100		●		●		●				●	
人材サービス業 N 社	51～100	●			●						●	●
IT ソリューション業 O 社	101～300	●			●	●		●			●	

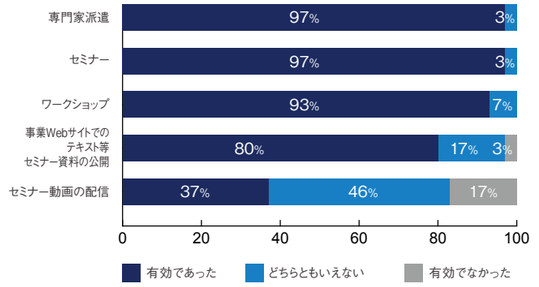
アンケート

本事業の参加者に対して、支援終了後にアンケート調査を実施いたしました。

事業全体の満足度

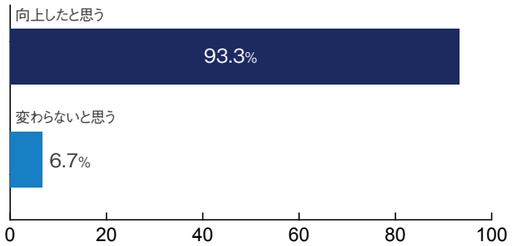


本事業の支援内容はいかがでしたか？



本事業全体の満足度については、83%の参加者が「満足」を、17%が「どちらかと言えば満足」と回答した。また、支援内容に関しては、セミナーと専門家派遣が有効であると感じた参加者が最も多かった。

事業参加前と比べて貴社の情報セキュリティレベルは向上しましたか？

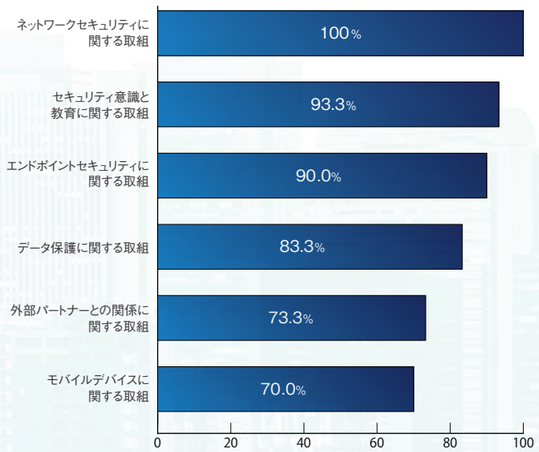


向上したと思う理由

1	自社に必要な対策の向上を図れたから	35.6%
2	従業員に対して教育を実施したから	21.9%
3	セキュリティ体制を強化できたから	20.5%
4	規程類が整備できたから	17.8%
5	その他	4.2%

事業に参加した企業の93.3%が、事業参加前と比べて情報セキュリティレベルが向上したと回答した。向上した理由として、自社に必要な対策の向上を挙げた企業が最も多く、続いて従業員への教育やセキュリティ体制の強化が挙げられた。またその他として、システム担当者の情報セキュリティの知識レベルの大幅な向上や、課題の明確化などがあった。

本事業を通じて取り組んだことは何ですか

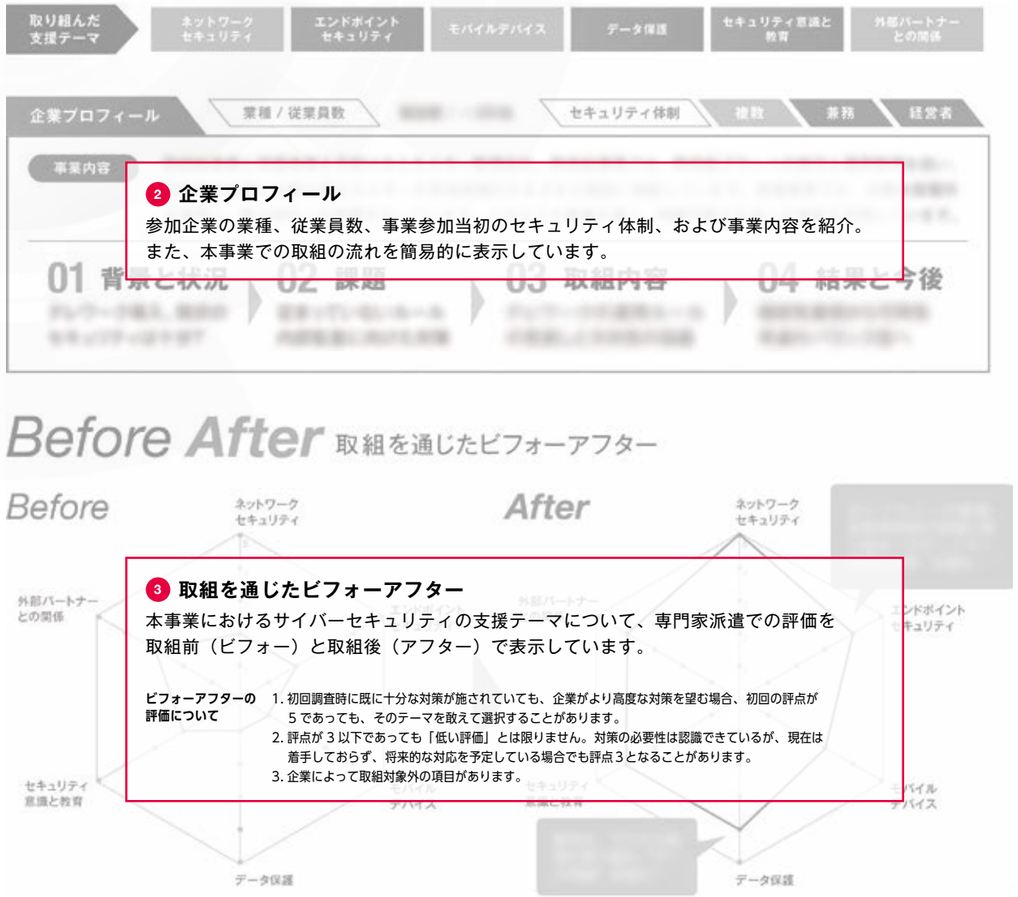


本事業を通じて、全参加企業がネットワークセキュリティに関する取組を行っている。この項目ではUTM等のネットワーク機器のアップデートやログの保管期間の見直しなど、管理強化がテーマとなっており、中小企業にとって最も取組が必要な項目だと考えられる。

次に多かった取組は「セキュリティ意識と教育に関する取組」(93.3%)であった。このテーマでは、定期的なセキュリティ教育の計画策定や最新の攻撃手法を盛り込んだ訓練などの具体的な教育内容の検討、情報セキュリティ規程の整備や具体的なルールなどを定めたガイドラインの策定、インシデント発生時の対応フローの作成や対応体制づくりなどに取り組んだ企業が多かった。

「エンドポイントセキュリティに関する取組」(90.0%)では、OSやウイルス対策ソフトウェアのアップデートの管理や資産管理の強化などの取組を行った。参加企業の多くが本事業を通じて情報セキュリティの向上に取り組むことができ、またその成果が出ていると言える。

事例の見方



1 取り組んだ支援テーマ
本事業における６つの支援テーマのうち、支援を行ったテーマを表示しています。

2 企業プロフィール
参加企業の業種、従業員数、事業参加当初のセキュリティ体制、および事業内容を紹介。
また、本事業での取組の流れを簡易的に表示しています。

3 取組を通じたビフォーアフター
本事業におけるサイバーセキュリティの支援テーマについて、専門家派遣での評価を取組前（ビフォー）と取組後（アフター）で表示しています。

ビフォーアフターの評価について
1. 初回調査時に既に十分な対策が施されていても、企業がより高度な対策を望む場合、初回の評点が５であっても、そのテーマを敢えて選択することがあります。
2. 評点が３以下であっても「低い評価」とは限りません。対策の必要性は認識できているが、現在は着手しておらず、将来的な対応を予定している場合でも評点３となることがあります。
3. 企業によって取組対象外の項目があります。

4 背景と課題
本事業の参加背景や参加時のサイバーセキュリティの対策状況を紹介しています。

5 セキュリティ課題
本事業の参加当初に企業側が認識していた課題と、専門家派遣の実施後に新たに明らかになった課題を整理しています。

6 取組内容
本事業で明確化された課題に対し、企業が取り組んだ内容を詳しく紹介しています。また、取組の流れをステップごとに表示しています。

7 結果と今後
本事業でのセキュリティ対策の取組の結果や効果、今後の展開について紹介しています。

8 経営者／参加者の声
本事業に参加しての所感や振り返りについて、経営層と実際に参加した担当者双方の視点で紹介しています。

フレームワークを活用し、自社で対応するべきセキュリティ対策を策定・推進

取り組んだ支援テーマ：ネットワークセキュリティ / エンドポイントセキュリティ / モバイルデバイス / データ保護 / セキュリティ意識と教育 / 外部パートナーとの関係

企業プロフィール　業種 / 従業員数：製造業 / ～５名　セキュリティ体制：1名体制 / 兼務 / 経営者

事業内容　化粧品原料の開発、製造、輸出入、販売を行う企業です。天然由来の原料を取り扱うことにより、環境に配慮した化粧品原料の開発を進めています。化粧品メーカーを主な取引先として、BtoBでビジネスを展開しています。

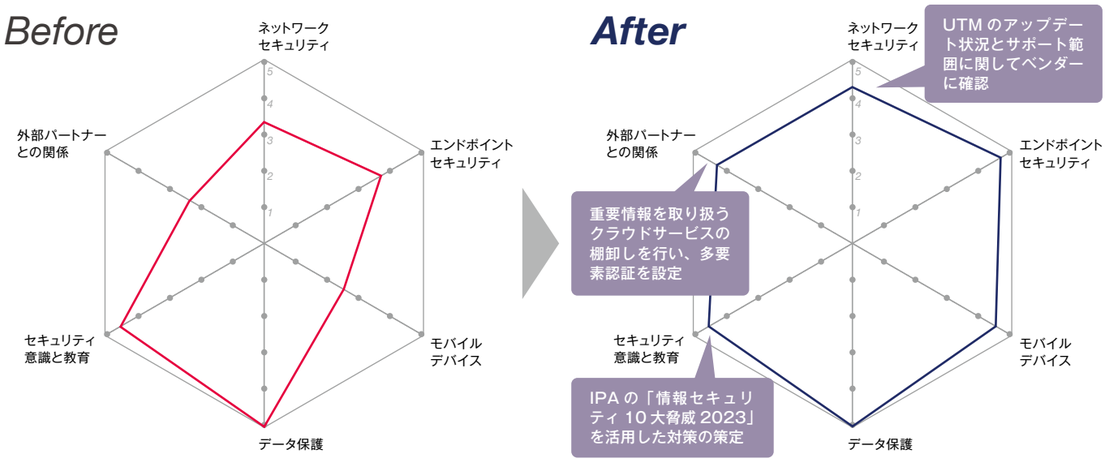
01 背景と状況　経営者1名体制でセキュリティ対策を推進

02 課題　自社に必要な対策や情報資産が整理されていない

03 取組内容　フレームワークを活用したセキュリティ対策の策定

04 結果と今後　明確化された対策の実行と社内教育の強化を実現

Before **After** 取組を通じたビフォーアフター



01 背景と状況

小規模事業者として人的資源やコストに制約がある中でセキュリティ対策を推進

セキュリティ担当は経営者が兼務

投入可能な人的資源やコストに制約

UTMは自社で導入済み

小規模事業者であるため、セキュリティ担当は経営者が兼任しています。セキュリティに関わる専門人材は配置できず、投資できるコストにも制約がある中で、経営者1名がセキュリティ知識を学びながら対応を進め、UTM（Unified Threat Management）も導入しています。

02 セキュリティ課題

自社に必要な対策や情報資産が整理されていない

当初の課題
- 必要なセキュリティ対策の過不足が把握できていない
- UTM の運用状況が管理できていない
- 重要情報を取り扱うクラウドサービスの棚卸しが未実施

専門家派遣支援で明らかになった課題
- 自社の情報資産の整理や把握ができていない
- UTM のアップデート状況や責任範囲が把握できていない
- 自社の業務に合わせたセキュリティ規程の見直しが必要

03 取組内容

STEP 1　本事業の専門家派遣により、自社のセキュリティ状況と必要な対策を明確化

本事業の専門家からのアドバイスにより、現状のセキュリティ課題を明確化し必要なセキュリティ対策を検討することにしました。まず、自社にとって重要な情報資産を明確にするため、情報資産の整理および把握から着手しました。

STEP 2　重要情報を取り扱うクラウドサービスの棚卸しを完了し、多要素認証機能を導入

顧客情報や製品情報など、重要な情報を取り扱うクラウドサービスに関する棚卸しを行いました。本事業の専門家と相談して、個々のクラウドサービスごとに想定されるリスクを評価するとともに、必要なセキュリティ対策の検討を行い、多要素認証の機能があるクラウドサービスについては設定を追加しました。

STEP 3　UTMのアップデート状況やサポート範囲に関してベンダーに確認

UTMの活用状況が把握できていないため、UTMを提供しているベンダーのサポート範囲の確認を進めました。その結果、ファームウェアの更新はベンダー側のサポート範囲となっている契約であることが確認できました。

STEP 4　IPAの「情報セキュリティ10大脅威2023」を活用した対策の策定

セキュリティ対策の具体的な対応を定めた手順書を作成するため、IPAが公開している「情報セキュリティ10大脅威2023」をわかりやすい「フレームワーク」として活用し、セミナー・ワークショップで学んだISMSの管理策と組み合わせて対策内容を検討することにしました。

フレームワークを活用したセキュリティ対策の策定

セキュリティ対策については、ベンダーのサポートを受けながら自社で対応可能な範囲で対策しているため、「自社のセキュリティ対策状況の過不足を明確にしたい」ということが本事業への参加目的の一つでした。本事業の専門家派遣におけるヒアリングを通して、さまざまな課題が洗い出されました。そこで、本事業の専門家のアドバイスにより、まず、社内の重要な情報資産の整理を行い、重要な情報を取り扱うクラウドサービスの棚卸しを進めるとともに、多要素認証機能を利用するように設定しました。また、ネットワークセキュリティ関連では、導入しているUTMのアップデート状況やセキュリティに関わる責任範囲が不明確であったため、ベンダーに問合せを行うことにより、ファームウェアの更新がベンダー側のサポート範囲となっていることを確認しました。セキュリティ規程は作成していましたが、具体的な対応を定めた手順書までは作成していませんでした。本事業の専門家からいくつかのフレームワークを紹介されましたが、専門知識がなくやや難しく感じられたため、独立行政法人情報処理推進機構（IPA）が公開している「情報セキュリティ10大脅威2023」をよりわかりやすい「フレームワーク」として参考にすることでセキュリティ対策の検討を進めていくことにしました。

04 結果と今後

明確化された対策の実行と社内教育の強化を実現

本事業の専門家派遣により、自社に必要なセキュリティ課題を明確化することができ、自社で対応できるセキュリティ対策を中心に、優先順位をつけながら進める方針を確立できました。また、本事業のセミナーやワークショップへの参加を通じて、セキュリティに関する知識が向上したことにより、今後はセキュリティ規程の共有や浸透を図り、社内教育を強化していく方針を固めました。

経営層としての声

会社経営においてサイバーセキュリティは切り離せない経営課題であると日頃から感じていましたが、本事業へ参加することで、対策の重要性をより強く感じるようになりました。今後はプライオリティを検討し投資先を判断することに加え、社員教育にも力を入れていきます。

参加者としての声

セキュリティ知識が不足している中で本事業へ参加しましたが、セミナーで難しいと感じた内容であっても、ワークショップのグループセッションにおいて、他の参加者の実体験に基づいた話を聞くことができ、少しずつ理解できるようになりました。非常に勉強になりました。

業務委託先とのセキュリティに関する契約の見直しとセキュリティ規程の再整備

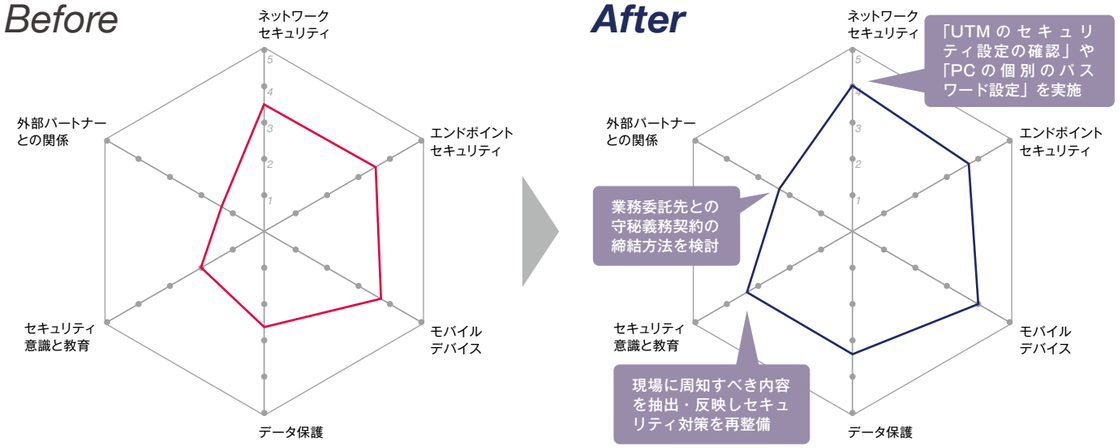
取り組んだ支援テーマ：ネットワークセキュリティ ／ エンドポイントセキュリティ ／ モバイルデバイス ／ データ保護 ／ セキュリティ意識と教育 ／ 外部パートナーとの関係

企業プロフィール　業種 / 従業員数：建築業 / ～5 名　セキュリティ体制：1名体制　兼務

事業内容　主に自社で開拓した顧客を対象に、地域密着型で建物のリフォームや外壁塗装サービスを提供している企業です。トイレや風呂など水まわりの内装工事や、バリアフリーのための工事なども請け負っています。

01 背景と状況　セキュリティ課題に対し優先度づけができていない
02 課題　セキュリティ対策内容に不安がある
03 取組内容　セキュリティ対策を強化しセキュリティ対策を再整備
04 結果と今後　セキュリティ対策強化を継続。今後は情報資産を整理

Before ***After*** 取組を通じたビフォーアフター



01 背景と状況

セキュリティ課題は多数あるが、課題対応の優先順位が判断できない

- 担当者は1名で他業務と兼務
- 必要なセキュリティ対策を知りたい
- 個人情報の管理方法に不安がある

セキュリティ担当者は1名で、多くのセキュリティ課題があることは認識していますが、課題対応の優先順位が判断できずにいました。また、個人情報を取り扱う機会が多いため、その管理方法についても不安があります。現在のセキュリティ対策を見直して、改善点を洗い出したいと考え、本事業に参加しました。

02 セキュリティ課題

セキュリティ対策に不安がある

当初の課題
- 社内のセキュリティ対策の状況把握
- セキュリティ規程類の作成が必要
- UTM 導入後の運用方法が不明確

専門家派遣支援で明らかになった課題
- 業務委託先との守秘義務契約が必要
- インシデント対応フローの作成
- 情報資産管理台帳の作成・整理

03 取組内容

STEP 1　本事業の専門家のヒアリングで課題を洗い出して優先順位づけを実施

まずセキュリティ対策の現状を把握するため、本事業の専門家からヒアリングを受けることにより、セキュリティ課題を網羅的に洗い出して優先順位づけを行いました。本事業の専門家から優先課題を選定する観点を学んだことにより、円滑に進めることができました。

STEP 2　業務委託先との守秘義務契約の締結方法を検討

最も優先度が高い課題として挙がった「業務委託先との守秘義務契約の締結方法の検討」から着手しました。すでに業務を委託している業務委託先とただちに契約を締結することは難しいため、契約更新や新規依頼の際に、守秘義務に関する項目を追加した新しい契約書について説明を行うことにしました。

STEP 3　本事業の専門家から提供を受けた資料を参考にセキュリティ規程を作成

次に、「セキュリティ規程の作成」に取り組みました。以前作成したセキュリティ注意事項は、簡易的な内容だったため、IPAの「情報セキュリティハンドブック」を参考に、現場に周知したい内容を中心に整理してセキュリティ規程の作成を進めました。

STEP 4　UTMのセキュリティ設定やPCのパスワードを見直してセキュリティ対策を強化

UTM導入後の管理運用ができていなかったため、本事業の専門家からアドバイスを受け、UTMのファームウェアのバージョンとログ取得設定の確認を行いました。また、本事業のセミナーで学んだパスワードの管理方法を参考に、業務で使用するPCに複雑なパスワードを個別に設定しました。

課題対応の優先順位を決め、セキュリティ対策を推進

本事業の専門家派遣では、現在のセキュリティ対策の状況について客観的な評価を受けるとともに、課題を洗い出しました。その結果、17件の課題がリストアップされたため、「すぐに対応できる」「費用が発生しない」「重要度が高い」という3つの観点から優先順位づけを行い課題に取り組みました。まず、業務委託先との守秘義務契約の締結方法の検討に着手しました。業務委託先とただちに契約を締結することは難しいため、契約更新や新規依頼の際に、あらためて契約書を作成することにしました。また、業務終了後に業務資料を返却することや顧客の個人情報などが記載されたデータを処分するなど、業務委託先との間の具体的なルールの策定を進めました。次に、セキュリティ規程の作成にも着手しました。本事業の専門家から提供を受けた独立行政法人情報処理推進機構（IPA）の「情報セキュリティハンドブック」を参考にして、現場に周知すべき内容を中心に整理することにより、セキュリティ規程を作成しました。また、以前から課題であったUTM（Unified Threat Management）のセキュリティ設定については、本事業の専門家からアドバイスを受けながら、ファームウェアのバージョンやログの取得期間などの確認を行いました。

04 結果と今後

情報資産を整理することによって、業務効率化まで実現

本事業の参加により、セキュリティ対策の優先順位が明確化され、自社にとって必要な課題に取り組むことができました。今後は、建屋の図面や間取りが記された資料など、業務上重要な情報資産の整理を進めていきます。セキュリティ対策の強化はもちろんですが、情報資産管理台帳を作成することにより各種資料や重要データの所在が整理され、業務効率化も実現できると考えています。

経営層の声

本事業の専門家によるヒアリングやセミナー・ワークショップで学んだ内容を、担当者から社内に共有することにより、全社的にセキュリティ意識を向上することができました。さらなるセキュリティ対策の強化のため、来年度に向けて予算を確保していく予定です。

参加者の声

本事業への参加を通して、自社のセキュリティ対策の方針が見えてきたことが最大の成果だと感じています。セミナーでセキュリティ対策を体系的に学ぶことにより、自社にとって本当に必要なセキュリティ対策を明確化することができました。今後も取組を継続していきます。

担当者の知識習得と導入製品の見直しにより、ベンダー任せのセキュリティ管理から脱却

取り組んだ支援テーマ：ネットワークセキュリティ / エンドポイントセキュリティ / モバイルデバイス / データ保護 / セキュリティ意識と教育 / 外部パートナーとの関係

企業プロフィール　業種 / 従業員数：製造業 / ～20 名　セキュリティ体制：複数 兼務 経営者

事業内容　デザイン制作、印刷、製本・加工までのサービスをワンストップで展開している印刷企業です。本社と事業所の計2拠点で業務展開しています。企業や教育関連、官公庁から多様な印刷物を手掛けています。

01 背景と状況　知識不足によりセキュリティ管理がベンダー任せ

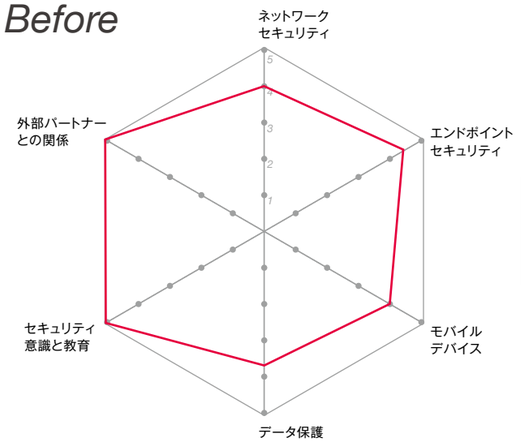
02 課題　セキュリティ対策に必要な製品を判断できる知見獲得

03 取組内容　自社に合ったセキュリティ機器の導入を検討

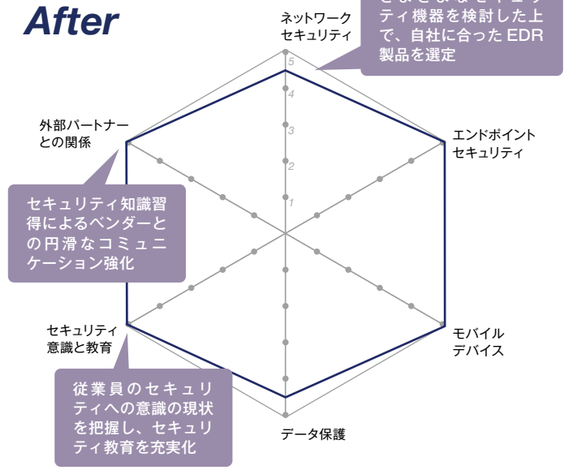
04 結果と今後　担当者はセキュリティ知識を獲得、教育にも注力予定

Before **After** 取組を通じたビフォーアフター

Before



After



01 背景と状況

担当者がセキュリティ対策の知見を獲得し、ベンダー任せの管理状況から脱却

プライバシーマークは取得済み

セキュリティ管理がベンダー任せに

担当者のセキュリティ知識不足

個人情報を取り扱う業務のため、プライバシーマーク（Pマーク）を取得しています。セキュリティ担当が代表から事務部門の役員に変更となり、セキュリティ知識不足からセキュリティ管理はベンダー任せとなっていました。自社でセキュリティ対策の要否判断ができる知見を獲得したいと考え、本事業に参加しました。

02 セキュリティ課題

セキュリティ対策に必要な知見の獲得

当初の課題

- セキュリティ機器の導入を検討したい
- 自社に必要なセキュリティ対策を明確にしたい
- セキュリティの知識がある従業員を増やしたい

専門家派遣支援で明らかになった課題

- ログ取得・監視など管理体制が整っていない
- 事業所の PC のアップデート状況の把握が必要
- 情報漏洩以外のインシデント対応が未策定

03 取組内容

STEP 1　本事業の専門家のヒアリングで課題を洗い出し、優先的に着手する課題を決定

当初はセキュリティ知識が不足していたため、対策すべき課題や方法が不明確でした。本事業の専門家派遣のヒアリングにより、課題を網羅的に洗い出すとともに、優先順位をつけることができました。その結果、自社にとって重要度の高い「セキュリティ製品の見直し」から着手することにしました。

STEP 2　ベンダーから情報収集してセキュリティ機器を検討、専門家と相談して選定

自社の環境に合った製品やサービスを選定するため、ベンダーから資料を取り寄せたり、展示会に参加することにより、情報収集を行いました。さまざまなセキュリティ関連の製品を検討した上で、最終的に本事業の専門家からアドバイスを受け、「SOCサービスが付帯したEDR製品」を選定しました。

STEP 3　IPAのセキュリティ診断を活用し現状を把握

自社のセキュリティ状況を確認するため、IPAが提供している「5分でできる!情報セキュリティ自社診断」を全従業員に実施しました。また、セキュリティ教育にIPAの公開している「情報セキュリティ10大脅威」の内容も盛り込んだほか、標的型メール訓練も行うことにしました。

STEP 4　セキュリティ知識の習得により、ベンダーとの円滑なコミュニケーションが可能に

本事業のセミナーやワークショップを通じてセキュリティ知識を習得したことにより、ベンダーとのコミュニケーションが円滑に行えるようになりました。ベンダーに対して、自社の環境や要望を具体的に説明することにより、自社に合った効果的なセキュリティ対策の強化が可能となりました。

情報収集を行い、自社に合った製品の見直しを検討

本事業の専門家によるヒアリングを通じて自社の状況を客観的に評価するとともに、セキュリティ対策の課題の洗い出しを実施しました。優先順位づけを行い、まず重要度の高かった「セキュリティ製品の見直し」という課題に取り組み、ベンダーから機器に関する資料を取り寄せることにより、自社に合ったセキュリティ製品やサービスを選定するための情報収集を行いました。さまざまな製品を検討した上で、本事業の専門家からアドバイスを受け、インシデント時の調査ができる「SOC（Security Operation Center）サービスが付帯したEDR（Endpoint Detection and Response）製品」を選定し、導入を決定しました。また、セキュリティ対策の強化のため、NAS（Network Attached Storage）のログ保管期間を確認することに加え、定期的に出力するように設定しました。さらに、独立行政法人情報処理推進機構（IPA）が提供している「5分でできる！情報セキュリティ自社診断」を全従業員に実施して現状を把握しました。本事業のセミナーやワークショップ通じてセキュリティ知識を習得したことにより、ベンダーと円滑なコミュニケーションを図ることができるようになりました。

04 結果と今後

担当者が習得したセキュリティ知識を社内教育に活用

担当者が習得したセキュリティ知識について、他の従業員に共有できる場を整備したいと考えています。今まではセキュリティに関する社内研修を不定期に行っていましたが、今後は定期的な情報発信および研修を行う予定です。また、「情報漏洩以外のインシデント対応」については、ウイルス対策や外部からの攻撃などの対応を整理して、文書化する取組を継続していきます。

経営層としての声

取引先からはさまざまなセキュリティ対策を強く求められています。セキュリティ対策は会社を存続させていくための重要な要素と考えており、今後も継続して取り組んでいきます。本事業への参加により、セキュリティ対策の強化を図ることができ、大変感謝しています。

参加者としての声

セキュリティ知識の不足を感じながら本事業に参加しましたが、セミナーの解説が丁寧でわかりやすかったため、少しずつ知識を習得できました。ワークショップでは他の企業の担当者と意見を交換することにより、自身のスキルアップを図ることができました。

ネットワークセキュリティおよびエンドポイントセキュリティを中心に技術的な対策を実施

取り組んだ支援テーマ：**ネットワークセキュリティ** / **エンドポイントセキュリティ** / モバイルデバイス / データ保護 / セキュリティ意識と教育 / 外部パートナーとの関係

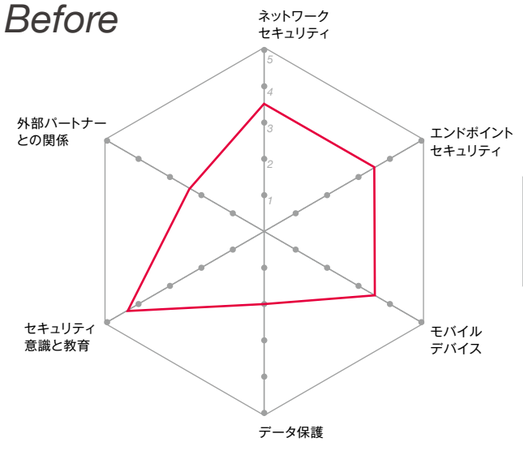
企業プロフィール　業種 / 従業員数：製造業 / ～50 名　セキュリティ体制：複数 / 兼務

事業内容　試作用の切削加工機を製造する企業です。自動車や医療器具など、多様な業界におけるプロダクト開発に貢献しています。また、3D プリンターの技術を駆使した造形サービスも展開しています。

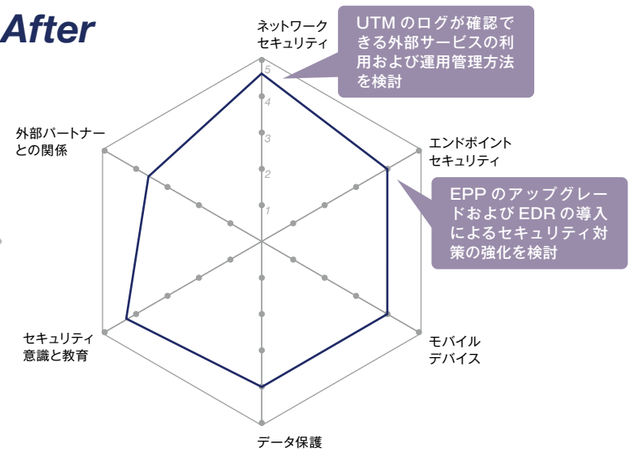
01 背景と状況　基本的なセキュリティ対策は実施済み
02 課題　UTM導入後に行うべき対策が不明確
03 取組内容　重要度の高い課題から取組を実行
04 結果と今後　技術面を中心にセキュリティ対策を強化

Before ***After*** 取組を通じたビフォーアフター

Before



After



01 背景と状況

基本的なセキュリティ対策により SECURITY ACTION（二つ星）を宣言

支援事業を活用してUTMを導入 → SECURITY ACTION（二つ星）を宣言 → 基本的なセキュリティ対策は実施済み

東京都「令和4年度中小企業サイバーセキュリティ向上支援事業」に参加し、同年にSECURITY ACTION（二つ星）を宣言しました。UTM（Unified Threat Management）の導入など基本的なセキュリティ対策は行いましたが、今後実施すべき対策が不明確です。

02 セキュリティ課題

UTM導入後に行うべきセキュリティ対策が不明確

当初の課題
- セキュリティ対策の客観的な評価ができていない
- セキュリティ規程の運用管理に不安がある
- セキュリティ対策製品に関する知識が不足している

専門家派遣支援で明らかになった課題
- UTM のログが確認できていない
- エンドポイントセキュリティの対策が不十分
- クラウドサービスのアカウント棚卸しができていない

03 取組内容

STEP 1　セキュリティ対策状況の確認および課題の洗い出し

本事業の専門家派遣によるヒアリングによって、セキュリティ対策状況の確認および課題の洗い出しを行い、対応すべきセキュリティ課題を把握することができました。本事業の専門家からのアドバイスを受け、優先度が高くすぐに対応できる課題から着手することにしました。

STEP 2　UTMのログを保管・活用するための運用管理方法を検討

ネットワークセキュリティに関しては、UTMのログが確認できていないことが明らかになったため、UTMのセキュリティ機能の設定追加や専用サーバの利用によるログの運用管理方法を検討しました。また、VPNにおける二要素認証を有効化し、従業員が出張する場合など一部業務での利用を開始しました。

STEP 3　EPPのアップグレードおよびEDRの導入を検討

エンドポイントセキュリティに関しては、業務用端末から有効期限が切れているウイルス対策ソフトウェアをアンインストールしました。また、導入済みのEPPの契約内容のアップグレードにより一元管理を可能とするとともに、EDRの導入について検討しました。

STEP 4　アカウントの棚卸しを実施してリスクを低減

クラウドサービスの利用状況を明らかにするため、従業員に向けてアンケートを実施し、アカウントの棚卸しを行いました。また、これまで一部削除されていなかった退職者のアカウントを削除することにより、情報漏えいに対するリスクを低減しました。

ネットワークおよびエンドポイントを重点的に強化

本事業のセミナーにおいて、セキュリティ規程作成後におけるPDCAサイクルの実行や、情報資産を棚卸しすることの重要性を認識しました。本事業のワークショップでは、情報資産をリスト化することに加え、重要度の高い課題からセキュリティ対策に取り組む方法を習得しました。本事業の専門家派遣においては、現状のセキュリティ対策における課題の洗い出しを行いました。その結果、UTMのログが確認できていないことが明らかになり、外部サービスの導入によるUTMのログの記録を検討しました。また、一部業務でVPN（Virtual Private Network）接続時に二要素認証を利用することにしました。エンドポイントセキュリティに関しては、業務用端末から有効期限が切れているウイルス対策ソフトウェアをアンインストールしました。さらに、EPP（Endpoint Protection Platform）のアップグレード、EDR（Endpoint Detection and Response）の導入を検討しました。また、クラウドサービスの利用状況が可視化されていなかったため、社内アンケートを行いアカウントの棚卸しを実施しました。あわせて、退職者のアカウントの削除を行い、情報漏えいのリスク低減を図りました。

04 結果と今後

技術面のセキュリティ対策から優先して対策を強化

課題に優先順位をつけ、短期的に取り組める課題から改善を行いました。ネットワークセキュリティやエンドポイントセキュリティの強化に加え、クラウドサービスやセキュリティ対策製品を選ぶ際のポイントが習得でき、非常に有意義でした。今後は、長期的な視点における運用方法の策定、サービス事業者との責任分界点の明確化などに取り組んでいきたいと考えています。

経営層の声

本事業を通じて、当社の事情に沿った具体的なアドバイスをいただき、大変参考になりました。セキュリティ対策を本格化し始めてから日が浅い状況ではありますが、取組を着実に推進することにより、セキュリティ対策を強化することができると感じました。

参加者の声

本事業への参加により、セキュリティ対策の基本となる考え方の習得から、技術面におけるさまざまな疑問を解消することができました。セミナーで知識を習得し、ワークショップで演習を実施できたことは、実際のセキュリティ対策を行う上で非常に役立ちました。

現場での運用を視野に規程類の改訂を推進
セキュリティ対策のPDCAの確実な循環へ

取り組んだ支援テーマ：**データ保護**／セキュリティ意識と教育／ネットワークセキュリティ／エンドポイントセキュリティ／モバイルデバイス／外部パートナーとの関係

企業プロフィール　業種 / 従業員数：製造業 / ～50名　セキュリティ体制：複数　兼務

事業内容　文化施設の展示ディスプレイおよび展示されている造形物の製作をメインに行っています。

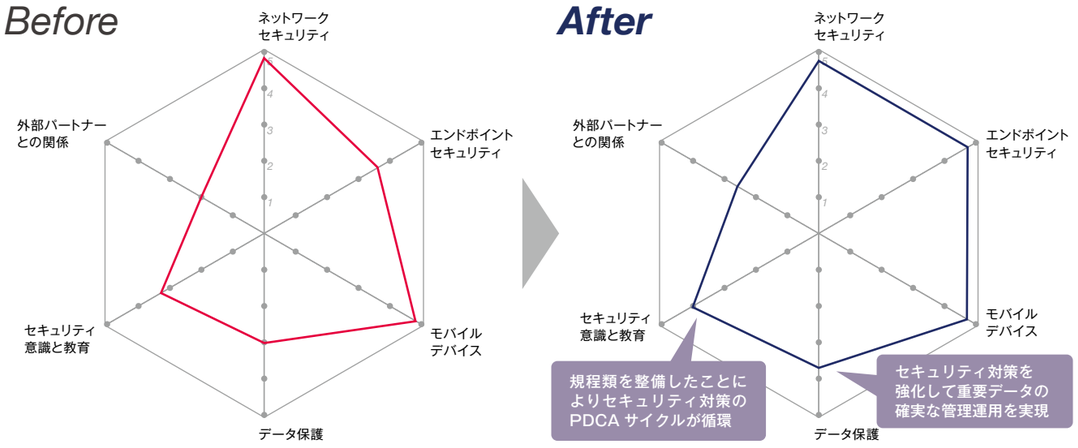
01 背景と状況　リソース不足で進まないセキュリティ対策

02 課題　セキュリティ対策のPDCAサイクルが回っていない

03 取組内容　規程類の整備と各種セキュリティ対策の実施

04 結果と今後　全社的なセキュリティ対策のPDCAの循環を目指す

Before ***After*** 取組を通じたビフォーアフター



01 背景と状況

取組意欲はあるもののリソース不足で思うように進まないセキュリティ対策

- SECURITY ACTION（二つ星）を宣言
- セキュリティ規程の作成がストップしている
- セキュリティ担当は2部署に1名ずつ配置

令和4年にSECURITY ACTION（二つ星）を宣言しましたが、以後の取組はやや断続的で、セキュリティ規程の作成も途中で止まっています。セキュリティ担当は技術部門、工場部門に1名ずつ配置していますが、リソースは足りていません。また、セキュリティに関する従業員の知識には個人差があります。

02 セキュリティ課題

セキュリティ対策のPDCAサイクルが回っていない

当初の課題

- セキュリティ規程が作成途中のため運用できていない
- 従業員のセキュリティに関する知識に個人差がある
- セキュリティ対策が十分か客観的な判断ができない

専門家派遣支援で明らかになった課題

- 業務データの運用・廃棄ルールが定まっていない
- 情報資産管理台帳の整備が行われていない
- 共有フォルダのアクセス制限が設定されていない

03 取組内容

STEP 1　課題の洗い出しと改善策の検討

本事業の専門家派遣において、課題の洗い出しを実施しました。セキュリティ規程および情報資産管理台帳の整備に加え、重要データの保護への対策を中心に、セキュリティ対策に必要な改善策を検討しました。

STEP 2　セキュリティ規程と情報資産管理台帳の整備に着手

IPAの提供する「情報セキュリティ関連規程」をひな型として、作成途中で止まっていたセキュリティ規程を見直し、確認すべき部分をリスト化した後、本事業の専門家から指摘を受けながら改訂を実施しました。
情報資産管理台帳は、IPAの提供する「リスク分析シート」を活用して記入を進めました。

STEP 3　重要データ保護として強化するべきセキュリティ対策を検討

重要データ保護として、共有フォルダのアクセス制限の設定、業務データの廃棄ルールを策定したほか、クラウド型グループウェアによる共有ツールの一本化などを検討しました。また、本事業の専門家からネットワーク構成図のテンプレートの提供を受け、新たにネットワーク構成図を作成しています。

STEP 4　「情報セキュリティハンドブック」を活用して従業員のセキュリティ意識の向上を促進

従業員教育に関しては、本事業の専門家派遣において紹介されたIPAの提供する「情報セキュリティハンドブック」を活用し、自社の環境や業務運用に即して見直しを行うことで教育資料を作成し、セキュリティ意識の向上を促しています。

規程類の整備と各種セキュリティ対策の実施に注力

本事業の専門家派遣において、セキュリティ対策状況の確認および課題の洗い出しを実施しました。その際に、セキュリティ規程および情報資産管理台帳の整備が不十分であることや、従業員のセキュリティ対策に関する知識に個人差があることなど、取り組むべき課題が明らかになりました。早速、セキュリティ規程および情報資産管理台帳の見直し、社内データの保護、従業員のセキュリティ教育の着手を実施しました。
セキュリティ規程に関しては、独立行政法人情報処理推進機構（IPA）のひな型をもとに整備を進め、客観的評価および改訂を実施しました。
情報資産管理台帳に関しては、ほぼ着手していなかったため、IPAの提供する「リスク分析シート」を活用して作成を進めました。
データ保護に関しては、共有フォルダのアクセス制限設定、業務データの廃棄ルールの明確化、クラウドサービス導入による共有ツールの一本化や多要素認証の導入などを進めました。また、本事業の専門家による事務所内のハードウェア設置環境などの目視チェックを受け、セキュリティ機器の配置および配線が安全であることを確認しました。従業員のセキュリティ教育に関しては、IPAの提供する「情報セキュリティハンドブック」を活用して教育資料を作成し、各自が勉強に取り組み始めています。

04 結果と今後

セキュリティ対策のPDCAサイクルの循環を目指す

セキュリティ規程と情報資産管理台帳の整備・改訂が終わり、従業員とともにセキュリティ対策のPDCAサイクルを回していく目途が立ちました。本事業に参加したセキュリティ担当者は知識が身につき、これまで抱いていた不安が払拭されました。今後は、クラウド型グループウェアの導入による共有ツールの一本化を推進しつつ、並行してリモートワークの管理体制を構築していく予定です。

経営層の声

本事業のセミナーやワークショップ、専門家派遣による指導を通じて、自社の社員だけでは学ぶことができない専門的な知見を得ることができました。セキュリティ担当者も我々経営陣も、今後の自社でのセキュリティ対策に自信を持って取り組むことができると考えています。

参加者の声

本事業の専門家派遣はもちろん、セミナーやワークショップでも有意義な時間を過ごすことができました。特に最新のセキュリティ対策に関する情報の入手先を知ることができたことは大きな収穫でした。本事業への参加を通じて刺激を受け、モチベーションが向上しました。

セキュリティ対策の体系的な知識を習得
最新の状況に合わせた効果的な対策を実行

取り組んだ支援テーマ：**ネットワークセキュリティ** / エンドポイントセキュリティ / **モバイルデバイス** / データ保護 / **セキュリティ意識と教育** / 外部パートナーとの関係

企業プロフィール　業種 / 従業員数：製造業 / ～100 名　セキュリティ体制：1名体制　兼務

事業内容　自動車、半導体、医療、食品など幅広い業種で使用される工業用温度計の開発設計、販売を行っている企業です。長年培ってきた高度な技術力を活かし、取引先の多様なニーズに対応した製品の製造も請け負っています。

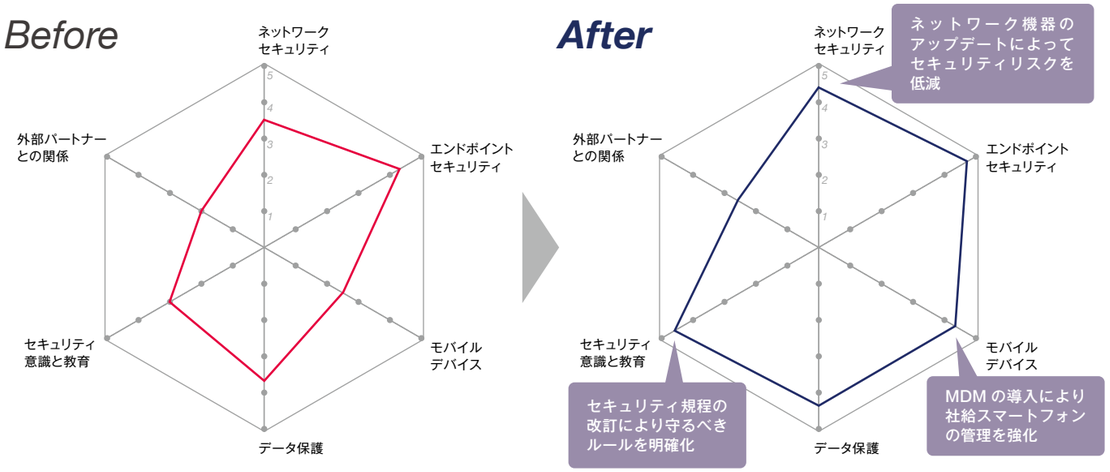
01 背景と状況　自社のセキュリティ対策を客観的に評価することが困難

02 課題　取り組むべき対策が明確化できていない

03 取組内容　セキュリティ知識を習得し管理体制の強化

04 結果と今後　最新のセキュリティ状況に柔軟に対応した対策を実行

Before ***After*** 取組を通じたビフォーアフター



01 背景と状況

担当者の独学により進めてきたセキュリティ対策に不安あり

- セキュリティ担当者は1名の管理体制
- 基本的なセキュリティ対策は実施済み
- 注意事項は部署ごとに紙で掲示

セキュリティ担当は1名で他業務と兼務しています。基本的なセキュリティ対策は講じていますが、客観的な評価ができないため、不安を感じています。従業員の教育面では、セキュリティ対策に関する注意事項を掲示板に貼り出し共有に努めています。テレワークが定着し、クラウドサービスの利用も活発化しています。

02 セキュリティ課題

セキュリティ対策の体系的な知識習得が必要

当初の課題
- セキュリティ対策に関する客観的な評価ができない
- 従業員のセキュリティリテラシーに不安がある
- セキュリティ規程の改訂が行われていない

専門家派遣支援で明らかになった課題
- 情報資産管理台帳を作成していない
- パスワードの使い回しが常態化している
- ファームウェアのアップデートができていない

03 取組内容

STEP 1　独学により進めてきたセキュリティ対策の状況確認と課題の洗い出し

これまで独学により進めてきたセキュリティ対策については、本事業のセミナーやワークショップを通じて、体系的な基礎知識を習得しました。また、本事業の専門家派遣により、現状のセキュリティ対策の把握と対応すべき課題の洗い出しを行いました。

STEP 2　すぐに対応できる課題から着手しセキュリティリスクを低減

すぐに取り組むことができる課題として、ネットワーク機器のファームウェアのアップデートに加え、サポート期限が迫っている自己所有端末のOSの確認とバージョンアップを実施しました。また、業務用のモバイルデバイスを管理するMDMを導入しました。

STEP 3　セキュリティ規程の見直しや情報資産管理台帳の作成を開始

独立行政法人情報処理推進機構（IPA）のひな型を参照してセキュリティ規程を見直し、不足事項の有無を確認しました。また、テレワーク関連の就業規則およびインシデントへの対応方法を盛り込みました。本事業のワークショップで学んだ知識を活かし、情報資産管理台帳の作成も開始しました。

STEP 4　今後取り組む課題を検討し方針を決定

常態化していたパスワードの使い回しを防止するため、一度のユーザー認証によって複数のシステムにログインできるシングルサインオンの導入を検討しました。また、セキュリティ担当の負担を減らすため、ネットワークログの確認や従業員教育を外部の専門家に業務委託することも検討しています。

すぐに対応できる課題から着手し長期的な方針を策定

本事業のセミナーにおいて、セキュリティ対策の基本を体系的に学びました。また、本事業の専門家派遣では、現状のセキュリティ対策の実施状況を改めて確認し、課題を整理しました。リスクが高くすぐに取り組むことができる課題として、本事業の専門家に指摘されたネットワーク機器のファームウェアのアップデートを実施しました。テレワークの際に従業員が使用している自己所有端末については、端末OSのサポート状況を確認し、サポート期限が迫っているOSのバージョンアップを行いました。また、業務用のモバイルデバイスを管理するためにMDM（Mobile Device Management）を導入しました。一方で、長期的に取り組む課題として、セキュリティ規程の見直しを開始し、テレワークの就業規則やインシデントへの対応方法の追加を検討しました。また、情報資産管理台帳の作成にも着手しました。各システムの認証におけるパスワードの使い回しの常態化に関しては、シングルサインオンの導入によるセキュリティ対策の強化とアカウント管理の負担軽減を検討しました。さらに、セキュリティ担当が1名の管理体制にリソース不足を感じているため、従業員教育やネットワークログの確認といった業務を外部に業務委託することも検討しています。

04 結果と今後

時代の流れに合わせたセキュリティ対策の強化に注力

これまで取り組んできた基本的なセキュリティ対策については、一定の評価が得られ不安が払拭されました。一方で、これまで気づいていなかった課題も明らかになり、早急に取り組むことでセキュリティに関わるリスクを低減することができました。今後は、長期的な各課題への取組と並行して情報収集を積極的に行い、最新の状況に合わせてセキュリティ対策を強化していきたいと考えています。

経営層の声

本事業に参加し、セキュリティ対策の重要性を改めて認識しました。専門家からの指摘により、セキュリティ担当者が1名では負担が大きいことがわかったため、外部に業務委託することにより、リソースの確保およびセキュリティ管理体制の強化を図りたいと考えています。

参加者の声

本事業のセミナーで、セキュリティ対策の基本を体系的に習得できました。ワークショップでは、他社の担当者が前向きにセキュリティ対策に取り組んでいる姿を見て、大いに刺激を受けました。また、専門家からのアドバイスにより、セキュリティ対策全般を強化できました。

業務に即したガイドラインの運用を開始
従業員のセキュリティへの取組意識を醸成

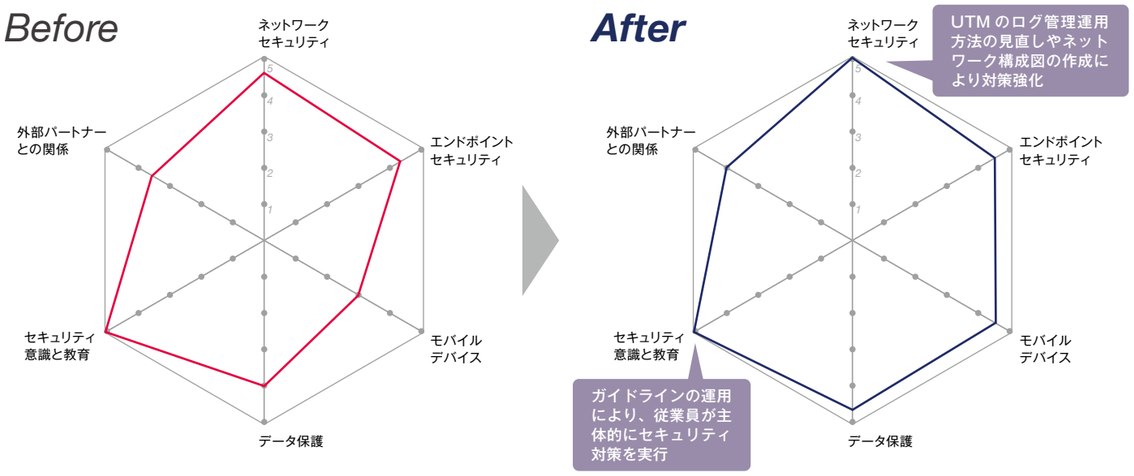
取り組んだ支援テーマ：ネットワークセキュリティ / エンドポイントセキュリティ / モバイルデバイス / データ保護 / **セキュリティ意識と教育** / 外部パートナーとの関係

企業プロフィール　業種 / 従業員数：製造業 / ～100 名　セキュリティ体制：複数　兼務

事業内容　携帯電話会社の通信基地局に設置する各種建設部材の設計・製造・施工を行っている企業です。設置場所の現地調査から製品試験までワンストップで行っています。また、防災・減災製品の開発・製造も手掛けています。

01 背景と状況　基本的なセキュリティ対策は実施済み
02 課題　従業員のセキュリティ意識が把握できず不安あり
03 取組内容　自社の業務に合わせたガイドラインの作成･運用
04 結果と今後　セキュリティに対する主体的な取組意識が向上

Before ***After*** 取組を通じたビフォーアフター



01 背景と状況

従業員のセキュリティ意識向上の必要性を強く感じている

- 基本的なセキュリティ対策は実施済み
- PCのパスワードが未設定
- 従業員のセキュリティ意識に不安あり

セキュリティ規程を作成し、基本的なセキュリティ対策は実施しています。一方で、PCの認証パスワードが設定されていないなどの不安も抱えています。また、従業員のセキュリティリテラシーの向上を目的として、標的型攻撃メール訓練を年2回実施するとともに、外部の講師による研修を不定期に行っています。

02 セキュリティ課題

セキュリティ対策に関わるガイドラインの作成が必要

当初の課題
- 自社のセキュリティ対策を客観的に評価できていない
- 従業員のセキュリティ意識に不安がある
- PC のパスワードが設定されていない

専門家派遣支援で明らかになった課題
- セキュリティのルールや手順が明文化されていない
- インシデントの対応フローが明確化されていない
- UTM のログ管理ができていない

03 取組内容

STEP 1　セキュリティ対策状況の確認および課題の洗い出し

本事業の専門家派遣において、現状のセキュリティ対策を確認し、課題の洗い出しを実施しました。その結果、「UTMのネットワークログ管理の見直し」や「従業員向けのガイドラインの作成」など、従来は意識していなかった新たな課題が明確になりました。

STEP 2　PCの認証パスワードを設定・自社ウェブサイトのセキュリティ設定を確認

早急に取り組める課題として、PCの認証パスワードを設定しました。そのほか、自社ウェブサイトにおけるセキュリティ対策状況を制作会社に確認しました。また、ネットワーク構成図の作成、UTMのログの長期保管のための情報セキュリティ対策製品およびEDRの導入検討などを行いました。

STEP 3　セキュリティ対策に関するガイドラインを社内に展開

従業員向けの具体的なガイドラインとしてIPAの提供する「情報セキュリティハンドブック」を自社の業務に合わせて修正し、社内に展開しました。今後、IPAの提供する「5分でできる!情報セキュリティ自社診断」を活用し、従業員のセキュリティ意識の状況を確認していく予定です。

STEP 4　インシデント管理体制の構築を検討

インシデント発生時における対応フローが不明確であったため、現場での運用に留意して極力わかりやすく文書化することに加え、インシデントの報告書の様式も整備することでインシデント内容や対応履歴を残すことを決定し、従業員に周知しました。

フレームワークを活用しガイドラインを作成

本事業の専門家派遣において、現状のセキュリティ対策の評価と課題の洗い出しを行いました。その結果、「UTM（Unified Threat Management）のログ管理運用方法の確立」、「従業員向けガイドラインの作成」といった新たな課題が明らかになりました。以前から課題だと感じていたデスクトップPCの認証パスワードは、すぐに設定しました。また、ウェブサイトの開発を委託している制作会社に問合せ、適切なセキュリティ設定がされていることを確認しました。さらに、UTMのログを長期保管する方法の検討、ネットワーク構成図の作成、EDR（Endpoint Detection and Response）の導入検討などを行いました。セキュリティ規程に基づく従業員向けの具体的なガイドラインが未整備だったため、独立行政法人情報処理推進機構（IPA）の提供する「情報セキュリティハンドブック」を自社の業務に合わせて修正し、社内に展開しました。不明確であったインシデントの対応フローについては、発生時の報告内容も含めて整備し、従業員に周知しています。今後、IPAの提供する「5分でできる！情報セキュリティ自社診断」を活用し、従業員のセキュリティリテラシーおよびセキュリティ意識の状況を確認していく予定です。

04 結果と今後

従業員のセキュリティへの主体的な取組意識を醸成

本事業におけるさまざまな取組により、従業員のセキュリティリテラシーが向上し、セキュリティ対策へ主体的に取り組む意識が醸成されると考えています。また、今後3ヶ年の中長期計画も作成しており、令和6年度のEDRの導入や定期的な教育実施などのイベントとともに、導入している機器類のリースやサポート終了などの時期も盛り込んで、継続的なセキュリティ対策を行っていきます。

経営層の声
情報セキュリティ対策への理解を深める良い機会となりました。セキュリティ対策に関するガイドラインの運用開始により、従業員のセキュリティ意識が向上し、社内体制の強化も図ることができました。今後も継続してセキュリティ対策を推進していきたいと考えています。

参加者の声
自社の業務に合わせて優先順位をつけて取り組む必要性など、中小企業のセキュリティ対策に欠かせない内容を習得することができました。また、ワークショップで他社の担当者との交流を通じ、さまざまなセキュリティ対策の情報を得たことも大きな収穫となりました。

今後の会社の規模拡大と従業員の増加を想定して、セキュリティ対策の優先順位を決定

取り組んだ支援テーマ：**ネットワークセキュリティ** / エンドポイントセキュリティ / モバイルデバイス / データ保護 / **セキュリティ意識と教育** / 外部パートナーとの関係

企業プロフィール　業種 / 従業員数：製造業 / ～100 名　セキュリティ体制：**複数** / **兼務**

事業内容　医療診断や治療、生命科学研究にイノベーションを起こすことを目指している大学発のベンチャー企業です。再生医療や医療検査診断、創薬についての最先端の研究結果や技術を用いて、ライフサイエンスツールを開発・販売しています。

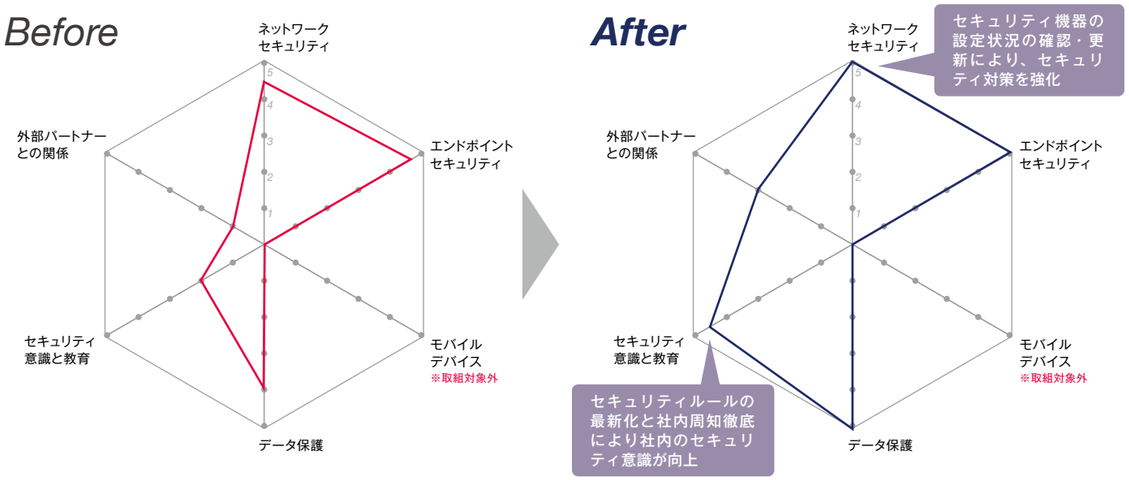
01 背景と状況　セキュリティ課題の優先順位づけができていない

02 課題　事業規模に合ったセキュリティルールが設定されていない

03 取組内容　セキュリティルールをアップデートし運用方法を確立

04 結果と今後　セキュリティルールの周知を図り社内教育に注力

Before **After** 取組を通じたビフォーアフター



01 背景と状況

セキュリティ対策状況の客観的な評価、課題の優先順位づけができていない

- 兼務の4名によるセキュリティ体制
- セキュリティ課題の優先順位が不明確
- 会社規模の拡大と従業員増加を予定

セキュリティ担当は他業務との兼務の4名です。セキュリティに関する課題があることは認識していましたが、優先順位づけの客観的な評価やアドバイスを必要としていました。今後、会社としての規模の拡大と従業員の増加を予定しており、必要なセキュリティ対策をあらかじめ検討しておきたいと考えていました。

02 セキュリティ課題

最新化したセキュリティルールに基づいた運用方法の確立

当初の課題
- 従業員の情報リテラシーに個人差がある
- セキュリティルールの見直しと修正が必要
- インシデント対応フローが未整備

専門家派遣支援で明らかになった課題
- セキュリティ機器の設定の確認とアップデートが必要
- アカウントの棚卸しおよび管理表作成ができていない
- 情報資産管理台帳の作成ができていない

03 取組内容

STEP 1　セキュリティ課題を洗い出してリスト化し、優先順位づけを実施

本事業の専門家によるヒアリングにより、セキュリティ対策の現状把握とセキュリティ課題の洗い出しを行いました。洗い出した課題について、「自社の事業に対する影響度とコストのバランス」、「今後の会社の規模拡大と従業員増加を想定したセキュリティ対策」を考慮して、優先順位づけを行いました。

STEP 2　セキュリティルールを昨今のセキュリティ情勢に合わせてアップデート

まず、最も優先度が高いセキュリティルールのアップデートに取り組みました。セキュリティルールについては、会社設立当初に作成し未更新だったため、昨今のセキュリティ情勢に対応する内容へ変更しました。従業員が増えていることから、社内へ周知徹底し、従業員のセキュリティ意識の向上を図りました。

STEP 3　マルウェア感染時やパソコンの紛失・盗難時のインシデント対応フローの策定

マルウェア感染時やパソコンの紛失・盗難時のインシデント対応フローの作成に取り組みました。本事業の専門家から提供を受けたIPAの「中小企業のためのセキュリティインシデント対応手引き」を参考にして、さまざまなインシデント発生時の具体的な対応を検討し、明文化しました。

STEP 4　セキュリティ機器の設定の確認とアップデートを実施

セキュリティ対策を技術的にも強化するため、ネットワーク機器の設定やウイルス対策ソフトウェアのスキャン設定などの確認とアップデートに取り組みました。その結果、ネットワークログの保管期間が導入当時から変更されていなかったため、保管期間を6か月間に延長しました。

セキュリティルールをアップデートし、社内へ周知徹底

本事業の専門家のヒアリングにより、自社のセキュリティ対策の現状を確認するとともに、セキュリティに関する課題を網羅的に洗い出しました。洗い出した課題の中から、「自社の事業に対する影響度とコストのバランス」を考慮することに加え、「今後会社の規模が拡大し、従業員が増加することを想定した際に必要となるセキュリティ対策」という観点からも、優先順位をつけていきました。まず、会社設立当初に作成し未更新だったセキュリティルールの見直しに着手しました。たとえば、使用ルールが不明確であったUSBの使用を原則禁止とし、総務部門が許可した場合のみ使用可能とするとともに、使用履歴を記録するルールに変更し、ルールに盛り込みました。更新した内容については、社内の全体ミーティングでアナウンスし、周知徹底を図っていきます。さらに、本事業の専門家から提供を受けた独立行政法人情報処理推進機構（IPA）の「中小企業のためのセキュリティインシデント対応手引き」を参考にして、インシデント対応フローの作成にも取り組みました。このほか、本事業の専門家からアドバイスを受け、ベンダーへセキュリティ機器のアップデート状況やログに関する設定内容を確認し、ログの保管期間の延長などを実施することにより、セキュリティ対策の強化を図りました。

04 結果と今後

社内教育を強化し、セキュリティ意識の向上を図る

当初からの課題であったセキュリティルールについては、最新化を図ることができました。更新した内容については、社内の全体ミーティングにて周知徹底していきます。また、各部門の担当者と協力して、情報資産管理台帳の作成も進めています。今後は社内教育の強化のため、セキュリティ対策の一般的な内容に社内ルールを盛り込んだ教育資材を作成し、理解度テストも実施していく予定です。

経営層の声

本事業の取組によりセキュリティ課題が洗い出されて、対応の優先順位と中長期的なセキュリティ対策計画が整理できました。こうした取組は取引先からの信頼感につながるものなので、必要に応じて予算化していくなど、継続的に対応していきたいと考えています。

参加者の声

本事業のセミナーやワークショップで自社に合ったセキュリティ対策を学ぶことができたほか、他企業のセキュリティ担当者と意見交換できたことは大変有意義でした。さらなるセキュリティ対策の強化に向けて、本事業で獲得した知見を最大限に活かしていきます。

インシデント対応フローやセキュリティ規程など、管理面でのセキュリティ対策を強化

取り組んだ支援テーマ：ネットワークセキュリティ / エンドポイントセキュリティ / モバイルデバイス / データ保護 / セキュリティ意識と教育 / 外部パートナーとの関係

企業プロフィール　業種 / 従業員数：建設業 / ～100名　セキュリティ体制：複数　兼務

事業内容　公害防止などの環境対策に関わるエンジニアリングやコンサルティングサービスを提供する企業です。培ってきた研究開発力を生かし、サステナブルな社会づくりや環境づくりに貢献しています。

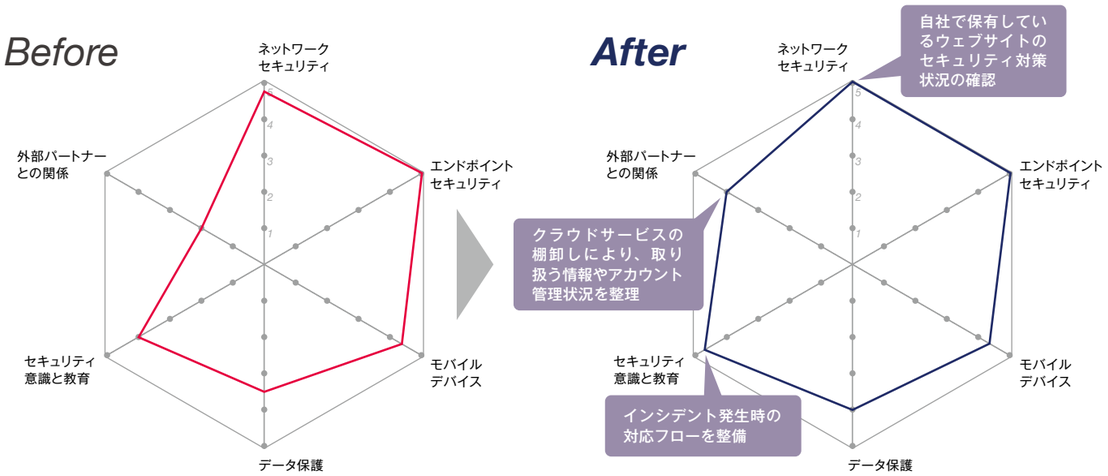
01 背景と状況　セキュリティ対策を進めているが規程類は整備中

02 課題　管理面での対策が不足、規程類の整備も必要

03 取組内容　インシデント対応や規程類など管理面の対策を強化

04 結果と今後　取組を通じて今後対応していくべき方向性が明確化

Before **After** 取組を通じたビフォーアフター



01 背景と状況

技術的なセキュリティ対策を進めているが、セキュリティ規程は整備中

- セキュリティ対策は複数名で対応
- 技術面での対策は自社で推進
- セキュリティ規程類は整備中

技術的なセキュリティ対策は、情報システム部門の複数名体制により、ベンダーのサポートを受けながら進めています。役員主導で全部門のマネージャーを集めて開催する情報セキュリティ委員会では、セキュリティ基本方針の策定を進めていますが、具体的なルールを盛り込んだセキュリティ規程の整備が必要でした。

02 セキュリティ課題

管理面での対策が不足、規程類の整備も必要

当初の課題
- 自社のセキュリティ対策の客観的な評価を得たい
- 運用ルールを盛り込んだセキュリティ規程の整備
- 情報セキュリティ委員会を効果的に運用したい

専門家派遣支援で明らかになった課題
- インシデント発生時の対応フローの決定
- 利用しているクラウドサービスの棚卸し
- 自社のウェブサイトのセキュリティ対策状況の確認

03 取組内容

STEP 1　インシデント発生時の詳細な対応フローの決定

インシデント発生時の対応フローの作成にあたり、本事業の専門家からIPAが提供する「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」を紹介され、参考にしました。インシデント発生時に誰がどのように対応するか、対外的に何をいつ公表するかなどの具体的な対応フローの整備を進めました。

STEP 2　クラウドサービスの棚卸しと、取り扱う情報やアカウント管理状況を整理

基幹システムをはじめ、社内で利用しているウェブサービスの棚卸しを実施しました。利用しているアカウントの管理や取り扱う情報の把握を進めるとともに、パスワードの桁数増加による認証強化の対策も行いました。

STEP 3　自社で保有しているウェブサイトのセキュリティ設定状況を委託先に確認

自社で保有しているウェブサイトについて、開発・保守・運用を委託しているベンダーに、開発におけるセキュリティ対策の状況や脆弱性診断の実施有無を確認しました。その結果、いずれも問題なく実施されていることが確認できました。

STEP 4　社内のセキュリティ規程類の評価と修正

情報セキュリティ委員会を中心として、IPAが公開している「中小企業の情報セキュリティ対策ガイドライン」を参考に、現場向けの運用ルールを盛り込んだセキュリティ規程の整備を進めました。本事業の専門家からアドバイスを受け、自社の業務に合わせた内容に修正しながら推進する方針を固めました。

インシデント対応や規程類など管理面での対策を強化

本事業の専門家によるヒアリングと課題の整理を行った結果、UTM（Unified Threat Management）などのセキュリティ機器やソフトウェアの導入は進んでいたため、本事業では管理面でのセキュリティ対策を中心に進めることにしました。まず、インシデント発生時の対応フロー作成から着手しました。特にランサムウェア感染が発生した際の具体的な対応や事態の公表判断について、担当者が具体的にイメージできていなかったため、本事業の専門家から参考資料の紹介を受け、対応フローの整備を進めることにしました。また、利用しているクラウドサービスの棚卸しを行い、使用しているアカウントや取り扱っている情報を把握するとともに、パスワードの桁数増加による認証強化も行いました。さらに自社で保有するウェブサイトの開発・保守・運用を委託しているベンダーに対し、セキュリティ設定状況を確認しました。
あわせて、現場向けの運用ルールを盛り込んだセキュリティ規程の整備も進めました。本事業の専門家からアドバイスを受け、独立行政法人情報処理推進機構（IPA）の提供する「中小企業の情報セキュリティ対策ガイドライン」を参考に、情報セキュリティ委員会で内容を協議しながら自社の業務に合わせて修正していくことにしました。

04 結果と今後

取組を通じて今後対応していくべき方向性が明確化

本事業での取組を通じて、セキュリティ対策における課題と対応するべき対策の方向性が明確になりました。現時点ではまだ取組を開始したところですが、セキュリティ規程類やインシデント対応フローの継続的な整備強化やアップデートを進めていきます。従業員教育についても、情報セキュリティ委員会において、標的型メール訓練の実施やセキュリティに関する動画配信などを計画しています。

経営層の声

当社では技術的なセキュリティ対策を推進していましたが、サイバー攻撃などのリスクへの対応が十分とは言い難い状況でした。本事業で得た知見をセキュリティ対策に反映させることにより、より万全なセキュリティ対策を講じていきたいと考えています。

参加者の声

本事業の専門家から受けたアドバイスや、セミナーで得た知識を活かし、セキュリティ対策の強化を進めることができました。ワークショップで他社の状況を聞くことができたことも、大きな成果の一つです。今後は学んだ内容を社内へ共有していきたいと考えています。

本事業の専門家のアドバイスにより、セキュリティ製品の導入計画立案や予算化を推進

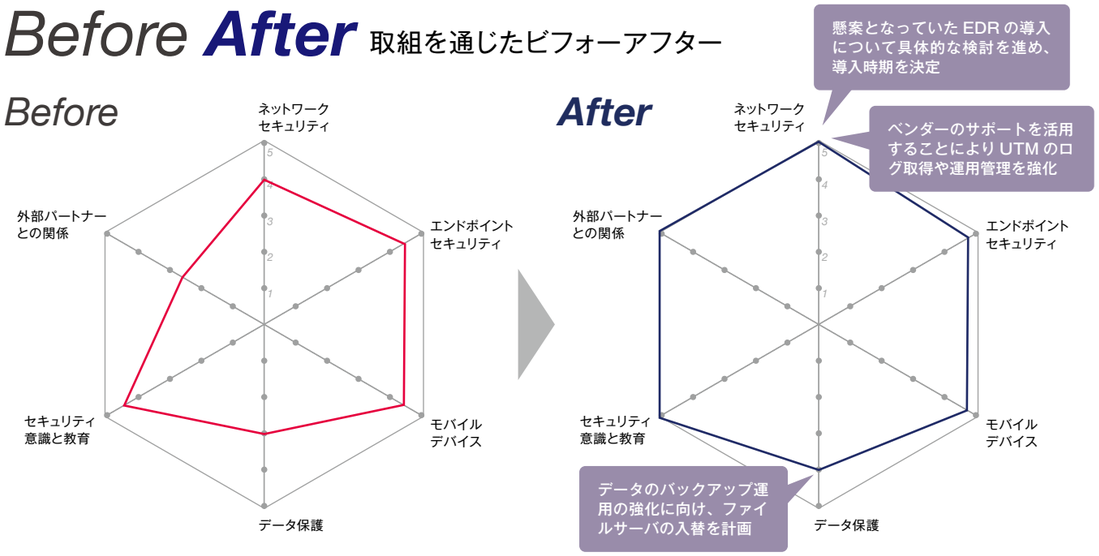
取り組んだ支援テーマ：**ネットワークセキュリティ** / エンドポイントセキュリティ / モバイルデバイス / **データ保護** / セキュリティ意識と教育 / 外部パートナーとの関係

企業プロフィール　業種 / 従業員数：農業 / 101～300名　セキュリティ体制：1名体制 兼務

事業内容　「持続可能な農業」を目指し、農業者や関連する事業者にさまざまな農業支援サービスを展開しています。農地活用、人材・経営支援など、農業界のバリューチェーン全体を俯瞰し、各フェーズの課題を解決するために多角的な事業を展開しています。

01 背景と状況　担当者1名の管理体制とセキュリティ知識の不足
02 課題　セキュリティ製品の選定とセキュリティ意識の向上
03 取組内容　EDR導入など具体的な取組方針を検討
04 結果と今後　セキュリティ製品の導入計画立案と予算化を推進

Before After 取組を通じたビフォーアフター



01 背景と状況

セキュリティ担当は1名の兼務体制、UTMの導入や規程類の整備は実施済み

担当者1名による管理体制 / セキュリティの専門的な知識が不足 / UTMや規程類の整備は実施済み

セキュリティ対策は、経営企画部門の担当者1名体制で他の情報システム業務を兼務しています。担当者は前職での経験を活かし、UTM（Unified Threat Management）やセキュリティ規程の整備などは自身で進めました。対策を体系的に学びたいと考え、本事業に参加しました。

02 セキュリティ課題

セキュリティ製品の選定とセキュリティ意識の向上

当初の課題
- 社内のセキュリティ意識に個人差がある
- 効果的なセキュリティ教育の実施方法を検討したい
- 対策に必要かつ適切な投資コストが不明確

専門家派遣支援で明らかになった課題
- UTMのログ管理などネットワーク対策の強化
- 重要データのバックアップ運用の整備
- 持ち出し用デバイスのデータ保護対策の強化

03 取組内容

STEP 1　本事業の専門家派遣に上長とともに参加し、迅速な対策の検討と予算化を推進

本事業の専門家派遣において、会社として不足しているセキュリティ対策について整理し、セキュリティ製品の導入を中心としたセキュリティ対策の強化を検討することにしました。上長とともに本事業の打合せに参加することで意思決定の早期化を図り、予算化など必要な措置もあわせて進めていきました。

STEP 2　本事業の専門家のアドバイスをもとにEDRの導入計画を策定

EDRの導入については、以前から検討していましたが、本事業の専門家からのアドバイスにより、同社のネットワーク環境において必要な機能に基づく製品選定を行い、令和6年春の導入に向けた具体的な導入計画を策定しました。

STEP 3　ファイルサーバの入替に伴い、データのバックアップ運用を見直し

データセンターで運用しているファイルサーバについては、入替を計画しています。製品選定の際に、重要データの世代管理などのバックアップ運用の強化策もあわせて検討することで、より効果的なバックアップ運用の実現を目指しています。

STEP 4　UTMのログ管理については、ベンダーとの連携による監視サービスの導入を検討

UTMから取得可能なログの取得や管理方法については、本事業の専門家からアドバイスを受け、ベンダーとの連携による監視サービスの活用を検討しています。取得したログの確認については、生成AIのサービスを活用する方法の提案を受け、活用を検討しています。

セキュリティ製品導入を中心とした対策強化策を立案

四半期に一度、経営層も参加するセキュリティ推進会議が開催されていますが、監査役より外部からのサイバー攻撃に対するセキュリティ対策の必要性などが指摘されていました。そのため、以前からEDR（Endpoint Detection and Response）の導入などを継続的に検討していました。本事業の専門家派遣において、セキュリティ対策に関わる課題を洗い出すとともに、セキュリティ製品の導入を中心とした具体的な検討を行い、導入計画の立案や予算化に向けた調整を進めました。
まず、EDRの導入については、令和6年春の導入に向けて自社のネットワーク環境に合わせた製品の選定および予算申請を進めています。また、重要データの保護については、ファイルサーバの入替を検討していたことから、製品選定に加えて世代管理などのバックアップ運用の強化策も検討することにしました。UTMのログ管理については、ベンダーの監視サービスの活用による運用管理の強化を検討しています。このほか、懸案となっていた社内のセキュリティ教育や持ち出し用デバイスのディスク暗号化といった対策については、長期的に取り組んでいく方針としました。セミナーやワークショップで得た知見をもとに、セキュリティ規程についても内容を補完していく予定です。

04 結果と今後

セキュリティ製品の導入計画立案と予算化を推進

セキュリティ対策の強化に向けて、本事業の専門家のアドバイスに基づき、製品の選定と導入計画の立案ができました。EDRの導入は予算申請を進め、今後の導入を予定しています。バックアップ運用の整備もスケジュールを策定しています。今後は担当者の増員などによる管理体制強化も進める予定です。本事業により、必要なセキュリティ対策の8割程度が達成できたと担当者は考えています。

経営層の声
本事業の専門家によって、当社のセキュリティ対策の状況が可視化され、必要なセキュリティ対策に関する支援を十分に受けられたと感じています。コスト面においても費用対効果が明確になったことで、当社のセキュリティ対策強化に大きく貢献いただき、感謝しています。

参加者の声
本事業への参加を通じて、これまでのセキュリティ対策に関する課題認識と取組の方向性が間違っていないことが確認できました。また、今後の対策に関する優先順位づけや計画立案に対する有効なアドバイスを受けることができました。今後も意識を高く持って推進します。

IT中心のセキュリティ対策から、確かなセキュリティ規程に基づいたセキュリティ対策へ

取り組んだ支援テーマ：**ネットワークセキュリティ** / エンドポイントセキュリティ / モバイルデバイス / データ保護 / **セキュリティ意識と教育** / 外部パートナーとの関係

企業プロフィール

- 業種 / 従業員数：製造業 / ～300 名
- セキュリティ体制：1名体制　兼務

事業内容　工業製品などの組立時に必要な特殊工具の製造・販売を行う機械工具メーカーです。工場を含め、国内外に複数拠点を持ち、販売代理店を通じて商品を提供しています。自社製品は、自動車、船舶、記憶媒体装置など、幅広い業種で使用されており、ものづくりを支える「製造業のための製造業」として貢献している企業です。

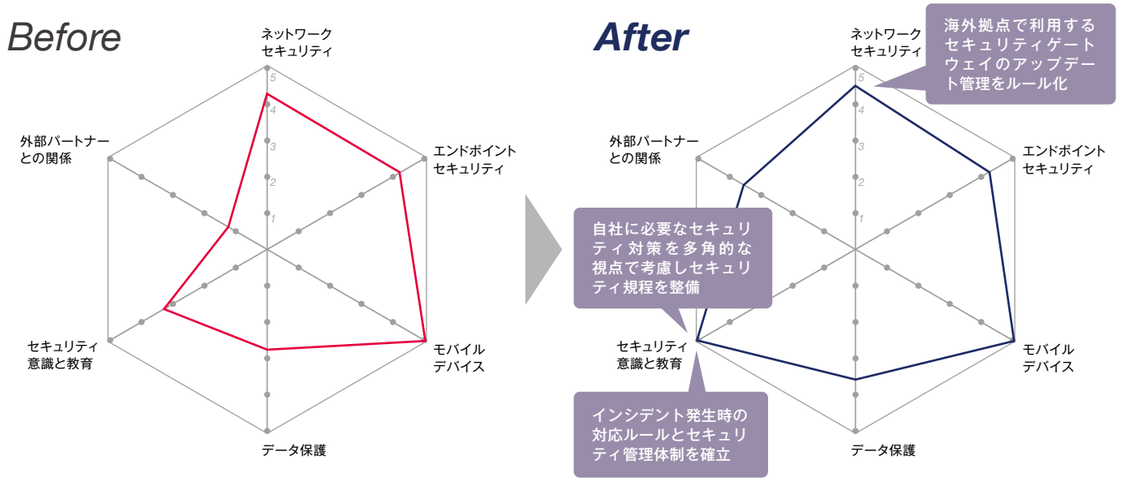
01 背景と状況　これまではITによるセキュリティ対策が中心

02 課題　体系的なセキュリティ方針や各種規程類の整備

03 取組内容　専門的な知見に基づくセキュリティ規程やルールの整備

04 結果と今後　セキュリティ規程が完成し、計画に対し7割の取組を達成

Before **After** 取組を通じたビフォーアフター



01 背景と状況

担当者1名の管理体制でITによるセキュリティ対策を中心に推進し、社内教育も開始

- 兼務の担当者1名での管理体制
- セキュリティ対策の知識を独学で習得
- 従業員向けセキュリティ教育を開始

セキュリティ担当は情報システム部門の課長1名が他業務と兼務しています。担当者はベンダーのセミナーなどを通じ独学でセキュリティ対策の知識を習得しつつ、経営層の理解を得ながらITによるセキュリティ対策を中心に推進しています。今年度から工場部門の役職者を対象に情報セキュリティ教育を実施しています。

02 セキュリティ課題

体系的な社内のセキュリティ方針や各種規程類の整備

当初の課題

- 体系的な知識がなくセキュリティ規程などが未整備
- セキュリティ人材育成と教育体制の強化

専門家派遣支援で明らかになった課題

- セキュリティ方針や社内ルールの体系化
- 社内のインシデント報告体制の確立・文書化
- サプライチェーンのネットワーク機器の管理

03 取組内容

STEP 1　専門家派遣によるセキュリティ対策に関する現状分析と課題整理、対応計画の策定

本事業の専門家派遣で同社のセキュリティ状況についてヒアリングを実施しました。セキュリティ方針や各種規程類の整備を最終目標として取組を進めることを確認し、ウィークポイントに対する対応計画を策定しました。

STEP 2　社内のインシデント報告体制の確立に向けたセキュリティ機器などの作業記録を取得

セキュリティ機器などの設定変更に関する作業記録を取得していなかったため、スプレッドシートによる管理を実施しました。また、インシデント発生時に別担当者が対応できるよう社内のインシデント報告体制を構築し、連絡網や体制図の作成ルールに関する明文化を進めました。

STEP 3　海外拠点で利用するセキュリティゲートウェイのアップデート状況の確認

海外拠点から自社のLANに接続する場合があるため、セキュリティゲートウェイに関するメーカーウェブサイトのリリース情報を毎週確認することとし、セキュリティパッチがリリースされている場合には確認後1週間以内に適用完了するルールとしました。

STEP 4　取組目標だったセキュリティ規程の完成と人材育成に関わる取組の推進

独立行政法人情報処理推進機構（IPA）が公開しているサンプル規程をひな型としてセキュリティ規程を作成し、本事業の専門家によるアドバイスを受けながら完成させました。また、セキュリティ規程の整備に伴い、社内のセキュリティ人材育成に向けての知識も習得しました。

セキュリティ規程やさまざまなルールづくりを推進

社内のセキュリティ意識を向上させ、インシデント発生時の対応ルールを浸透させていくことが重要であると捉え、製品の設計データや特許に関する情報などの漏えいを防ぐため、今年度から工場部門の役職者を対象に情報セキュリティ教育を継続的に実施しています。あわせて、体系的な知識に基づいたセキュリティ規程やルールの整備を最終目標として取組を推進しました。セキュリティ規程は、本事業の専門家派遣でのアドバイスにより、セキュリティに関わる人員や役割、クラウドサービス利用時の規程を含む、数十ページに上る文書を作成しました。また、セキュリティ機器などの設定変更に関する作業記録を取得していなかったため、変更履歴をすべて確認できるよう、作業記録に関する情報はスプレッドシートを活用して一元化する管理方法を確立しました。これにより、インシデント発生時の対応ルールが明確になりました。また、セキュリティ管理体制の強化に向け、担当者自身が人材育成できるよう教育実施なども盛り込んだセキュリティ規程の整備も行いました。このほか、海外拠点で利用するセキュリティゲートウェイのアップデート管理に関するルール化を推進しました。全従業員へのスマートフォン貸与を進めた際には、運用に関するルール作成にも知見を活かしています。

04 結果と今後

本事業で設定した対応計画の7割程度を達成

本事業で設定した対応計画に基づき、担当者を中心にセキュリティ対策を進めた結果、対応計画の7割程度を事業期間内に達成できました。個々の課題を着実に進めたことにより、最終目標としていたセキュリティ規程の整備も完了させることができました。残りの3割については今回の取組を活かしながら、ファイル共有に関する可視化ツールの導入を検討するなど、来期以降も継続していく方針です。

経営層の声

体系的なカリキュラムと実践を伴うワークショップまで無償で受講でき、非常に有益でした。今回を機に社内教育への取組を開始し、全社への情報展開や波及効果に期待しています。全従業員へのスマートフォン貸与を進めており、セキュリティ意識の向上が必要だと感じています。

参加者の声

これまでは独自にセキュリティ対策を進めてきましたが、専門家の的確なアドバイスに加え、ワークショップでは他社の担当者と同じ悩みを共有できたことで解決策が見えてきました。本事業への参加によりセキュリティ対策を大きく前進させることができたと思います。

取引先が求める厳格なセキュリティ新基準の準拠に向けたセキュリティ対策を実行

取り組んだ支援テーマ：**ネットワークセキュリティ** / エンドポイントセキュリティ / モバイルデバイス / データ保護 / **セキュリティ意識と教育** / 外部パートナーとの関係

企業プロフィール　業種 / 従業員数：製造業 / ～300 名　セキュリティ体制：**複数**　**兼務**

事業内容　各種電子機器や制御機器の設計・製造、開発受託を主軸として、自社製品の販売事業も展開している電子機器メーカーです。情報通信機器や医療機器などの分野において、IoT機器の小型基盤開発や比較的大きな装置の組立から検査を実施するなど、取引先からの多様なニーズに対応しています。

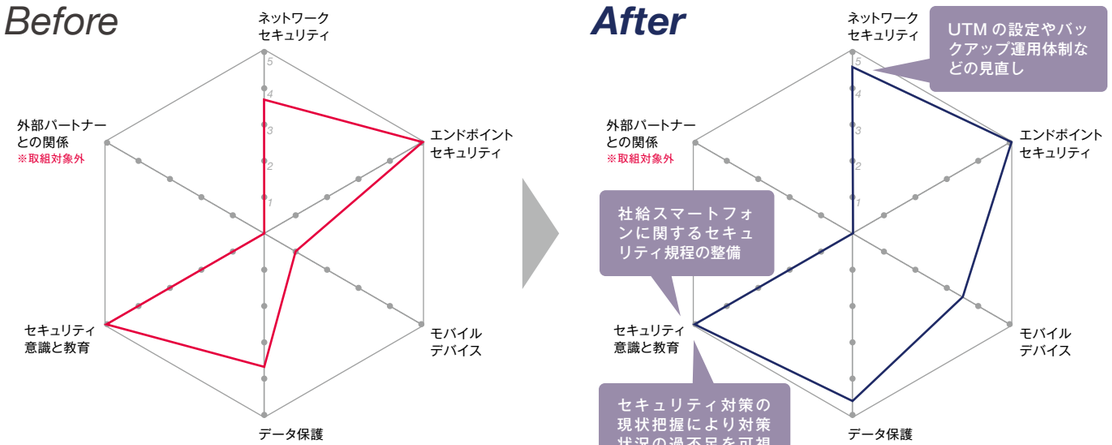
01 背景と状況　セキュリティ規程の整備や技術的対策は一通り実施済み

02 課題　取引先が求める厳格なセキュリティ新基準への対応

03 取組内容　セキュリティ新基準準拠のための現状把握と対応検討

04 結果と今後　本事業終了後もセキュリティ対策の取組と予算化を推進

Before **After** 取組を通じたビフォーアフター



01 背景と状況

取引先が求めるセキュリティ新基準に対応する必要性が新たに浮上

- セキュリティ規程の更新は随時実施
- 隔月でセキュリティ委員会を開催
- セキュリティ新基準への対応が必要

10年以上前からセキュリティ規程の整備や更新を行うとともに、隔月でセキュリティ委員会を開催するなど、一通りのセキュリティ対策は講じています。令和7年度から厳格なセキュリティ基準への準拠が主要取引先に求められていることもあり、セキュリティに関する知見を得ることなどを目的に本事業に参加しました。

02 セキュリティ課題

取引先が求めるセキュリティ新基準準拠に向けた課題対応

当初の課題
- 社内のセキュリティ対策の現状把握および評価
- セキュリティ新基準への準拠に向けた課題の可視化

専門家派遣支援で明らかになった課題
- UTM の設定の見直し
- バックアップからデータを復旧する方法の見直し
- 社給スマートフォンの利用ルールを制定

03 取組内容

STEP 1　UTMの設定確認とログの活用

UTMによるさまざまなセキュリティ機能を十分に活用できていなかったため、まずはログを活用したセキュリティ状況の確認を実施することにしました。UTMから出力される週次レポートの内容を確認し、不明点についてはベンダーへの問合せや自社での調査を実施しました。

STEP 2　バックアップからデータを復旧する方法の検討

セキュリティ要件の一つとなっている「復旧」に対応するため、バックアップからのデータ復旧に要する時間を短縮することを目的に、ファイルサーバの入替を検討することにしました。

STEP 3　社給スマートフォンに関するセキュリティ規程の整備

社給スマートフォンに関しては、本社勤務の従業員にのみ支給されているため使用者は限られているものの、セキュリティ規程は未整備だったため、社内の利用ルールを明文化し、セキュリティ規程に盛り込むことにしました。

STEP 4　取引先が提示したセキュリティチェックリストに基づく課題の可視化と対応策検討

本事業の参加の主目的である、取引先が求めるセキュリティ新基準への準拠を進めるため、取引先から提示されたチェックリストに基づき現状整理を行い、セキュリティ課題の可視化を行いました。本事業の専門家と相談しながら不足しているセキュリティ対策を検討し、順次対策を講じることにしました。

セキュリティ新基準への準拠に向けたセキュリティ対策の整備

同社は既にISMS認証要件を満たしているものの、令和7年度より取引先から高いレベルのセキュリティ基準を要求されています。そのため専門家派遣では、取引先が求める新基準への準拠に向けた課題を中心に対応しました。導入済みのUTM（Unified Threat Management）に関しては、ファイアウォール以外の機能が無効になっていたため、ログの管理設定を再確認するとともに、ベンダーによるアップデート管理に関するアドバイスを受けました。また、社給スマートフォンに関しては、使用者は少ないもののセキュリティ規程が未整備だったため、運用ルールなどの整備を進めました。この他、ファイルサーバの入替時にデータをコピーするために2週間かかったことから、令和5年度中にデータの復旧方法を再検討することにしました。また、取引先が求めるセキュリティ新基準への準拠に向けて、取引先から提示されたチェックリストに基づき現状を整理し、本事業の専門家による確認を踏まえてセキュリティ課題の可視化を行い、「ログの改ざんや消失の防止策、監視ツールの導入など管理方法の検討」、「ソフトウェアの構成管理用ツールの選定と管理手順の作成」、「インシデント対応手順書の整備と対応訓練の実施計画作成」など、必要な対応策を検討しました。

04 結果と今後

セキュリティ新基準への準拠に向けた取組を継続

取組を進めた結果、取引先が求めるセキュリティ新基準への準拠に向けた知見や気づきを得ることができました。また、本事業の専門家からアドバイスを受け、独立行政法人情報処理推進機構（IPA）が公開しているひな型を参考にすることにより、セキュリティ規程などを効率的に整備する方法などを習得できたほか、予算化が必要なセキュリティ対策についても継続して進めていく方針です。

経営層の声

本事業への参加を通じてセキュリティ担当が専門的な知識を習得し、セキュリティ対策の整備につながったことは有意義だったと感じています。取引先からの信頼維持および向上を目指し、セキュリティレベルを高めることができるセキュリティ管理体制の構築に期待しています。

参加者の声

本事業の専門家や他社の担当者との会話を通じて、自社のセキュリティ対策に関する取組が一定の水準に達していることを確認できました。今回得た知見から従業員が安心して事業活動できる環境の整備に取り組みます。本事業に参加することができて大変感謝しています。

本事業の専門家からのアドバイスを活用し、インシデント対応フローを具体化して作成

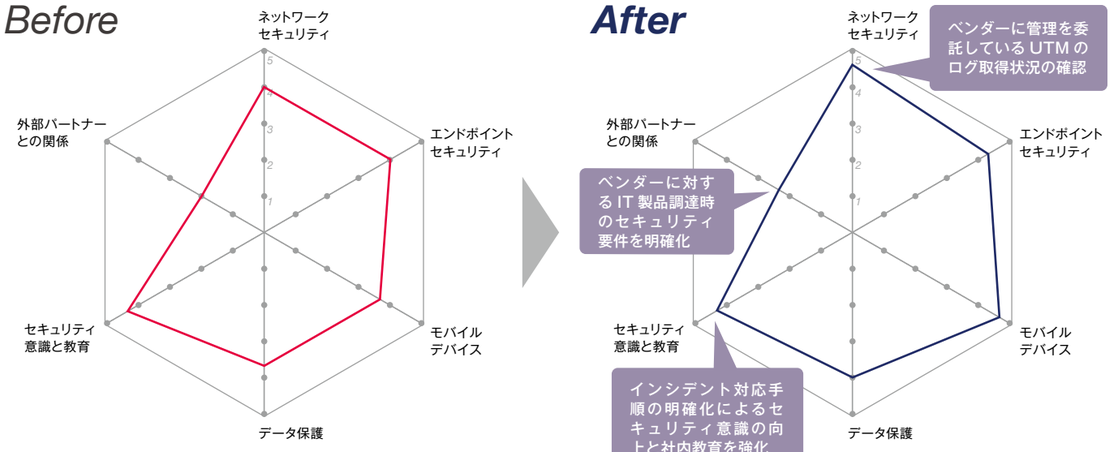
取り組んだ支援テーマ：ネットワークセキュリティ / エンドポイントセキュリティ / モバイルデバイス / データ保護 / セキュリティ意識と教育 / 外部パートナーとの関係

企業プロフィール　業種 / 従業員数：製造業 / ～300 名　セキュリティ体制：複数　兼務

事業内容　オフィス用品の製造販売および輸入販売を行っています。取引先の多様なニーズに対応するため、幅広い製品を取り扱っており、快適なオフィス環境に貢献するソリューションを提供しています。また、海外に拠点を置くグループ会社を通じて、国際市場への販路拡大も進めています。

01 背景と状況　セキュリティに関するルールの見直しと刷新
02 課題　インシデント報告後の対応が明確化されていない
03 取組内容　インシデント発生時の具体的な手順を検討
04 結果と今後　インシデント対応の明文化・フロー化を推進

Before **After** 取組を通じたビフォーアフター



01 背景と状況

セキュリティに関するルールの刷新と社内教育制度の整備が必要

- 業務でPCを使用する機会が増加
- セキュリティのルールの見直しが必要
- 社内のセキュリティ研修を不定期で開催

テレワークなどにより業務でPCを使用する機会が増加したため、情報セキュリティに関するルールの刷新および社内教育制度を整備する必要性を感じています。セキュリティ担当は2～4名が兼任で担当しています。社内教育では独立行政法人情報処理推進機構（IPA）の資料をもとに不定期で研修を実施しています。

02 セキュリティ課題

インシデント対応フロー作成とセキュリティ教育整備

当初の課題
- セキュリティ規程は基本的な内容しか決定していない
- インシデント報告後の対応フローが不明確
- セキュリティ教育の定期的な実施計画の立案が必要

専門家派遣支援で明らかになった課題
- ベンダーの製品調達時のセキュリティ要件が不明確
- ウイルス対策ソフトウェアの定期スキャンが未実施
- ネットワークログの取得ができていない

03 取組内容

STEP 1　セキュリティ関連の課題を洗い出し、優先的に着手する課題を決定

本事業の専門家のヒアリングにより、セキュリティに関する7つの課題をリストアップしました。優先順位を検討し、課題の中でも緊急性が高く、本事業に参加する前から課題であったインシデント対応のフロー作成を最優先に着手することにしました。

STEP 2　「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」をもとに手順検討

IPAが提供している「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」を参考にして、自社の事業に合わせた対応手順を検討しました。セキュリティ担当部門内に加えて、他の部署や取引先にもインシデント対応フローを公開する必要があるため、慎重に進めています。

STEP 3　ログの取得、ベンダーへのIT製品調達時のセキュリティ要件を確認

ネットワークログの取得ができていなかったため、ベンダーにログの取得状況の確認を行いました。また、IPAが提供している「IT製品の調達におけるセキュリティ要件リスト」を参考にして、ベンダーへのIT製品調達の際に設定すべきセキュリティ要件について検討し明確化しました。

STEP 4　インシデント対応フロー作成に必要な調整を実施。令和6年度での予算化が決定

インシデント対応フロー作成に関しては、ベンダーへ依頼する作業などを整理しています。検討を進める上で明確になった課題に関しては、順次対応しています。また、インシデント対応に関わる費用については、令和6年度での予算化を進めています。

インシデント発生時の具体的な手順とフローの整備

本事業に参加する前から課題であったインシデント対応フローの作成と、重要性の高いセキュリティ課題を個別に対応することにしました。インシデント対応フローに関しては、一次報告後の対応手順や、インシデント履歴の管理方法が明文化されていませんでした。そのため、本事業の専門家からIPAが提供している「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」を紹介され、記載されている内容を参考にして対応手順の具体化を進めています。セキュリティ担当部門の調整に加えて、他の部署やベンダーとも連携しながらインシデント対応フローを作成しています。また、セキュリティ対策の見直しと刷新も行いました。ネットワーク機器に関しては、ネットワークログが取得できていなかったため、本事業の専門家からアドバイスを受けながら、ネットワークログの取得状況についてベンダーに確認を行いました。また、ベンダーへのIT製品の調達に関わるセキュリティ要件を設定していなかったため、IPAが提供している「IT製品の調達におけるセキュリティ要件リスト」を参考にして、本事業の専門家と相談しながら不明点を洗い出すことにより、自社として必要となるセキュリティ要件を明確化しました。

04 結果と今後

インシデント対応の手順化、セキュリティ体制を改善

本事業に参加する前は、自社のインシデント対応について不足している点が理解できていませんでしたが、本事業の専門家派遣やセミナー・ワークショップを通じて、取り組むべき課題が明確になりました。今後は、明確になった課題を解決することに注力します。また、今まで不定期で実施していたセキュリティ教育については、定期的に効率よく学習できる仕組みづくりを進めていく予定です。

経営層の声

サイバーセキュリティ対策は事業を存続するためにも喫緊の課題ですが、社内のリソースで対応することは難しく、東京都主催で本事業を実施いただき大変助かりました。人材不足の中、セキュリティ人材の育成という面に力点が置かれていることは価値があると感じています。

参加者の声

本事業のワークショップにおいては、一般的なセキュリティ対応を自社の業務に落とし込む難しさを実感しました。一例として、リスク管理の課題では、情報資産を洗い出すことに予想以上に時間がかかりました。このような知見を得ることができたことは良い経験となりました。

技術面偏重のセキュリティ対策から脱却
バランスの取れたセキュリティ管理体制を構築

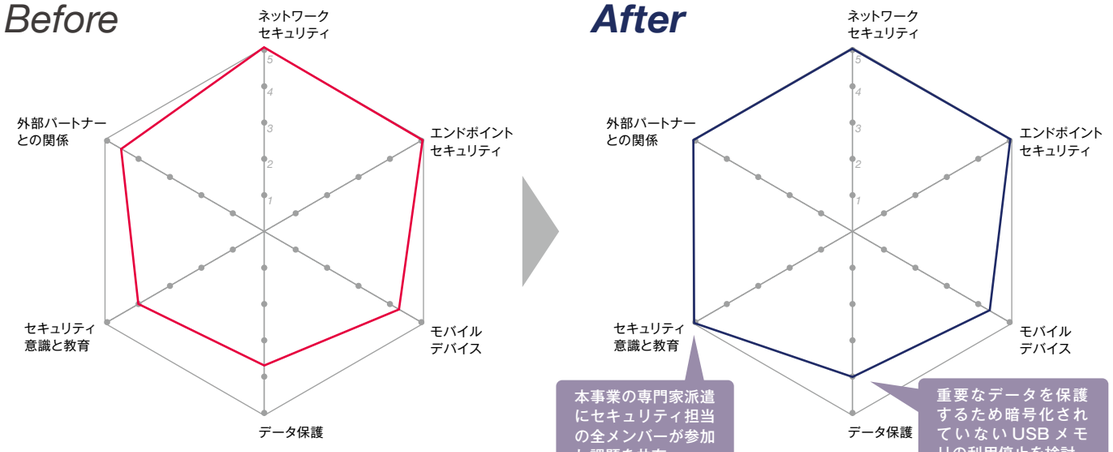
取り組んだ支援テーマ：**データ保護**／ネットワークセキュリティ／エンドポイントセキュリティ／モバイルデバイス／セキュリティ意識と教育／外部パートナーとの関係

企業プロフィール　業種 / 従業員数：製造業 / ～300 名　セキュリティ体制：複数　兼務

事業内容　建築物の内外装に使用する金属製建材の設計・製造・施工を手掛ける企業です。これまで蓄積してきた技術力と最新のテクノロジーを組み合わせ、住宅、オフィス、店舗、学校などの多様な施設に取りつけるオーダーメイドの金属製建材を製造しています。近年は国内に加え、海外のさまざまなプロジェクトにも携わっています。

01 背景と状況　技術面偏重のセキュリティ対策に不安あり
02 課題　取り組むべき課題の優先度が不明確
03 取組内容　技術面以外のセキュリティ対策を中心に実施
04 結果と今後　バランスの取れたセキュリティ管理体制を構築

Before ***After*** 取組を通じたビフォーアフター



01 背景と状況

技術面を中心とした現状のセキュリティ対策状況を第三者視点から評価したい

- セキュリティ対策は技術面が中心
- セキュリティ知識は独学で習得
- セキュリティ対策関連の委員会を組織

セキュリティ担当者が独学で習得した知識をもとに、技術面を中心としたセキュリティ対策を講じています。令和3年にSECURITY ACTION（二つ星）を宣言した際に、社内の各部門より1名ずつ参加する形でセキュリティ対策の強化を目的とする委員会を組織し、月1回定例会を開催しています。

02 セキュリティ課題

各セキュリティ対策の優先順位が明確になっていない

当初の課題
- セキュリティ担当者が知識を身につける機会がない
- セキュリティ対策として不十分な対策を知りたい
- 従業員への効果的な教育方法がわからない

専門家派遣支援で明らかになった課題
- USB メモリの使用が常態化し、管理できていない
- セキュリティ規程が整備できていない
- インシデントの発生や対応の履歴が記録できていない

03 取組内容

STEP 1　セキュリティ対策の基本となる考え方とフレームワーク活用の重要性を理解

セキュリティ対策の基本的な考え方を理解することにより、現状では技術的なセキュリティ対策に偏重していることに気づきました。また、セキュリティ対策の策定に際しては、フレームワークを活用することにより、ゼロベースで対策を検討することなく、効率的かつ網羅性をもって推進できることを学びました。

STEP 2　「緊急性の高い課題」と「中長期的に取り組んでいく課題」への分類を実施

本事業の専門家派遣において洗い出された、さまざまなセキュリティ課題に対して、影響度や緊急度による優先順位づけを行いました。「緊急性の高い課題」、「中長期的に解決していく課題」に分類し、セキュリティ対策の強化を目指す委員会で共有することにより具体的な対策を検討しました。

STEP 3　本事業の専門家派遣にセキュリティ対策に取り組む委員会の全メンバーが参加

本事業の専門家派遣にセキュリティ対策に取り組む委員会の全メンバーが参加する回を設けて、座談会形式で質疑応答を実施しました。メンバー間の課題共有に加え、本事業の専門家による明快なアドバイスによって、一人一人のメンバーが抱えていた不安や悩みを解消することができました。

STEP 4　技術面にとらわれることなく、網羅的な観点からセキュリティ対策を実行

具体的なセキュリティ対策としては、「USBメモリの利用停止のルール化」、「セキュリティガイドライン作成への着手」、「ヒヤリハット事案を含むインシデントの記録および是正プロセスの策定」などを行うことで、技術面にとらわれることなく、網羅的な観点から対策を実行しています。

セキュリティ対策の強化を目指す委員会主導の管理強化

本事業のセミナーにおいて、セキュリティ対策の基本的な考え方を理解したことに加え、セキュリティ対策の策定にフレームワークを活用することの重要性に気づきました。本事業の専門家派遣では、現状の対応で不十分な対策を洗い出した上で、さまざまなセキュリティ課題に対して影響度や緊急度による優先順位づけを行い、「限られたリソースおよび予算で迅速に取り組む緊急性の高い課題」、「中長期的に解決していく課題」に分類しました。セキュリティ意識の向上を目的として、本事業の専門家派遣の中にセキュリティ対策の強化を目指す委員会の全メンバーが参加する座談会の場を設けました。座談会では活発な質疑応答が行われ、メンバー間で課題を共有することに加え、セキュリティに関する知識のアップデートを行うことができました。リスクの高い課題への取組としては、「暗号化されていないUSB メモリによるデータの持ち出しが常態化している」ことを指摘され、今後の利用停止を検討しました。セキュリティ規程に関しては、社内向けのセキュリティガイドラインから段階的に作成していくことを決定し、着手しています。インシデント対策としては、インシデント発生の傾向を可視化するためにヒヤリハット事案を含めて記録し、組織内で共有できるようにしました。

04 結果と今後

セキュリティ対策に取り組む委員会の活発化が目標

セキュリティ対策全般において、緊急度および重要度の高い課題を把握しました。それらを解決する計画を立て、来年度より本格的に取り組む予定です。中長期的に取り組む課題としては、各部署のセキュリティ対策における手順の策定を予定しています。また、セキュリティ対策に取り組む委員会の活動を活発化し、全社的にセキュリティ対策を推進していきたいと考えています。

経営層の声

本事業への参加を通じ、現状のセキュリティ対策において対応できていることと、今後取り組むべき課題が明確になりました。本事業で習得した知識を活かして、今後のセキュリティ対策を全社的に進め、取引先に安心してもらえるセキュリティ管理体制の構築を目指します。

参加者の声

これまで実施してきた自社のセキュリティ対策が、技術的な管理策に偏っていたことを痛感しました。今後は、「人的」「組織的」「物理的」なアプローチを段階的に進めていき、バランスの取れたセキュリティ対策を実施していきたいと考えています。

情報資産の棚卸しを行い、リスクを分析
セキュリティ規程を修正し円滑な運用を実現

取り組んだ支援テーマ：ネットワークセキュリティ / エンドポイントセキュリティ / モバイルデバイス / データ保護 / セキュリティ意識と教育 / 外部パートナーとの関係

企業プロフィール

- 業種 / 従業員数：製造業 / ～300 名
- セキュリティ体制：複数 / 兼務

事業内容

主に自動車、スマートフォンなどに使われる半導体や電子部品にめっき加工を行っています。取引先の製品の部分的な加工に加え、企画段階から試作・開発、量産、アフターフォローに至るまで、あらゆる生産プロセスをめっき技術でサポートするサービスを提供しています。

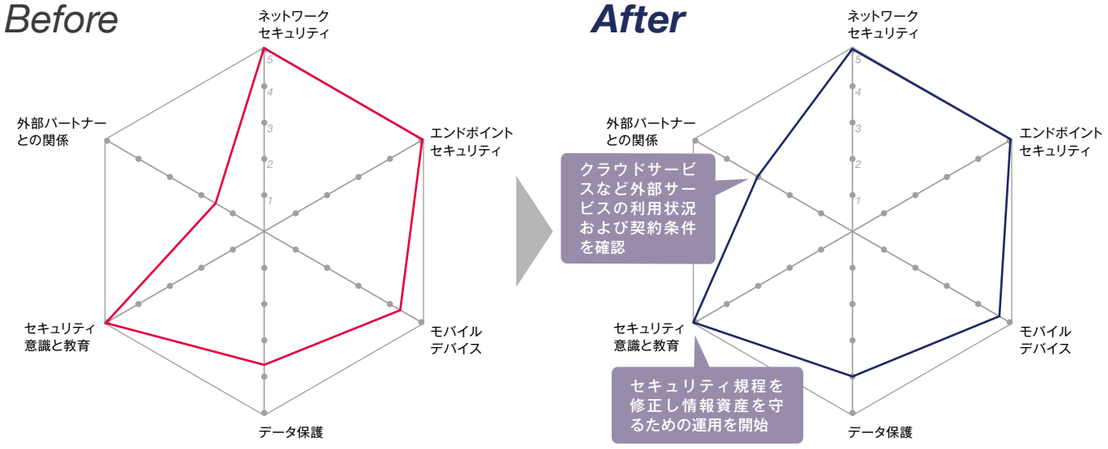
01 背景と状況
取引先の要望をベースとするセキュリティ対策を実施

02 課題
情報資産に紐づくセキュリティ規程の運用が不十分

03 取組内容
情報資産を守るための セキュリティ対策を実現

04 結果と今後
全従業員によるセキュリティ規程の運用が目標

Before ***After*** 取組を通じたビフォーアフター



01 背景と状況

セキュリティ規程の社内展開が不十分で現場に浸透していない

- 取引先の要望で具体的な対策に着手
- 規程類の運用が浸透していない
- 担当者3名のセキュリティ管理体制

約15年前、取引先からISMSに則ったセキュリティ対策を要望され、セキュリティ規程を作成しました。その後、約5年前に見直しを行いましたが、セキュリティ規程が自社の業務に適合していなかったため、社内へ浸透せず円滑な運用ができていません。セキュリティ対策は担当部署の3名が主導しています。

02 セキュリティ課題

情報資産を守るためのセキュリティ対策が不十分

当初の課題

- セキュリティ対策の客観的評価ができていない
- セキュリティ規程の PDCA サイクルが回っていない
- 情報資産の棚卸しができていない

専門家派遣支援で明らかになった課題

- リスク対応の要否判断ができていない
- 外部サービスの利用状況が把握できていない
- 業務委託先のセキュリティ対策が管理できていない

03 取組内容

STEP 1　現状のセキュリティ対策を点検し、課題の洗い出しを実施

本事業の専門家派遣において、現状のセキュリティ対策を点検し、課題の洗い出しを実施しました。その結果、「セキュリティ規程のメンテナンス」、「情報資産の棚卸し」、「各部門のセキュリティ対策状況の可視化」、「社内における意識共有の強化」などの課題が浮き彫りとなりました。

STEP 2　セキュリティ規程の評価と情報資産の棚卸しを実行

見直しが必要だったセキュリティ規程は、IPAの提供するひな型を参照し、相違点を確認しながら修正しました。運用にあたっては、ISMSのPDCAサイクルに則った運用を行う方針としました。情報資産の棚卸しは、IPAの提供する「リスク分析シート」を活用し、各部門と連携して行いました。

STEP 3　全社的なセキュリティ対策状況の可視化に着手

各部門におけるクラウドサービスや取引先のEDIサービスなどの利用･契約状況を調査しました。また、業務委託先との契約状況やセキュリティ対策の要求内容などの把握も進めており、各部門におけるセキュリティ対策状況の可視化を行いました。

STEP 4　経営層に対してセキュリティ対策の重要性を説明し、全社的な取組に拡大

経営層に対して、セキュリティ対策に関する理解と全社に向けた発信について相談しました。セキュリティ対策の現状および課題、基本的な考え方、今後に向けた展望を説明することにより、セキュリティ対策が全社的な活動となることを目指していきます。

情報資産の重要度に基づくセキュリティ対策を実施

本事業の専門家派遣において、現状のセキュリティ対策を改めて点検し、課題の洗い出しを実施しました。ネットワーク関連のセキュリティ対策については、一定の評価が得られましたが、運用面や現場への浸透に関する課題が浮き彫りとなりました。また、各部門における取引先のEDI（Electronic Data Interchange）サービスなど外部サービスの利用・契約状況や、業務委託先のセキュリティ対策状況の把握など、「各部門のセキュリティ対策状況の可視化」という新たな課題に気づきました。セキュリティ規程に関しては、現場に十分浸透しておらず最新化などの運用管理ができていなかったため、見直しが必要だと考えていました。そこで、独立行政法人情報処理推進機構（IPA）の提供するひな型との相違点を確認し、必要に応じて修正を実施しました。記載項目の網羅性や現場運用との整合性を精査するとともに、ISMSに則った運用を行うことを検討しました。情報資産の棚卸しに関しては、各部門にIPAの提供する「リスク分析シート」への記入を依頼することに加えて、情報資産の重要性について理解を促しました。さらに、経営層に対してセキュリティ対策の現状および重要性を説明し、経営層と一体となったセキュリティ対策の推進を予定しています。

04 結果と今後

セキュリティ対策のPDCAサイクルを全社的に実行

情報資産の重要度を分類し、その結果に基づいて各種のセキュリティ対策を講じるという基本的な対策の強化を進めることができました。また、各部門におけるセキュリティ対策の状況も可視化されました。今後は、経営層をはじめとする全従業員で役割を分担し、セキュリティ対策のPDCAサイクルを実行することで、より強固なセキュリティ管理体制を構築していきたいと考えています。

経営層の声

当社が抱えているセキュリティ対策の課題に関して、本事業の専門家派遣において実情に沿ったアドバイスをいただき、改善への道筋がつきました。今後はセキュリティ規程に沿った明確な運用ルールを設け、共通認識のもとでPDCAサイクルを回していきたいと考えています。

参加者の声

本事業の専門家派遣において、自社のネットワークに関するセキュリティ対策を評価されたことは自信につながりました。人的リソースが不足している状況ですが、セキュリティ対策のPDCAサイクルの実行などにより、一つ一つの課題に順次対応していく予定です。

専門技術コンサルティング業 A 社

実効性のあるルールを策定し、教育方法を検討
従業員一人一人の自発的な取組を促進

取り組んだ支援テーマ：**ネットワークセキュリティ** / エンドポイントセキュリティ / モバイルデバイス / データ保護 / **セキュリティ意識と教育** / **外部パートナーとの関係**

企業プロフィール

業種 / 従業員数：学術研究・専門・技術サービス業 / ～20名

セキュリティ体制：1名体制 / 兼務 / 経営者

事業内容：再生可能エネルギーに関わる技術コンサルティングを行っている企業です。取引先からの依頼を受け、発電所の立地計画から発電量の予測、レイアウトの検討などを行い、カーボンニュートラルの実現に貢献しています。

01 背景と状況
基本的なセキュリティ対策は実施済み

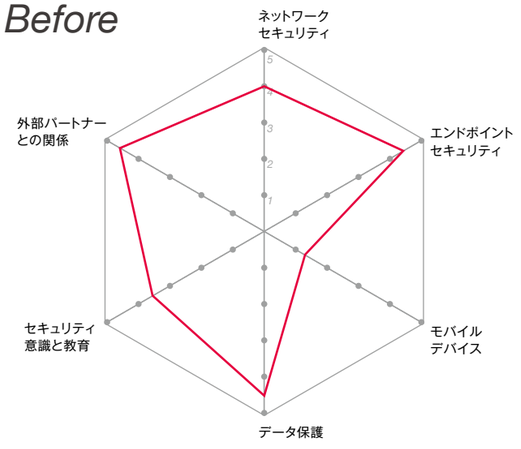
02 課題
実効性のあるセキュリティ教育ができていない

03 取組内容
ガイドラインを策定し、今後の教育方針を検討

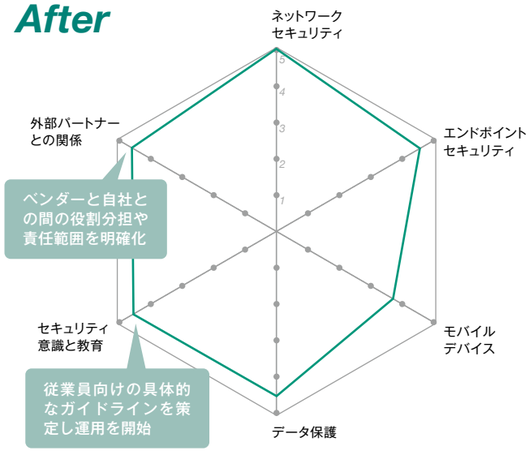
04 結果と今後
従業員一人一人の主体的な取組を促進

Before ***After*** 取組を通じたビフォーアフター

Before



After



01 背景と状況

基本的なセキュリティ対策から、実効性のある対策による強化が必要

基本的なセキュリティ対策は実施済み / ベンダーの責任範囲が不明確 / 実効性のある教育方法を模索中

UTM（Unified Threat Management）やアンチウイルスソフトウェアの導入など、基本的なセキュリティ対策は実施済みですが、ベンダーと自社の対応範囲の責任分界点が不明確です。取引先との信頼関係を構築・維持するため、継続的かつ実効性のあるセキュリティ対策を模索しています。

02 セキュリティ課題

実効性のあるセキュリティ対策および教育が必要

当初の課題
- 従業員向けのガイドラインが策定されていない
- 実効性のあるセキュリティ教育ができていない
- ベンダーと自社との責任範囲が不明確

専門家派遣支援で明らかになった課題
- 対応課題の明確化と優先順位づけが必要
- ノート PC のディスク暗号化を実施していない
- クラウドサービスでの多要素認証が導入されていない

03 取組内容

STEP 1 セキュリティ課題の洗い出しおよび詳細化

現状のセキュリティ対策を確認し、これまで大枠で捉えていた課題を洗い出し、詳細化した上で、実行すべき取組を明確にしました。さらに、課題の重要度を順位づけすることにより、今年度中に取り組む課題と来年度以降に取り組む課題に仕分けしました。

STEP 2 従業員向けの具体的な利用ルールを作成

セキュリティ規程に基づく従業員向けのガイドラインとして、テレワークを含むモバイル端末使用時の具体的な利用ルールを作成し、現場での運用の定着を進めています。また、活用しているクラウドサービスの整理を行い、クラウドサービス利用時の多要素認証の導入などの認証強化を検討しています。

STEP 3 セキュリティ教育の拡充・浸透に向けて外部講師の活用を検討

策定したガイドラインの形骸化を防ぐとともに、セキュリティ意識を浸透させるために、セキュリティ対策への理解を深める仕組みづくりを検討しました。セキュリティ担当者によるさまざまな情報共有とあわせて、外部講師を招いて研修を行うことにより、セキュリティ教育を拡充する方針を固めました。

STEP 4 セキュリティ対策に関するベンダーとの役割分担や責任範囲を明確化

現在のセキュリティ対策の状況と自社との役割分担や責任範囲を、ベンダーに確認しました。機器のファームウェアのアップデートに関しては、自社の対応範囲であることが明確になりました。UTMやシステムのログなどの管理に関しては、取得方法や保存期間などの観点から運用方法を検討しています。

ガイドラインの策定と実効性のある教育方法を検討

本事業の専門家派遣において、現状のセキュリティ対策を評価して課題の洗い出しと詳細化を行い、解決するべき課題の優先順位を明確化しました。まず、既存のセキュリティ規程に基づく従業員向けのガイドラインとして、テレワークを含むモバイル端末使用時の具体的な利用ルールを作成し、現場での運用の定着を進めています。また、クラウドサービス利用時における多要素認証の導入による認証強化も検討しています。社内セキュリティ教育の拡充・浸透という面においては、セキュリティ担当者による最新の脅威に関する情報共有などを継続することに加え、外部講師を招いた研修を検討することにより、より実効性のある教育実施の方法を検討しています。ネットワークセキュリティの強化策として、UTMの設定などのセキュリティ対策状況およびベンダーの対応範囲について、ベンダーに確認しました。機器のファームウェアのアップデートに関しては、自社の対応範囲であることを確認し、今後の運用方法を検討しています。ネットワークやシステムのログなどの管理に関しては、取得方法や保存期間など運用の観点から、クラウドサービスによるログ管理を検討しています。ノートPCにおけるディスク暗号化については、ツールの適用を予定しています。

04 結果と今後

継続的かつ実効性のあるセキュリティ対策を推進

本事業への参加により、セキュリティ対策における課題の把握と必要な対策を整理することができました。今後はセキュリティ教育を強化していき、従業員が知識を深めることによりセキュリティに関する意識を向上させ、自発的にセキュリティ対策へ取り組むことを促していきます。ビジネス面においても、取引先との信頼関係を築いていく基盤になると考えています。

経営層としての声

本事業を通じ、企業が経営基盤を強固にするための取組の一環として、セキュリティ対策の重要性を認識することができました。従業員のITに関するスキルレベルに違いがある中で、従業員一人一人が納得して対応できるような仕組みの構築を進めていきたいと考えています。

参加者としての声

本事業のセミナーで網羅的な知識を習得したことに加え、他社のセキュリティ対策から気づきを得ることも多くありました。また、専門家からの適切なアドバイスにより、セキュリティ対策強化に向けた具体的な進め方や今後のプランニングができたと実感しています。

セキュリティ対策のフレームワークを習得
規程類を整備し管理体制強化の土台を構築

取り組んだ支援テーマ：ネットワークセキュリティ / エンドポイントセキュリティ / モバイルデバイス / データ保護 / セキュリティ意識と教育 / 外部パートナーとの関係

企業プロフィール

業種 / 従業員数：金融業・保険業 / ～20名

セキュリティ体制：1名体制　兼務

事業内容

投資助言・代理業の登録を申請し、開業準備を進めています。開業後は、顧客と投資顧問契約を結び、暗号資産に関する価値を調査・分析し、投資判断に基づく助言を行っていく予定です。また、ブロックチェーン関連のコンサルティング事業や、金融商品関連情報の発信およびメディアの管理運営事業も展開する予定です。

01 背景と状況
独学によって進めているセキュリティ対策に不安がある

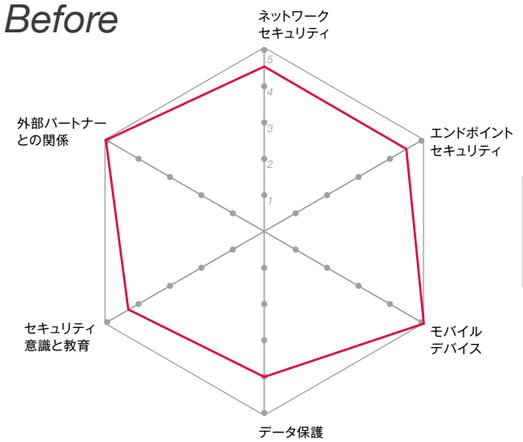
02 課題
開業に向けてセキュリティ対策の強化が必須

03 取組内容
セキュリティ対策のフレームワークを活用

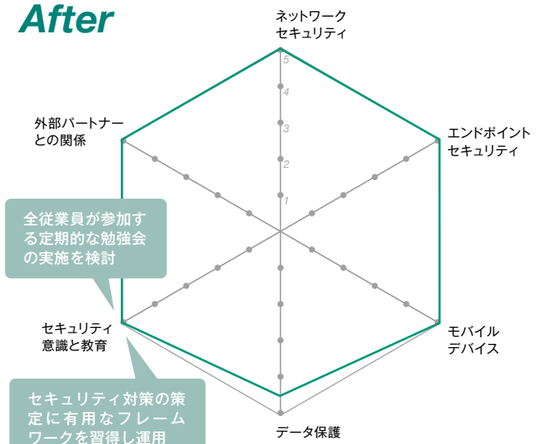
04 結果と今後
さらなるリテラシーの向上を目指し努力を継続

Before ***After*** 取組を通じたビフォーアフター

Before



After



01 背景と状況

投資助言業の開業に向けて、業態に則したセキュリティ対策を講じたい

- 投資助言業の開業準備中
- 顧客と電子契約する仕組みを導入予定
- 独学でセキュリティ対策を実施している

投資助言業の開業準備を進めています。電子契約で顧客の個人情報を取り扱う予定のため、情報セキュリティについては万全の対策を講じる必要があります。現状はセキュリティ担当者が独立行政法人情報処理推進機構（IPA）の各種ドキュメント類を参照し、独学で勉強しながらセキュリティ対策を実施しています。

02 セキュリティ課題

個人情報を取り扱うサービス事業者としての知識習得が必須

当初の課題

- セキュリティ対策のためのフレームワークを習得したい
- セキュリティ規程の維持管理が実施できていない
- 「個人情報保護法」に則した措置の知識を得たい

専門家派遣支援で明らかになった課題

- 情報資産管理台帳を作成していない
- 従業員の意識を共有する場を設定できていない
- ウェブサイトのセキュリティ対策状況の確認が不十分

03 取組内容

STEP 1　フレームワークを理解し、セキュリティ対策の策定に活用

セキュリティ対策の検討を進める上で、「情報資産の洗い出し～リスク分析と可視化～セキュリティ対策の優先順位の決定と計画的な実行～定期的な見直し」、という一連の流れが重要であることを理解しました。具体的なセキュリティ対策の検討については、フレームワークを活用して進めています。

STEP 2　セキュリティ対策の土台となるセキュリティ規程類を整備

作成途中となっていたセキュリティ規程の見直しに加え、情報資産管理台帳やリスク管理表、ネットワーク構成図の作成を進め、セキュリティ対策の具体的な方針を固めました。また、「個人情報の保護に関する法律についてのガイドライン」に記載されている措置が講じられていることを確認しました。

STEP 3　ウェブサイト開発におけるセキュリティ対策状況を確認

開業後には顧客と電子契約を締結するため、ウェブサイトの開発を委託している制作会社が実施しているセキュリティ対策状況について問合せを行い、SSL（Secure Sockets Layer）の導入や海外からのアクセス制限などの対策が講じられていることを確認しました。

STEP 4　従業員のリテラシー向上を目指した取組を決定

セキュリティ対策に関する社内の情報共有を行うため、新たに勉強会の場を設けることにしました。また、セキュリティ担当者は、セキュリティ対策のより深い知識を体系的に身につけるため、情報セキュリティマネジメント資格試験の受験に向けた勉強を開始しました。

リスクの可視化と各種セキュリティ対策を実行

本事業のセミナーにおいて、情報資産の洗い出しとリスク分析、各種セキュリティ対策の策定と定期的な見直しという一連のサイクルを把握できたことにより、検討するべきことが明確になりました。具体的なセキュリティ対策の検討に関しては、フレームワークを活用して進めています。また、本事業の専門家からアドバイスを受け、情報資産管理台帳やリスク管理表、ネットワーク構成図の作成に加え、インシデント対応方法などを含めたセキュリティ規程の改訂を進めました。さらに、個人情報保護委員会が公開している「個人情報の保護に関する法律についてのガイドライン」に記載されている「講ずべき安全管理措置の内容」を参照し、現状の認識および措置が正しいことが確認できました。構築中のウェブサイトに関しては、制作会社にセキュリティ対策状況を確認することにより、セキュリティ面での安全性が担保できました。そのほか、ノートPCのディスク暗号化の確認、クラウドサービスにおける多要素認証および資産管理ソフトウェアの導入を検討しています。セキュリティ教育に関しては、最新の脅威に対する情報共有などを行うため、定期的に勉強会を開くことにしました。さらに、セキュリティ担当者が情報セキュリティマネジメントの資格取得を目指すことも決定しました。

04 結果と今後

セキュリティ対策の策定に有用なフレームワークを習得

セキュリティ対策のフレームワークについて理解を深めることができました。当初の懸念事項であった、「個人情報保護法」に則したさまざまな措置の妥当性を確認できたことは、事業を進める上での大きな安心材料となりました。今後は開業に向けて、セキュリティ対策をさらに強化するために、定期的な勉強会を行うほか、サービス事業者としてISMS認証の取得も目指していきたいと考えています。

経営層の声

インターネット上で契約を完結する業態であるため、ウェブサイトのセキュリティ対策が確認できたことは非常に有意義でした。セキュリティ担当者が本事業で習得した知識を全従業員で共有し、セキュリティ対策に関するリテラシーを全社的に高めていきたいと考えています。

参加者の声

これまでは独学で勉強しながらセキュリティ対策を講じてきましたが、本事業でフレームワークを習得するなど、ようやくスタートラインに立てたと感じています。本事業で習得した知識を活かし、情報セキュリティマネジメント資格の取得に向けた学習を進めていきます。

担当者の負荷を極力削減し、ベンダーとの連携強化によるセキュリティ対策を推進

取り組んだ支援テーマ：**ネットワークセキュリティ** / エンドポイントセキュリティ / モバイルデバイス / データ保護 / **セキュリティ意識と教育** / 外部パートナーとの関係

企業プロフィール

業種 / 従業員数：生活関連サービス業・娯楽業 / 6 ～ 20 名

セキュリティ体制：**1名体制**　**兼務**

事業内容

地域密着型で葬祭サービスを提供している企業です。事前のご相談からご葬儀の手配などをサポートする葬祭事業を中心に、葬儀ホールの運営や終活支援、地域イベント支援など、幅広い事業を通じて地域に寄り添うエンディングの総合サポート企業を目指しています。

01 背景と状況
セキュリティ対策はベンダー任せで状況が把握できていない

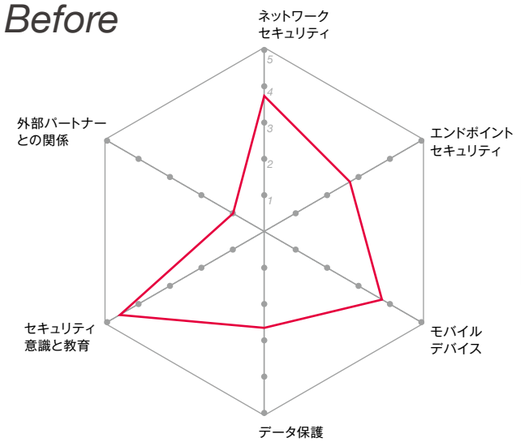
02 課題
担当者が多忙なため、セキュリティ対策が進まない

03 取組内容
課題への対応を行いながら、ベンダーとの連携を強化

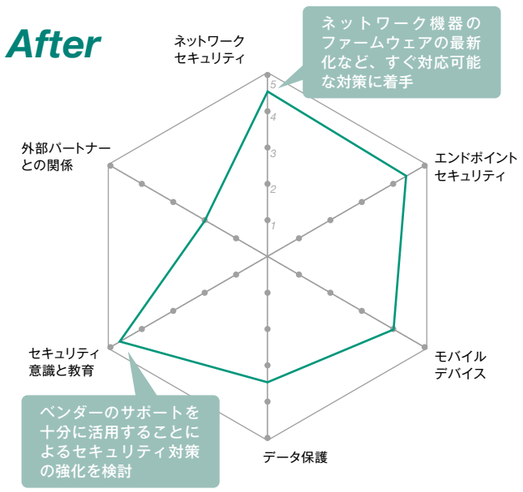
04 結果と今後
担当者の多忙を考慮したセキュリティ対策強化を推進

Before **After** 取組を通じたビフォーアフター

Before



After



01 背景と状況

セキュリティ対策はベンダー任せとなっており、現状が把握できていない

セキュリティ対策はベンダー依存 / UTMやウイルス対策は実施済み / SECURITY ACTION（二つ星）を宣言

セキュリティ対策はベンダーに任せており、セキュリティ担当者は、インシデントなどが発生した場合のベンダーとの連絡が主な対応業務となっていました。そのため、自身がセキュリティに関する知識を習得することに加えて、社内のセキュリティ意識向上を図りたいと考え、本事業への参加を決定しました。

02 セキュリティ課題

ベンダーとの役割分担や責任範囲が明確化されていない

当初の課題
- セキュリティ対策はベンダーに依存している
- セキュリティ規程を更新していない
- セキュリティ教育は必要な対策の周知のみ実施

専門家派遣支援で明らかになった課題
- ベンダーとの役割分担が明確化されていない
- アカウント管理の運用方法がルール化されていない
- インシデント発生時の対応が明文化されていない

03 取組内容

STEP 1　本事業の専門家派遣におけるセキュリティ対策状況の整理と課題の洗い出し

本事業の専門家において、「UTMのログ取得状況や保存期間、ファームウェアのアップデート状況、ウイルス対策ソフトウェアの定期更新やスキャン設定などが把握できていない」、「パスワード設定ルールが定められていない」など、さまざまな課題が洗い出されました。

STEP 2　ベンダーとの役割分担を明確化し、セキュリティ対策の強化を促進

本事業の専門家からアドバイスを受け、ベンダーとの役割分担や責任範囲の明確化を進めることに加え、セキュリティ対策強化に向けたベンダーとの協議を通じて関係性を深め、連携強化を図っていくことにしました。ベンダーとの協議には経営層も同席し、具体的なセキュリティ対策強化の検討を行いました。

STEP 3　UTMやウイルス対策の最新化に加え、新たにセキュリティ対策ツールを導入

導入当時から更新していなかったUTMやウイルス対策ソフトウェアを新たな製品へ入れ替えました。さらに資産管理ツールやデータ暗号化ソフトウェアも新たに導入し、セキュリティ対策の強化を図ることにしました。

STEP 4　自社で保有しているウェブサイトの運用管理についても確認

自社で保有しているウェブサイトの運用管理についても、独立行政法人情報処理推進機構（IPA）の公開している「ウェブサイトのセキュリティ対策のチェックポイント20ヶ条」を参考にして、セキュリティ対策状況やベンダーの対応範囲などの確認を進めていくことにしました。

セキュリティ対策の取組を通じたベンダーとの連携強化

セキュリティ対策についてはベンダーに委託し、UTM（Unified Threat Management）やウイルス対策ソフトウェアも導入しており、基本的なセキュリティ対策は行っています。本事業の専門家派遣において、セキュリティ対策状況の整理と課題の洗い出しを行った結果、「UTMのログ取得状況やファームウェアのアップデート」、「ウイルス対策ソフトウェアの更新設定」などの情報を把握できていないといった指摘を受け、セキュリティに関するリスクを認識しました。セキュリティ担当者は社内業務の変更に伴い非常に多忙であるため、本事業の専門家から、ベンダーとの役割分担や責任範囲を確認することに加え、ベンダーとの協議を重ねる中で関係性を深め、連携強化を図ることなどの提案を受けました。同社では自社に設置しているサーバ環境で顧客情報の管理を行っていますが、ベンダーと協議した結果、セキュリティ製品のリプレースを進めることで、セキュリティ対策の強化を図っていくことにしました。システムの全体像を把握するため、ネットワーク構成図の作成をベンダーに依頼したほか、導入時から更新していなかったUTMやウイルス対策ソフトウェアの入替を検討するとともに、資産管理ツールやデータの暗号化ソフトウェアの導入を進めています。

04 結果と今後

多忙な業務を考慮し、ベンダーとの協力体制を構築

他業務と兼任のセキュリティ担当者が非常に多忙であることを考慮し、セキュリティ対策はベンダーとの協力体制のもとで進めていくことを確認しました。今後は導入したセキュリティ製品の最新化やソフトウェアのアップデートについても、担当者が実施目的について把握し、役割分担や責任範囲を明確化した上でベンダーに依頼する形で進めていく方針です。

経営層の声

葬祭サービス企業としてお客様の個人情報を取り扱うため、セキュリティ対策への取組は喫緊の課題となっています。本事業への参加により、今後対応するべき対策や管理体制構築の方向性が明確化されました。今後もセキュリティ強化を着実に進めていきたいと考えています。

参加者の声

業務が多忙をきわめる中での参加となりましたが、本事業の専門家からのアドバイスや提示いただいた資料がセキュリティ対策を進める上で非常に参考になり、具体的なアクションにつながりました。本事業から得られた知見を活かし、今後も継続的に対策の強化を図っていきます。

従業員のITリテラシーとのバランスを考慮したセキュリティ対策の強化を推進

取り組んだ支援テーマ：ネットワークセキュリティ / エンドポイントセキュリティ / モバイルデバイス / データ保護 / セキュリティ意識と教育 / 外部パートナーとの関係

企業プロフィール
業種 / 従業員数：サービス業 / ～20名
セキュリティ体制：複数 / 兼務 / 経営者

事業内容
従業員の仕事力の把握を目的とした独自の適性検査サービスを展開しています。また、人材育成のための研修や組織・人事に関するコンサルティング事業も行っています。コンサルティング事業では、人材の個性に注目した人事戦略と組織づくりなど、総合的なサポートを行っています。

01 背景と状況
セキュリティ対策に漠然とした不安があり評価を受けたい

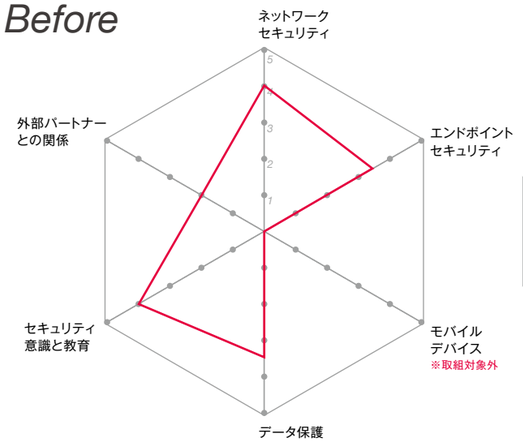
02 課題
自社の状況に合わせたセキュリティ対策の強化が必要

03 取組内容
優先度の高い課題に取り組みセキュリティ対策を強化

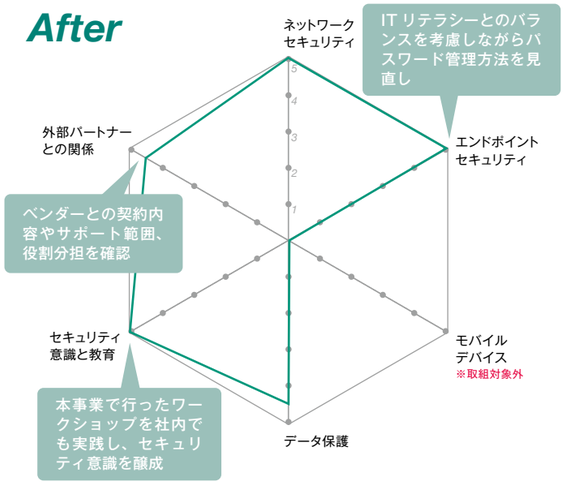
04 結果と今後
取り組んでいるセキュリティ課題に継続して注力する

Before **After** 取組を通じたビフォーアフター

Before



After



01 背景と状況

セキュリティ対策は実施してきたが現状の対策に漠然とした不安がある

- 他業務を兼務する担当者2名で管理
- ベンダーの提案や意見に頼りがち
- 従業員のリテラシーに個人差あり

セキュリティ担当は2名が兼務しています。必要なセキュリティ対策を実施してきたものの、ベンダーの提案をそのまま受け入れることが多く、現状のセキュリティ対策に不安がありました。また、従業員のITリテラシーには個人差があることから、組織内で実現可能なセキュリティ対策を講じたいと考えていました。

02 セキュリティ課題

セキュリティ対策を見直し実現可能な内容を検討する

当初の課題
- 現状のセキュリティ対策の第三者評価を得たい
- IT リテラシーに関わらず実施できる対策を検討
- インシデント対応の具体的なフローの手順化

専門家派遣支援で明らかになった課題
- ベンダーに依頼しているサポート範囲の明確化
- クラウドサービスの契約内容や役割分担の確認
- 情報資産の棚卸しの実施とデータの必要性の精査

03 取組内容

STEP 1 本事業の専門家とのヒアリングで課題を洗い出し、取り組む課題をピックアップ
本事業の専門家のヒアリングによって、現状のセキュリティ対策への評価と課題の洗い出しを行いました。洗い出された課題の中でも、「パスワード管理の見直し」、「インシデント対応フローの作成」、「ベンダーとの契約内容の精査」といった優先度の高い課題に取り組むことにしました。

STEP 2 個人差がある従業員のITリテラシーを考慮したセキュリティ対策を検討
従業員のITリテラシーに個人差があるため、パスワード管理の見直しに対しても、現場の運用を考慮した対応を検討する必要がありました。複雑なパスワードの設定を行うと、現場の運用に混乱が生じることが予想されたため、物理的なUSBキーによるパスワード認証の導入を検討しています。

STEP 3 社内でワークショップを行い、インシデント発生時の具体的な対応フローを作成
本事業のワークショップを参考に、社内でもワークショップを実施し従業員同士で議論しながら、インシデント発生時の具体的な手順を整理して、インシデント対応フローを作成しています。あわせて、情報資産の棚卸しも進めており、自社にとって本当に必要な情報資産かどうか見極めを行っています。

STEP 4 ベンダーとの契約内容やセキュリティ機器の機能・設定を確認
ベンダーのサポート範囲の確認のため、ベンダーとの契約内容およびセキュリティ機器の機能や設定を確認しました。本事業の専門家からベンダーへの確認事項のアドバイスを受け、具体的な確認を進めることができました。クラウドサービスについても、選定のための基準を作成しました。

ITリテラシーを考慮したセキュリティ対策の実行

本事業の専門家派遣で、現状のセキュリティ対策に関する課題をリスト化し、優先度の高い課題から取り組みました。例えば、パスワード管理では、従業員のITリテラシーに個人差があることから、複雑なパスワード設定では現場の運用が困難になるという課題がありました。そのため、本事業の専門家から物理的なUSBキーによるパスワード認証の提案を受け、導入に向けて検討しています。
インシデント対応フローの作成については、独立行政法人情報処理推進機構（IPA）の「情報セキュリティ10大脅威」などの資料を参考に、ランサムウェア感染の対策などの具体的な対応を検討しています。本事業のワークショップを参考に、社内でも同様のワークショップを行い、従業員同士で議論しながら、インシデント発生時に「誰が」「どのような対応を行うべきか」という具体的な手順を整理し、対策内容の文書化を進めています。さらに、各部門に依頼して情報資産の棚卸しを進めており、「保存するべき資産」と「処分するべき資産」の振り分けを行い、自社にとって本当に必要な情報資産を見極めています。ベンダーとの関係の見直しと強化のため、本事業の専門家から事前に確認事項のアドバイスを受け、現在の契約内容やセキュリティ機器の機能や設定に関する確認も行いました。

04 結果と今後

セキュリティ対策への不安を解消。引き続き課題に注力

洗い出されたさまざまな課題に対しては、まだ取組を開始した段階ですが、具体的な対応の方向性が明確となったため、以前から感じていた不安感は解消されました。令和6年度には、ネットワーク環境の更新を予定していますが、ベンダーに対して当社としてのセキュリティ要件や優先順位を伝えることで、必要なセキュリティ対策が実現可能な製品の導入を進めていく予定です。

経営層としての声
セキュリティに詳しい人材やコスト面で制約もありますが、当社の事業展開において、セキュリティ対策は必要不可欠な領域です。当社の環境を理解いただき、さまざまなご提案やご支援をいただけたことに感謝しております。

参加者としての声
セキュリティ対策に関する理解が深まるほど、事前予防や対策、リスクを低減するための検討の必要性に気づくことができました。知識の習得により、ベンダーとのコミュニケーションも可能となってきており、今後も根気強く会話を重ねながら対策を強化していきます。

ノートPCのパスワード管理体制を構築
端末を外部に持ち出す際の運用ルールを策定

取り組んだ支援テーマ：ネットワークセキュリティ / エンドポイントセキュリティ / モバイルデバイス / データ保護 / セキュリティ意識と教育 / 外部パートナーとの関係

企業プロフィール
業種 / 従業員数：卸売業・小売業 / ～20名
セキュリティ体制：1名体制 兼務

事業内容
機械工具関連の卸売を手掛ける企業です。自動車メーカーをはじめ、さまざまな分野の工場で使用される工具や資材を幅広く取り扱っています。取引先から依頼を受け、各種機械工具関連製品の見積もりから仕入れ、販売までワンストップで行っています。

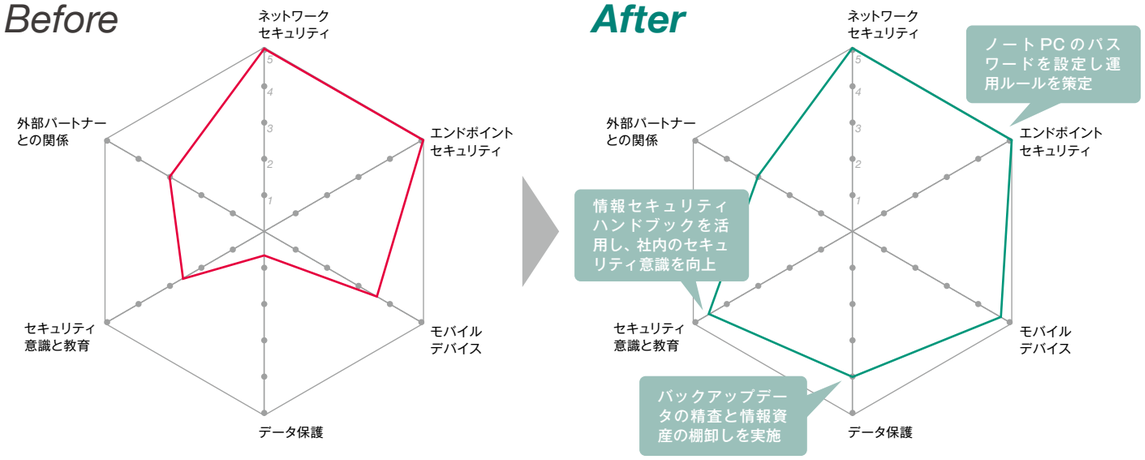
01 背景と状況
従業員のセキュリティリテラシー向上が必要

02 課題
PC使用時のパスワード管理が不十分

03 取組内容
PCにパスワードを設定し運用ルールを策定

04 結果と今後
ノートPCの安全な運用方法を確立

Before ***After*** 取組を通じたビフォーアフター



01 背景と状況

デスクトップPCから ノートPCへの入替を予定

セキュリティ担当者1名の管理体制
ノートPCの導入を予定
全社的なセキュリティ意識向上が必要

セキュリティ担当者1名が、ベンダーと連携しながら独学でセキュリティ対策を講じています。今後、リモートワークを含めたフレキシブルな働き方を実現するため、デスクトップPCからノートPCへの入替を行いました。従業員のセキュリティリテラシー向上のため、社内教育の必要性を感じています。

02 セキュリティ課題

ノートPCへの入替に伴い、運用ルールの策定が課題

当初の課題
- セキュリティ対策に関する客観的な評価ができない
- 従業員のセキュリティリテラシーに不安がある
- PC のパスワード管理が不十分

専門家派遣支援で明らかになった課題
- 業務データをバックアップする場所が不明確
- ノート PC の運用方法が定まっていない
- 情報資産の棚卸しができていない

03 取組内容

STEP 1 現状のセキュリティ対策の確認および課題の洗い出し
本事業の専門家派遣を通じて、現状のセキュリティ対策における課題を洗い出しました。ネットワークセキュリティおよびエンドポイントセキュリティに関しては、一定の水準を満たしていることが確認できた一方で、PCのパスワード管理方法の整備などの課題が明らかになったため、必要な対策を検討しました。

STEP 2 デスクトップPCからノートPCへの入替に伴い、運用ルールを策定
社内のデスクトップPCをノートPCへ入れ替えるタイミングで、一台ずつ個別に10桁以上のパスワードを設定しました。また、ファイルやデータはクラウドストレージに保存するなど、運用ルールを策定しました。さらに、セキュリティパッチやアンチウイルスソフトウェアのアップデートを行いました。

STEP 3 各種業務データの精査と情報資産の棚卸しを実施
各種業務データの内容を把握し分類･整理するとともに、バックアップの保存先を確認しました。また、IPAの提供するリスク分析シートを活用した情報資産の棚卸しを行い、重要度とリスクの洗い出しを実施しました。さらに、リスクを低減するため、クラウドストレージへのデータ移行を検討しています。

STEP 4 情報セキュリティハンドブックを活用し、社内教育を実施
従業員教育については、以前から朝礼や社内チャットを介してセキュリティ関連のインシデント事例や注意事項などを周知していましたが、さらなるセキュリティ意識向上のため、IPAの提供する情報セキュリティハンドブックを自社の業務内容に合わせて見直し、社内に展開しました。

PCのパスワード設定および運用ルールの策定を実施

本事業の専門家派遣において、現状のセキュリティ対策における課題を洗い出しました。ネットワークセキュリティおよびエンドポイントセキュリティに関しては一定水準を満たしているという評価を受けた一方で、PCのパスワード管理など改善すべき課題も明らかになったため、重要度の高い課題から対応する方針を固めました。PCにパスワードが設定されておらず、他従業員のPCを使用して代理で業務を行うこともあったため、デスクトップPCからノートPCへ入れ替えるタイミングで、一台ずつ個別に10桁以上のパスワードを設定しました。また、ノートPCを外部に持ち出す際のセキュリティリスクを低減するため、ファイルやデータはクラウドストレージに保存するなど、運用ルールを定めました。さらに、セキュリティパッチの更新やアンチウイルスソフトウェアのアップデートなども行いました。また、各種業務データの内容と保存先を分類・整理するとともに、独立行政法人情報処理推進機構（IPA）の提供するリスク分析シートを活用した情報資産の棚卸しを行い、重要度とリスクの洗い出しを実施しました。従業員教育については、IPAの提供する情報セキュリティハンドブックを自社の業務に合わせて見直し、社内に展開することで、セキュリティ意識向上を図りました。

04 結果と今後

フレームワークを活用して継続的な取組を推進

PCのパスワード設定に関する運用管理面を整備したほか、情報資産の棚卸しや従業員のセキュリティ意識向上など、さらなるセキュリティ対策の強化に取り組むことができました。今後は、重要データの保護のためのクラウドストレージへのデータ移行や、フレームワークを活用したセキュリティ対策の具体的な対応方法の検討などを行い、継続的な取組を推進していく予定です。

経営層の声
本事業を通して、セキュリティ対策の重要性をより深く理解することができました。今後は、全社的なセキュリティリテラシーの向上を図りつつ、現場での運用を考慮したセキュリティ管理体制を構築していきたいと考えています。

参加者の声
本事業のセミナーで実務的な知識を吸収し、ワークショップで実践的な取組を経験することにより、セキュリティ対策の全体像が把握できました。また、他社との交流を通じてセキュリティ対策の比較や情報交換ができ、非常に有意義な時間を過ごすことができました。

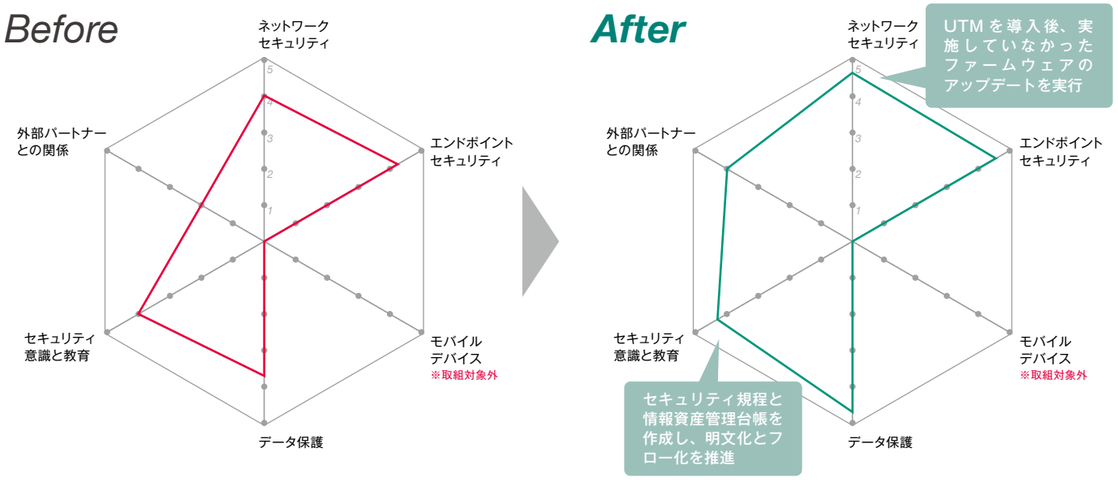
セキュリティ規程類の作成とルール化を行い、セキュリティ対策の見直しと刷新に着手

取り組んだ支援テーマ：ネットワークセキュリティ／エンドポイントセキュリティ／モバイルデバイス／データ保護／セキュリティ意識と教育／外部パートナーとの関係

企業プロフィール　業種 / 従業員数：学術研究・専門・技術サービス業 / ~20名　セキュリティ体制：複数　兼務

事業内容　公認会計事務所として、会計・税務申告などの税務・経理サービスを提供しています。加えて、継続的な財務管理を行うことにより、中長期的な視点での借入戦略を構築し、企業の成長をサポートしています。また、経営者や従業員を対象とした財務教育のセミナーを主催するなど、教育サービスも展開しています。

Before ***After*** 取組を通じたビフォーアフター



01 背景と状況

コロナ禍を機にセキュリティ管理体制の刷新が必要となったが知識が不足

- 他業務と兼務の担当者2名での管理
- 在宅勤務でセキュリティ強化が必要
- セキュリティ対策の知識が不足

セキュリティ担当は代表と管理部門の2名が兼務しています。セキュリティ対策は講じていますが、想定されるインシデントに応じた対策はできていません。コロナ禍を機に取引先との面談がオンラインになったことに加え、在宅勤務の導入により、セキュリティの強化が急務となったため本事業に参加しました。

02 セキュリティ課題

現状のセキュリティ対策の見直しと管理体制づくり

当初の課題
- セキュリティ規程の評価と修正
- セキュリティ機器の保守および運用体制の見直し
- セキュリティに関する教育体制の構築

専門家派遣支援で明らかになった課題
- ベンダーとの契約内容が曖昧で責任範囲が不明確
- ソフトウェアやサービスのセキュリティ体制の調査
- インシデント発生時の連絡体制が不明確

03 取組内容

STEP 1　リスト化した課題から緊急性の高い課題を優先的に着手

本事業の専門家派遣によるヒアリングを受け、自社のセキュリティに関する11件の課題を洗い出しリスト化しました。リスト化した課題に対し、本事業の専門家からのアドバイスを受けながらセキュリティ対策の要否を判断し、緊急性が高い課題を優先的に取り組むことにしました。

STEP 2　セミナー講師のアドバイスを受け、UTMとサーバのアップデートを実施

UTM（Unified Threat Management）のファームウェアのアップデートについては、機器の導入後から実施していなかったため、すぐに着手しました。本事業のセミナー講師にアップデートのタイミングについて質問したところ、的確なアドバイスを受けることができ、アップデート作業に安心して臨むことができました。

STEP 3　ガイドラインを参考にセキュリティ規程と情報資産管理台帳を作成

独立行政法人情報処理推進機構（IPA）の提供する「中小企業の情報セキュリティ対策ガイドライン」をベースにして、自社の業務に合わせて内容を見直すことにより、セキュリティ規程と情報資産管理台帳を作成することにしました。また、セキュリティ業務の文書化により、属人化の解消を進めています。

STEP 4　従業員のセキュリティ意識を向上するとともに、情報共有の機会が増加

「中小企業向けサイバーセキュリティ対策の極意」の冊子を貸出図書として共有するほか社内ポータルにも掲載し、従業員のセキュリティ意識向上を図っています。その結果、以前からインシデント発生時に活用していたセキュリティ管理専用チャットでは、ヒヤリハットの周知など情報の共有が増えました。

セキュリティ対策や管理体制を改善しセキュリティ意識を向上

本事業の専門家派遣を通じて、課題の洗い出しを行い、緊急性が高い課題を優先的に着手しました。セキュリティ機器のアップデートについては、導入後から実施しておらず、本事業の専門家より「早急に実施すべき」と指摘を受けたため、すぐにベンダーに相談しました。ベンダーによるサポートを受ける際には、本事業のセミナー講師から複数の対象機器のアップデートのタイミングなど具体的なアドバイスを受けることができ、非常に参考になりました。同時に、ソフトウェア会社やベンダーに対するセキュリティ管理体制の調査を実施していなかったため、ヒアリングを行うことで、契約内容や対応範囲を再確認することができました。また、社内のセキュリティ規程や各種文書類の見直しを実施した結果、不十分であることが判明したため、セキュリティ規程と情報資産管理台帳を改めて作成しており、令和6年3月に完了する予定です。セキュリティ教育については、本事業で提供を受けた「中小企業向けサイバーセキュリティ対策の極意」の冊子を社内で共有することにより、従業員のセキュリティ意識を高めています。また、セキュリティ意識が高まったことにより、ヒヤリハットやインシデント報告を行うためのセキュリティ管理専用チャットを介して、従業員間での情報交換の機会も増加しています。

04 結果と今後

セキュリティ対策の重要性を再認識。教育は継続検討

社内のセキュリティ対策について見直しをする良い機会となりました。本事業を通じて改めてセキュリティ対策の重要性を再認識するとともに、教育体制の強化に加えて従業員のセキュリティ意識も向上させなければならないという新たな決意が生まれました。今後は、取引先や従業員の増加を見込んでいるため、セキュリティ対策の強化に向けた予算化も前向きに検討していきます。

経営層の声

当社のような中小企業は、本格的なセキュリティ対策の検討や学習の機会がありません。本事業のセミナーやワークショップで勉強させていただき、実際に取り組める機会をいただき大変参考になりました。本事業については、継続的に取り組んでいただきたいと感じています。

参加者の声

数多くあるセキュリティ対策の課題から、至急取り組むべき課題なのか否かという優先順位づけができたことにより、やるべきことが明確になりました。さまざまな課題が残されていますが、セミナーやワークショップで学んだ知識を活かして引き続き取り組んでいきます。

電子機械器具卸売業 G 社

事業で習得した知見を活用し、社内のセキュリティ対策やベンダーへの対応力を強化

取り組んだ支援テーマ：ネットワークセキュリティ / **エンドポイントセキュリティ** / モバイルデバイス / **データ保護** / **セキュリティ意識と教育** / 外部パートナーとの関係

企業プロフィール

業種 / 従業員数：卸売業・小売業 / ～20名

セキュリティ体制：**複数** / **兼務**

事業内容

電子機器の製造受託を行うEMS事業、顧客の要望に基づいた設計・生産を行うODM事業を柱として、事業を展開しています。主な取扱製品は、金融機器、事務機器、交通インフラ機器、情報端末、医療関連機器、モビリティ機器などで、海外の自社工場で製造しています。東京本社のほか、海外に4拠点を持っています。

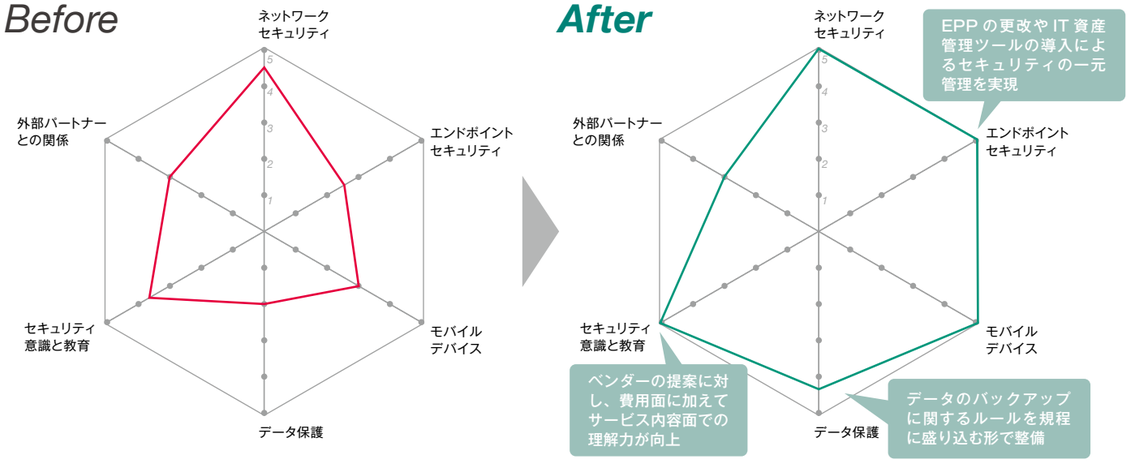
01 背景と状況
自社のセキュリティ状況を客観的に判断することが困難

02 課題
セキュリティ知識の向上と強化に向けた体制づくり

03 取組内容
エンドポイントセキュリティやデータ保護などの対策

04 結果と今後
必要な対策が明確化され担当者の取組意欲が向上

Before ***After*** 取組を通じたビフォーアフター



01 背景と状況

知識不足や体制未整備により自社のセキュリティ対策に関する客観的な判断が困難

- 管理部門の2名による管理体制
- 兼任のためセキュリティ知識が不足
- セキュリティ対策の体制整備

セキュリティ担当は管理部門の部長と課長の2名が兼務しています。セキュリティ知識の不足によりベンダーの提案をそのまま受け入れる場合が多く、またデータのバックアップを個人任せにするなど運用ルールも整っていませんでした。自社のセキュリティ状況を客観的に判断できる知識を身につけたいと考え本事業に参加しました。

02 セキュリティ課題

セキュリティ対策の体制づくりとシステムの導入

当初の課題

- セキュリティ状況を客観的に判断できる知識の習得
- 導入するセキュリティシステムなどの客観的評価
- 個人任せのデータバックアップ運用の整備

専門家派遣支援で明らかになった課題

- EPP の一元管理、持ち出し PC のデータ暗号化が未対応
- 社内 PC などのアップデート管理が行き届いていない
- データのバックアップに関するルールや方針が未整備

03 取組内容

STEP 1 セキュリティ課題の洗い出しとリスト化、対策時期を定めた目標設定

本事業の専門家派遣で行ったヒアリングをもとにセキュリティに関わる10課題を洗い出し、対策のリスト化を実施しました。さらに対策の実施時期を定め、優先順位を決めた上で対策に着手することにしました。

STEP 2 ネットワーク構成図の更新やデータ保護によって対応できる取組を優先的に着手

すぐに対応できる取組として、まずはネットワーク構成図の更新に着手しました。社内データ保護への対応については、社内PCに実装されたツールで暗号化の手順書を作成し、データ保護方法を明文化しました。その他にもデータの廃棄方法や保管場所に関する社内ルールの作成を進めました。

STEP 3 EPPの更改やIT資産管理ツールの導入など、予算化が必要な対策の実施

社内PCの一元管理を実現するため、コーポレートタイプのアンチウィルスへの更改やIT資産管理ツール導入に関わる費用の見積り予算化を進めています。重要データのバックアップ方法については、社内ルールや方針の策定を進めました。

STEP 4 本年度中の対応とした社内勉強会の実施とともに、今後も継続する対策の確認

社内セキュリティ意識向上のため、独立行政法人情報処理推進機構（IPA）が公開している企業向け教材を参考資料として配布し、社内勉強会を実施しました。その他のモバイルデバイス対策、パートナー企業や利用中のクラウドサービスの責任範囲に関する課題は来期以降の取組としました。

専門家派遣により設定された10課題に対する取組を推進

本事業の専門家派遣でヒアリングを実施し、エンドポイントセキュリティ・データ保護・セキュリティ意識を中心にセキュリティに関わる10課題を洗い出し、進め方を検討しました。まず、時間と費用をかけずに対応できる取組から優先的に着手し、次のステップとして、担当者が重要な取組と位置づけた「EPP（Endpoint Protection Platform）のコーポレートタイプへの更改」「IT資産管理ツールの導入」「データバックアップの社内ルール化」を進めることにしました。この中には費用のかかるものもあるため、内容と費用の精査を行い予算化を検討しています。同社の取引先には大手企業が多く、BCP（事業継続計画）の取組についてヒアリングを受けることがあるため、その対策強化にもつながると考えています。また、セミナー・ワークショップへの参加を通じてセキュリティに関する知識を習得し、パートナーであるベンダーへの対応力向上にも努めました。さらに、データバックアップのルール化を進めるにあたり、セキュリティ規程の整備を行うとともに、社内勉強会を実施しています。これらの取組により、社内のセキュリティ状況の把握ができたとともに、ITシステムやツールの導入、社内のセキュリティ意識向上など対策強化を図りました。

04 結果と今後

セキュリティ課題の明確化が具体的なアクションに

本事業によりセキュリティに関する課題が明確化され、具体的なアクションができました。自社の状況に合わせたソフトウェアやツールの導入の検討、データバックアップやセキュリティ対策に関する社内勉強会も実施するなど、目標の9割以上が達成できたと担当者は考えています。セキュリティ対策の強化は取引先の信頼度のアップにもつながる見込みで、今後も継続して取り組む予定です。

経営層の声

セキュリティ対策は当社の重要課題の一つと捉えており、東京都の支援でこのような事業に参加させていただき感謝しています。担当者から足りていなかったセキュリティ対策に関する提案を受け、事業の成果を実感しています。今後もセキュリティ対策を強化していきます。

参加者の声

これまでセキュリティ対策は、曖昧に進めていた部分がありましたが、やるべきことが明確になり、能動的にアクションを起こせるようになりました。セキュリティに対する意識が高まり、それを社内全体に広げていくことができたことも成果の一つであると感じています。

労務コンサルタント業 H社

機密情報を守るため、セキュリティ対策の運用管理を自社で行う体制へ

取り組んだ支援テーマ：ネットワークセキュリティ / エンドポイントセキュリティ / モバイルデバイス / データ保護 / セキュリティ意識と教育 / 外部パートナーとの関係

企業プロフィール

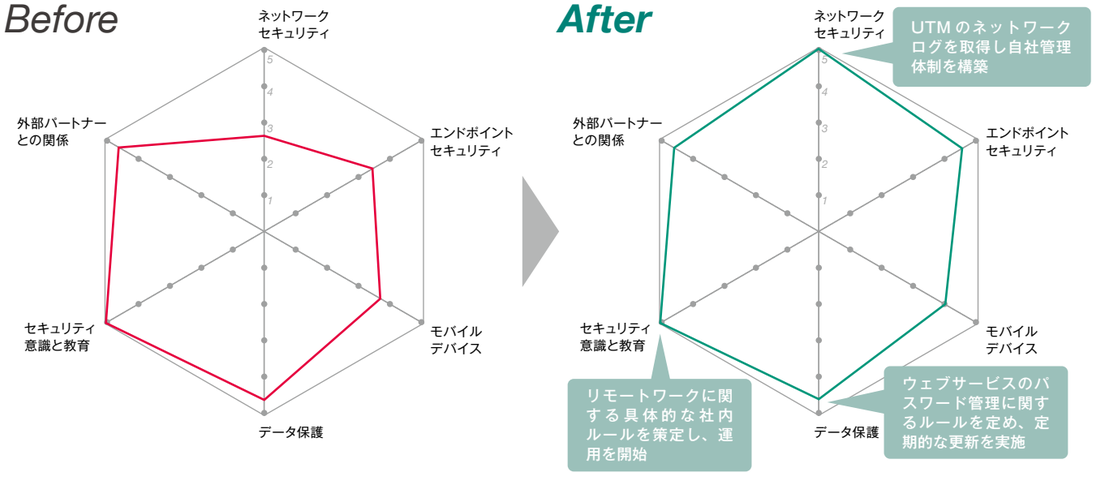
業種 / 従業員数：サービス業 / ～50名

セキュリティ体制：複数 / 兼務 / 経営者

事業内容

関連会社である社会保険労務士法人と連携し、人事労務コンサルティングサービスを提供する企業です。取引先の労務相談や給与計算、社会保険や雇用保険などの手続きに関するアウトソーシング業務を行うほか、各種手続きに必要なオンライン申請向けソフトウェアの開発・販売なども行っています。

Before ***After*** 取組を通じたビフォーアフター



01 背景と状況

関連会社の社会保険労務士法人と共同でセキュリティ対策を推進

- 関連法人と連携し2名による管理体制
- 関連法人はISMS認証取得済み
- セキュリティ教育を定期的に実施

セキュリティ対策に関しては、ISMS認証取得済みの関連法人と連携し、担当者2名により対応しています。ISMSに準じたセキュリティ規程の作成と更新に加え、セキュリティ教育も定期的に実施しています。身近な企業がランサムウェアの被害を受けたため、セキュリティ対策の強化を図りたいと考え本事業に参加しました。

02 セキュリティ課題

ネットワークセキュリティの管理体制の強化

当初の課題

- セキュリティ対策に関する従業員教育の不足
- セキュリティ管理体制の強化に向けた人材育成
- セキュリティ機器の管理・運用がベンダー任せ

専門家派遣支援で明らかになった課題

- ウェブサービスのセキュリティ対策の強化
- セキュリティ機器のログ情報取得と管理体制の構築
- 重要データのバックアップ運用の強化

03 取組内容

STEP 1　自社で提供しているウェブサービスに関するパスワード管理体制の確認

自社で提供しているオンライン申請サービスにおいては、機密性の高い情報を取り扱うため、パスワード管理に関するルールを策定する必要がありました。退職者などによる不正アクセス防止のため、社内で使用するパスワードの定期的な変更などのルールを明文化するとともに、定期的な更新を実施することにしました。

STEP 2　UTMのネットワークログの取得と管理体制の構築

東京都「令和3年度中小企業サイバーセキュリティ向上支援事業」に参加した際に設置したUTMに関して、アップデート状況を確認しました。また、本事業の専門家からのアドバイスにより、ネットワークログの取得および管理体制の構築を実施することにしました。

STEP 3　バックアップ頻度の見直しやクラウド活用によるバックアップ運用の強化を検討

取引先に関する重要なデータは、複数拠点に設置しているファイルサーバで世代管理されているものの、マルウェアに感染した場合には、複数拠点のファイルサーバが同時感染するリスクがあります。そのため、バックアップの頻度の見直しやクラウドサービスの活用などによるバックアップ運用の強化の検討を進めています。

STEP 4　リモートワークにおけるVPN利用に関するルールを策定し、運用を開始

従業員がリモートワークで業務に対応するため、社内LANへのVPN接続におけるリスクを可視化し、セキュリティ対策を検討しました。その結果、VPNアカウントの共有禁止など具体的な項目を盛り込んだルールを策定し、運用を開始しました。

ウェブサービスやUTMなどの自社管理体制の構築

取引先に関する機密性の高い情報を取り扱っているため、本事業の専門家派遣でセキュリティ対策が必要な課題をリスト化しました。その結果、自社で提供しているオンライン申請のウェブサービスやオンラインシステムに関するセキュリティ仕様の確認と、社内で使用しているパスワードの管理に関するルールの策定および運用改善に着手しました。また、以前導入したUTM（Unified Threat Management）のファームウェアのアップデート状況については、ベンダー側の定期更新により最新化されていることを確認しました。インシデント発生時にはベンダーから通知がくることを確認しましたが、自社でもネットワークログを取得し管理していく方針です。さらに、取引先に関する重要なデータについては、本社およびその他の拠点に設置しているファイルサーバで世代管理されているものの、マルウェアによる複数拠点の同時感染などを考慮したバックアップ運用の見直しが課題となっていました。そこで、クラウドサービスを活用したバックアップ運用などの検討を進めています。このほか、リモートワーク環境下で社内LANに接続するためのVPN（Virtual Private Network）のアカウント管理についてもルール化し、運用を開始しました。

04 結果と今後

知識の向上により取引先からの信頼につながる見込み

本事業のセミナーやワークショップに参加し、セキュリティに関する知識や他社の取組状況に関する情報を得たことにより、担当者のセキュリティ知識が向上しました。本事業の専門家によるアドバイスに基づいて取組を進めた結果、各対策の目的を理解することができました。今後も自社の業務に合わせたセキュリティ対策の検討や、取引先からの監査への対応に活用していきます。

経営層としての声

本事業のセミナーに代理出席した際には、内容が非常にわかりやすく、グループワークが中心のワークショップでは他社との会話が参考になりました。今後は推進するセキュリティ対策のレベルを検討する必要があるため、本事業で得た知識を活かしていきたいと考えています。

参加者としての声

セキュリティ対策を推進することにより、サイバー攻撃などのセキュリティリスクを下げることができることを改めて実感しています。身近な企業がランサムウェアの被害を受けたこともあり、限られた条件においても有効な対策を進めていきたいと考えています。

業務で使用するMac端末やネットワーク機器類の自社管理体制の構築を推進

取り組んだ支援テーマ：ネットワークセキュリティ / エンドポイントセキュリティ / モバイルデバイス / データ保護 / セキュリティ意識と教育 / 外部パートナーとの関係

企業プロフィール

業種 / 従業員数：学術研究・専門・技術サービス業 / ～50名

セキュリティ体制：複数 / 兼務

事業内容

業界を問わず商業デザイン全般のデザイン制作を請け負う企業です。経験豊富なデザイン職の従業員が数十名在籍しています。取り扱うデザインの領域は幅広く、紙媒体からデジタル案件までさまざまな事業を展開しています。

01 背景と状況
セキュリティ専門人材が不在で現在の対策に不安あり

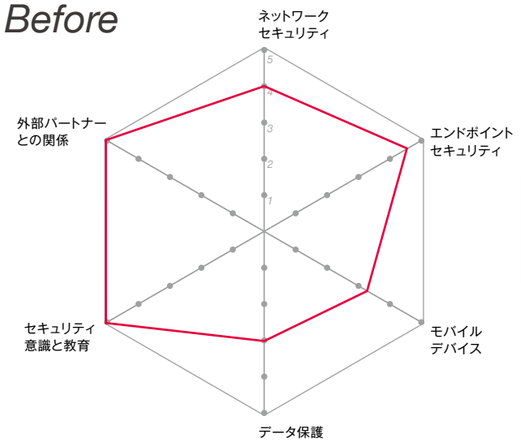
02 課題
Mac端末の運用管理方法の確立と機器類の知識習得

03 取組内容
Mac端末やUTMなどの自社管理体制の構築

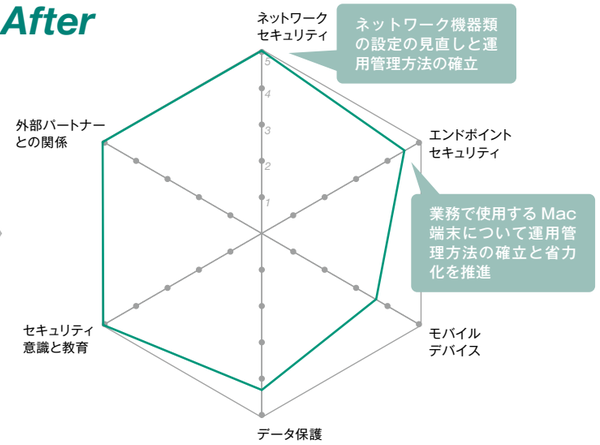
04 結果と今後
セキュリティ知識の習得と取り組むべき対策の明確化

Before ***After*** 取組を通じたビフォーアフター

Before



After



01 背景と状況

セキュリティの専門人材がいないため、現在の対策や管理体制に不安がある

- 担当者は2名が兼務する管理体制
- 業務に多数のMac端末を使用
- VPN機器の設定の見直しはベンダーに依存

セキュリティ担当は管理部門の2名が他業務と兼任しています。導入済みのネットワーク機器やファイルサーバの管理はベンダーに依存しているため、管理状況を把握できていません。業務で使用する多数のMac端末やネットワーク機器などの管理体制に不安があります。

02 セキュリティ課題

Mac端末やネットワーク機器類の自社管理の実現

当初の課題

- ネットワーク機器類の管理はベンダーに依存
- 社内に多数ある Mac 端末の管理工数が多い
- VPN 機器のアップデート管理状況が不明確

専門家派遣支援で明らかになった課題

- OS のバージョン確認など管理の省力化
- VPN 機器の設定状況の確認と見直し
- ネットワーク機器類の運用管理方法の確立

03 取組内容

STEP 1　本事業の専門家によるセキュリティ対策状況の確認と課題の整理

UTMやルータなどのネットワーク機器やEDR（Endpoint Detection and Response）製品のセキュリティ対策状況について、本事業の専門家によるヒアリングおよび評価を受けました。その上で、取り組むべき課題と優先順位を決定しました。

STEP 2　業務で使用するMac端末の運用管理方法の確立と省力化

社内に多数保有しているMac端末は、3か月に1回の頻度でOSやソフトウェアのバージョンなどを一台ずつ確認しており、管理に時間を要していました。本事業の専門家からアドバイスを受け、従業員からアンケートを回収し機器情報を収集することにより、運用管理方法の確立と省力化を実施しました。

STEP 3　VPN機器の新機種への入替に際し、セキュリティ設定についてベンダーに確認

VPN機器については、令和5年9月に新機種への入替を行い、必要なセキュリティ対策の設定と使用しているVPN接続方式をベンダーと確認することができました。VPN機器のファームアップについてはベンダーと協議し、その都度ベンダーと確認しながら手動で実施することを取り決めました。

STEP 4　ベンダーに依存していたUTMやルータのセキュリティ設定を自社で管理

UTMやルータなどのネットワーク機器の管理については、ベンダーに委託していました。本事業の専門家からアドバイスを受け、担当者自身が管理画面から情報を確認する方法を習得し、ネットワークログの確認・保存を自社で実施できるようになりました。

業務に使用するMac端末や各種機器類の運用管理を自社で実施

デザイン業務で使用するMac端末については、取引先の制作データに対応する必要があり、OSやソフトウェアのバージョンが複数存在するため、機器管理に手間がかかることが大きな課題でした。そこで、本事業の専門家からアドバイスを受け、3か月ごとに従業員からアンケートを回収し、OSのバージョンやアプリケーション情報を確認することにより、運用管理方法の確立と省力化を図りました。また、VPN（Virtual Private Network）機器の設定については、導入時からベンダーに依存していたため不安を抱えていましたが、令和5年9月に新機種への入替を行い、必要なセキュリティ対策が設定されていることの確認と、今後のアップデートの管理方法の取り決めを実施しました。あわせて、UTM（Unified Threat Management）などのネットワーク機器の管理について、本事業の専門家から管理画面によるログの確認と保存に関するアドバイスを受け、自社での管理体制の整備を進めることにしました。本事業のセミナーやワークショップでは、セキュリティに関する体系的な知識の習得に加えて、フレームワークを活用したセキュリティ規程やインシデント対応ルールなど規程類の整備に関する実用化に向けた知見も得ることができました。

04 結果と今後

技術的な対策の知見を獲得、今後取り組むべき対策を明確化

本事業への参加により、Mac端末の運用管理やネットワークセキュリティなどの技術的な対策面での知見を獲得し、具体的な手順に基づいた対策を進めることができました。今回の取組によって、セキュリティ対策全般に関する理解を深めたことに加え、対策するべき課題と対応の優先順位を可視化することによって、今後の対策の方向性が明確化されたことは、大きな成果の一つです。

経営層の声

本事業への参加により、当社のセキュリティレベルの現状と課題を把握し、解決に向けたアドバイスを受けることができました。これまでも技術的な対策を中心に積極的に取り組んできましたが、現状に甘んじることなく今後も取組を継続させていきたいと考えています。

参加者の声

これまでは、自社のセキュリティ対策の現状が評価できずに大きな不安を感じていました。本事業への参加を通じて、自社で取り組むべき課題の明確化と必要なセキュリティ対策の実施により、想定以上の成果を得ることができ、非常に感謝しています。

社内の情報資産の整理と継続的な管理方法を確立、セキュリティ教育の強化を推進

取り組んだ支援テーマ：ネットワークセキュリティ / エンドポイントセキュリティ / モバイルデバイス / データ保護 / セキュリティ意識と教育 / 外部パートナーとの関係

企業プロフィール
- 業種 / 従業員数：情報通信業 / ～50名
- セキュリティ体制：複数 / 兼務
- 事業内容：流通小売業に特化したクラウド型の基幹システムを開発、提供するITソリューション企業です。

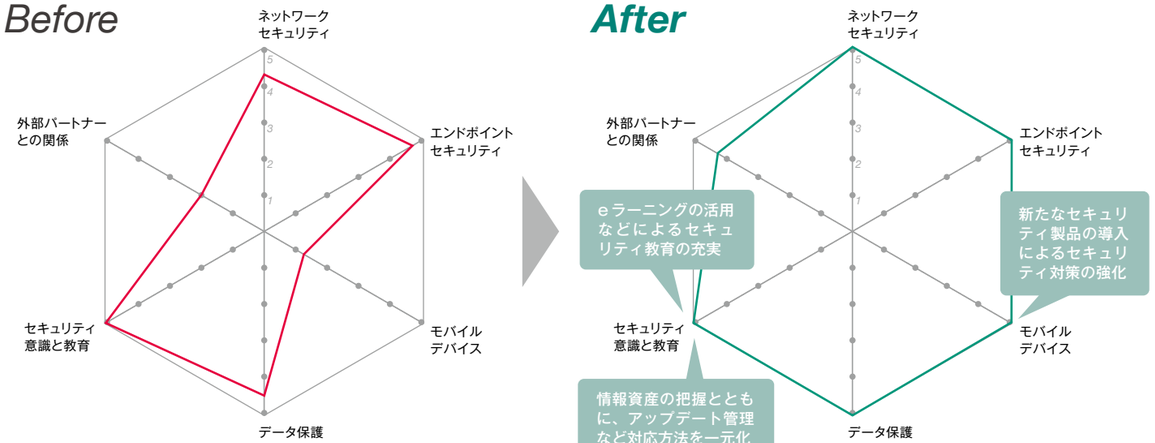
01 背景と状況
ISO認証を取得済みだが、セキュリティ対策に不安

02 課題
情報資産の把握と管理、セキュリティ教育の強化

03 取組内容
情報資産管理やクラウドサービスのセキュリティ対策を検討

04 結果と今後
情報資産の管理方法やセキュリティ教育を強化

Before After 取組を通じたビフォーアフター



01 背景と状況

セキュリティ対策には注力しているが、時代に合った対策となっているか不明

- セキュリティ委員会による管理体制
- ISO/IEC27001 認証を取得済み
- 自社の環境に合った対策か不安あり

情報セキュリティ委員会9名による管理体制です。ISO/IEC27001認証を取得しているほか、各部門長が参加する情報セキュリティ委員会を月1回開催するなど、セキュリティ対策には注力しています。しかし、認証取得から時間が経過しており、現在の環境に合った対策となっているのか不安を感じています。

02 セキュリティ課題

情報資産の把握と管理方法の見直し･社内教育の強化

当初の課題
- セキュリティ業務の属人化が進んでいる
- 情報資産の管理方法の確立が必要
- 社内のセキュリティ教育体制の強化

専門家派遣支援で明らかになった課題
- OS やセキュリティパッチのアップデート運用見直し
- クラウドサービスのセキュリティ対策の確認
- リモートワーク環境の評価と見直し

03 取組内容

STEP 1　セキュリティ対策が必要な課題を洗い出し、優先順位を決定

本事業の専門家派遣により、セキュリティ対策が必要な課題の洗い出しを行いました。その結果、セキュリティに関わる20課題が明確化されました。対策に必要な時間やコストを考慮した上で優先順位をつけ、「情報資産の把握と管理方法の確立」を最優先課題として着手することにしました。

STEP 2　情報資産の具体的な管理方法を確立して社内ルール化

資産管理ツールの活用により、OSやセキュリティパッチのアップデートを一元管理することに加え、ライセンス管理表も作成し、資産管理の運用について社内ルール化しました。また、スマートフォンの管理のため、MDM（Mobile Device Management）を導入しました。

STEP 3　クラウドサービスのセキュリティ対策状況を確認

同社製品であるクラウド型基幹システムのセキュリティ対策について理解を深めるため、本事業の専門家からセキュリティチェックの観点について説明を受けました。また、未導入だったWAFの製品選定に関するアドバイスを受け、導入を検討することにしました。

STEP 4　eラーニングの活用などによる社内セキュリティ教育の充実

前年度から取り組んでいる年1回のセキュリティ教育については、さらなる内容の充実を図るため、本事業の専門家からeラーニングの活用や標的型訓練メールの実施などの提案を受け、eラーニングの導入から推進することにしました。

情報資産管理やクラウドサービスのセキュリティ対策を強化

本事業の専門家派遣によりセキュリティに関する20の課題を洗い出し、セキュリティ担当者が重視していた「情報資産の把握と管理方法の確立」を最優先課題として着手することにしました。資産管理ツールを活用した社内PCのOSやセキュリティパッチのアップデートの一元管理に加えて、ライセンスの管理表の作成により、正確かつ効率的な情報資産の棚卸し方法の構築を目指すことにしました。あわせて、同社が顧客に提供しているクラウド型基幹システムに利用している、クラウドサービスのセキュリティ対策状況の確認を行いました。本事業の専門家からセキュリティチェックの観点について説明を受けたほか、Webアプリケーションの脆弱性を突いた攻撃に対するセキュリティ対策の一つであるWAF（Web Application Firewall）製品の導入についてアドバイスを受けました。社内のセキュリティ教育については、独立行政法人情報処理推進機構（IPA）が毎年公開している「情報セキュリティ10大脅威」をもとに実施していますが、さらなる充実を図るため、本事業の専門家からeラーニングの活用や標的型訓練メールの実施などの具体的なアドバイスを受け、eラーニングの導入の検討を前向きに進めることにしました。

04 結果と今後

情報資産の管理方法や社内セキュリティ教育を強化

本事業の専門家からアドバイスを受け、情報資産のアップデート管理方法に対するルール化を進め、セキュリティ規程の見直しも実施しました。新たにMDMの導入も決定し、管理体制強化に向けて前進することができました。さらに、社内セキュリティ教育については、本事業の専門家からのアドバイスをもとに、研修内容を経営層、システム管理者、一般従業員に分けて実施していく方針です。

経営層の声

外部監査でセキュリティ対策内容の指摘を受けた後も、改善できずにいました。担当者より本事業で学んだ知識を切り口とした継続的な教育体制が構築できたことは、大きな成果となりました。セキュリティに対する脅威の形態に合わせた取組が大切であると再認識しました。

参加者の声

セキュリティ対策に割けるリソースが限られており、業務が属人化していましたが、本事業の専門家から客観的な評価とセキュリティ対策に関するアドバイスを受けられたことは大きな成果だと感じています。自社の弱みを俯瞰でき、非常に有意義な事業であると感じました。

セキュリティ規程やインシデント対応フローの明文化でセキュリティ業務の属人化を解消

取り組んだ支援テーマ：**ネットワークセキュリティ** / エンドポイントセキュリティ / モバイルデバイス / データ保護 / **セキュリティ意識と教育** / 外部パートナーとの関係

企業プロフィール

業種 / 従業員数：学術研究・専門・技術サービス業 / ～50名
セキュリティ体制：**複数** / **兼務**

事業内容

設計段階の製品・構造物に対して生じる物理現象をコンピュータ上で解析するCAEを通じた設計支援やその受託解析を展開する企業です。官公庁や研究開発部門から高度な解析業務も請け負っています。また、エンジニアリングやジョブ管理など業務システムのインフラ構築・保守・運用なども行っています。

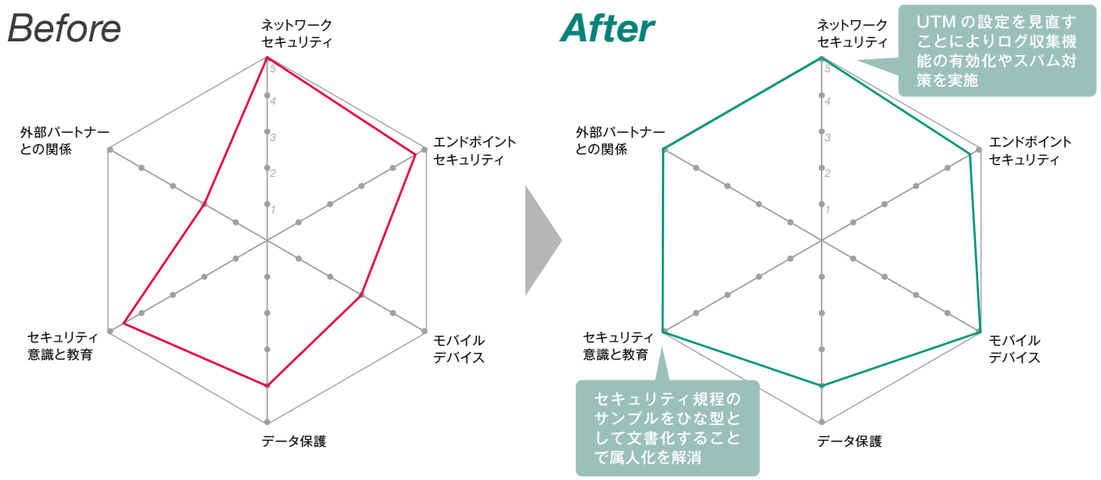
01 背景と状況
セキュリティ対策の属人化解消と知識向上

02 課題
セキュリティ規程とインシデント対応ルールの作成

03 取組内容
セキュリティ規程を作成し社内共有およびフロー化

04 結果と今後
ISMS認証取得に向けてセキュリティ対策を継続

Before ***After*** 取組を通じたビフォーアフター



01 背景と状況

ISMS認証取得に向けてセキュリティ環境の改善と知識の取得が必要

- セキュリティ対策への意識は高い
- ISMS認証取得を目標にしている
- セキュリティ知識習得とスキル向上が必要

ネットワーク機器やセキュリティ関連ソフトウェアのアップデートなど、セキュリティ対策には留意している一方で、セキュリティ業務の属人化が課題でした。将来的にISMS認証取得を目指しているため、さらなるセキュリティ強化に向けたスキル向上や知識の習得を図りたいと考え、本事業に参加しました。

02 セキュリティ課題

セキュリティ規程の明文化と対策の見直しが不可欠

当初の課題

- 実施しているセキュリティ対策の評価・見直しが不足
- 社内セキュリティ規程が明文化されていない
- UTMの機能が十分に活用できていない

専門家派遣支援で明らかになった課題

- インシデントやヒヤリハットの収集・周知フロー確立
- セキュリティ製品の取り扱いや運用についての文書化
- 従業員に対するセキュリティ理解度の定期的な確認

03 取組内容

STEP 1 セキュリティ課題のリスト化を行い、より注力すべき課題を選択

本事業の専門家によるヒアリングを行い、12点のセキュリティ課題のリスト化を行いました。その中でも「セキュリティ対策の評価･見直し」や「セキュリティ規程の作成」につながっていく課題を優先的に取り組むことにしました。

STEP 2 セキュリティ規程のサンプルを参考にして自社の現場レベルまで落とし込み

セキュリティ規程を作成するにあたり、本事業の専門家から提供を受けたIPAが公開しているセキュリティ規程のサンプルを参考にしました。規程に盛り込むべきところを明確化し、セキュリティ製品の管理画面へのログイン方法や取り扱い方法について、文書化を行いました。

STEP 3 ISMS認証取得を意識しながら、必要な対応方針の検討を実施

将来的なISMS認証取得を意識しながら、セキュリティ規程や対策の修正作業を進めています。ISMS認証取得に向けては、他にも必要な検討項目があることもわかり、情報資産管理台帳の作成やリスクの洗い出しと分類を行いながら、現場レベルで必要なリスク対策の検討を行っています。

STEP 4 チェックシートを用いて、ルールや対応フローの理解度を確認

社内のセキュリティリテラシーを高めるために定期的に行っている勉強会のあとに、チェックシートを用いて従業員の理解度と定着度の確認をすることにしました。また、セキュリティに関する年間スケジュールを作成し、ISMS認証の取得スケジュールやリソースの検討も行っていく予定です。

セキュリティ意識の向上と社内教育の強化を推進

本事業の専門家ヒアリングを通じて12点の課題が挙がりました。その中から目標としている「ISMS認証取得」につながる課題に絞り込み、対策を策定しました。具体的には、独立行政法人情報処理推進機構（IPA）が公開しているセキュリティ規程のサンプルを参考に必要な情報を集約し、現場レベルでのルールや管理体制を整理しました。セキュリティ製品の取り扱いや運用方法を文書化することにより、業務の属人化を回避することが目的です。また、何らかのトラブルが発生した際に作業内容の振り返りも行えるようになりました。同時に、セキュリティ規程の修正や従業員への教育などを定期的な活動とするために、年間を通したセキュリティ対策のスケジュールを作成中です。その他、定期的に行っている勉強会後に、チェックシートを用いて理解度と定着度を確認することにより、社内に残存しているセキュリティリスクをチェックできるようにしています。課題であったインシデント対応に関しては、オープンソースの管理ツールを用いて管理しています。インシデントやヒヤリハットの収集や周知に関しては、各従業員が書き込むようにすることにより、過去の対応を検索し、履歴を確認できるようになりました。

04 結果と今後

セキュリティ状況を把握し明文化とフロー化を実施

本事業の取組により、改めて社内のセキュリティ状況を把握し、セキュリティ規程の明文化およびフロー化を実施することができました。目標としていた「ISMS認証取得」に必要なセキュリティ対策の基礎的な部分は取り組むことができたと考えています。また、本事業を機に、新たに2名の従業員がセキュリティ担当に着任することが決まり、継続してセキュリティ対策の強化に取り組みます。

経営層の声

本事業でセキュリティ業務の明文化およびフロー化を実施したことで、社内の他の業務でも同様の標準化を進めることができました。その点を高く評価しています。また、以前導入した機器に関しても、本事業の専門家から活用方法を的確に明示いただいたことも感謝しています。

参加者の声

セミナー・ワークショップで最新の技術や知識を習得し、他社と意見交換できたことは刺激になりました。また、既存のセキュリティ製品を応用することにより、予算を抑えつつ不足部分をカバーできる方法など実践的な内容を学習できたことも本事業の成果だと感じています。

ネットワークセキュリティ強化のための機器導入とランサムウェア感染時の対応の手順化

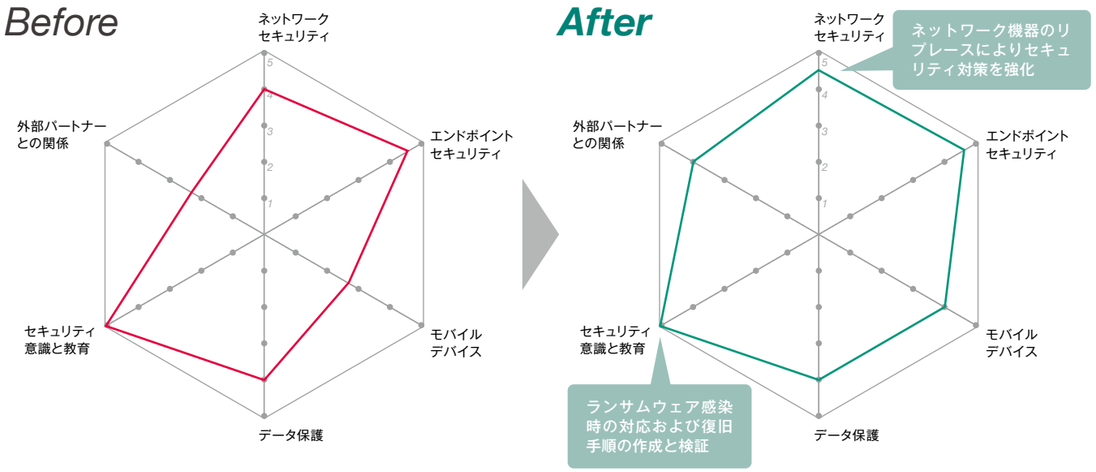
取り組んだ支援テーマ：**ネットワークセキュリティ** / エンドポイントセキュリティ / モバイルデバイス / データ保護 / **セキュリティ意識と教育** / 外部パートナーとの関係

企業プロフィール　業種 / 従業員数：情報通信業 / ～50名　セキュリティ体制：**複数** / **兼務**

事業内容　インターネットに関連する包括的なサービスをワンストップで提供しています。ウェブアプリケーションの設計・開発、ウェブサイトのデザインから、ネットワークの設計やサーバ構築・運用・保守に至るまで、インターネットに関わるあらゆる要望に対応できる体制を整えています。

01 背景と状況　現状のセキュリティ対策を見直して改善したい
02 課題　セキュリティ対策の実施状況と実施すべき対応の把握
03 取組内容　セキュリティ対策強化とインシデント対応の文書化
04 結果と今後　対象をインシデント全般に広げて文書化を進める

Before **After** 取組を通じたビフォーアフター



01 背景と状況

ISMS認証を取得しているものの、社内のセキュリティ対策に不安がある

- セキュリティ対策に不安がある
- 第三者による評価を受けたい
- 担当者のスキルアップを図りたい

ISMS認証を取得しており基本的なセキュリティ対応は行っていますが、社内のセキュリティ対策への不安がありました。本事業の専門家から現状の評価を受けることに加え、担当者がセキュリティ知識を習得し、部門内に共有することで部門全体としてレベルアップを図りたいと考え、本事業に参加しました。

02 セキュリティ課題

セキュリティ対策の実施状況確認と未実施項目の改善

当初の課題
- サポートが終了したネットワーク機器がある
- ランサムウェア感染時の対応が不明確
- 取り組むべき課題の優先順位をつけることができない

専門家派遣支援で明らかになった課題
- ネットワーク機器のログが取得できていない
- アカウントの一元管理ができていない
- EDR の導入につき専門家の意見を聞きたい

03 取組内容

STEP 1　本事業の専門家と課題を洗い出し、事業に対する影響度で取り組む課題を決定

本事業の専門家のヒアリングにより、現状のセキュリティ対策を評価し、課題をリスト化しました。洗い出された課題の中で自社の事業に対する影響度に基づき優先順位づけを行い、「ネットワーク機器のリプレース」「ランサムウェア感染時の対応手順の作成」について優先的に対応することにしました。

STEP 2　ランサムウェア感染時の対応手順を整理して文書化を進める

まず、「ランサムウェア感染時の対応手順の作成」に着手し、事前準備、一次対応･復旧の手順、復旧後の対応など一連の対応フローを文書化しました。今回はランサムウェアに関するインシデント対応の手順書を整備していますが、今後、さまざまなインシデントに対応するための手順書を作成する予定です。

STEP 3　VPN機器やEDRを購入するための助成金の申請準備を進める

ネットワーク機器のリプレースについては、サポートが終了したVPN機器の購入許可を社内で得ることができたため、助成金の申請準備を進めています。また、導入を検討していたEDRについても、あわせて助成金の申請が行えるよう、社内の調整を進めています。

STEP 4　セキュリティ対策について社内全体でのチェック体制を整備

サポートが終了している機器類の棚卸し作業やランサムウェア感染時の対応手順について、社内のISMS委員会と連携することにより、ISMS認証の更新における手順に組み込むことを検討しています。セキュリティ担当のみにとどまらず、社内全体へ浸透させるような仕組みを構築しました。

セキュリティ対策強化とインシデント対応手順の作成

本事業の専門家によるヒアリングで現状を確認し、セキュリティ対策の課題を洗い出しました。その後、自社の事業に対する影響度を考慮して優先順位をつけました。その中でも、業務停止やクライアントからの信用を失う可能性があることから、「ランサムウェア感染時の対応手順の作成」を重要度の高い課題として優先的に取り組むことにしました。事前準備、一次対応・復旧の手順、復旧後の対応などに関する文書化を行っています。さらに、さまざまなインシデントにも対応できるよう、その他の手順書も作成する予定です。また、担当者のアサインや対策委員をどう編成するのかという点についても社内調整を進めています。サポートが終了したVPN（Virtual Private Network）機器については、機器購入の許可が下りたため、助成金の申請準備を進めています。本事業の専門家から客観的な指摘を受けたことで、社内の上申をスムーズに進めることができました。同じく導入を検討していたEDR（Endpoint Detection and Response）についても、費用面での懸念がありましたが、あわせて助成金を活用するために社内の調整を進めています。

04 結果と今後

インシデント全般への対応についても文書化を進める

セキュリティ対策の課題に取り組むことで、社内の調整や情報共有を図り、社内全体のセキュリティに対する意識が向上しました。今後は、引き続きランサムウェア感染時の対応手順書の作成を推進しながら、他のインシデント対応についても手順化を進めていきます。また、セキュリティ機器の入替については、助成金の申請準備を行っており、来年度中の導入に向けた社内調整を進めていきます。

経営層の声

本事業の専門家による調査を受け、自社の脆弱性について新たな課題が見つかりました。また、セキュリティ担当の意識向上の機会を得ることができ、非常に感謝しています。今後は、一過性ではない継続的なセキュリティ対策強化へつなげていきたいと考えています。

参加者の声

本事業の専門家に質問しながら、一緒にセキュリティ対策の課題に取り組むことができたため安心感がありました。また、ワークショップでは他企業のセキュリティ担当との意見交換を通じて、他社の取組やセキュリティ対策について知ることができ、大変勉強になりました。

実効性のあるセキュリティ対策を実現するため、運用管理の強化を図る取組を推進

取り組んだ支援テーマ：**ネットワークセキュリティ** / エンドポイントセキュリティ / モバイルデバイス / データ保護 / **セキュリティ意識と教育** / 外部パートナーとの関係

企業プロフィール　業種 / 従業員数：情報通信業 / ～ 100 名　セキュリティ体制：**複数** / **兼務**

事業内容　高度な精密機械の輸送、運搬サービスを展開している企業です。取引先から請け負った輸送業務に加え、特殊な環境下での精密機械の設置業務を行っています。また、対象製品の輸送に関わるシステムの開発も手掛けるなど、先端技術に関わる領域で事業を展開しています。

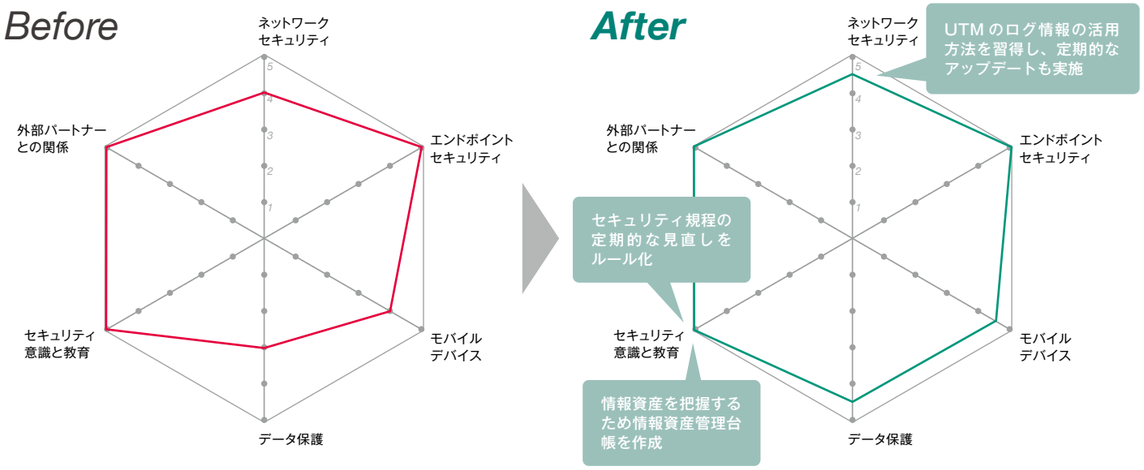
01 背景と状況　セキュリティ対策を積極的に推進

02 課題　セキュリティ対策の運用ルールや管理が不十分

03 取組内容　対策やルールの運用開始と情報資産管理台帳の作成

04 結果と今後　セキュリティ実装計画をもとに対策を推進

Before **After** 取組を通じたビフォーアフター



01 背景と状況

各種セキュリティ製品の導入やセキュリティ規程の整備を積極的に推進

経営層はセキュリティ対策に協力的 / 各種セキュリティ製品は導入済み / 担当者は経験が浅く、知識が不足

経営層はセキュリティ対策やコストについての理解があり、各種セキュリティ製品などの整備を進めています。セキュリティ担当者は、情報システム部門の責任者を含め複数名いますが、令和5年4月に着任した担当者1名が実作業を行う管理体制です。担当者は日頃からセキュリティ対策の情報収集を行っています。

02 セキュリティ課題

導入済みのセキュリティ製品など各種対策の運用

当初の課題
- 担当者のセキュリティ知識やスキルの向上
- 不足している対策の把握および評価

専門家派遣支援で明らかになった課題
- ネットワークログに関する情報の把握
- ネットワーク機器に関するアップデートの定期運用
- 情報資産管理台帳の作成

03 取組内容

STEP 1　UTMから取得するネットワークログに関する情報収集や管理を優先的に着手

本事業の専門家より「UTMから取得するネットワークログの情報把握」と「ネットワーク機器の運用管理」について指摘を受けました。そのため、UTMから取得できるログの種類や管理方法に関する知識を習得するとともに、ベンダーと相談しながらログを活用した運用管理の明確化を進めました。

STEP 2　セキュリティ規程の定期的な見直しをルール化

セキュリティ規程について、新たな規程を盛り込む際のルールや定期的な見直しタイミングが定められていなかったため、四半期に1回の頻度で見直す方針を決定し、運用面での対策を強化しました。

STEP 3　社内の情報資産の把握・管理を目的に、情報資産管理台帳の整備に着手

本事業のセミナー・ワークショップを通じて得た知識を活かして、情報資産の洗い出しやリスク分析を開始し、情報資産管理台帳の整備に着手しました。ワークショップで他社のセキュリティリスクに対する具体的な対策や考え方などを聞くこともできたため、非常に参考になりました。

STEP 4　中長期で取り組むセキュリティ課題を可視化する「セキュリティ実装計画」を作成

本事業により優先的に取り組むことになったセキュリティ課題の対応を進めるとともに、新たに顕在化した課題や中長期で取り組む必要がある課題については、本事業のセミナーの中で紹介されたフレームワークを参考に、「セキュリティ実装計画」として可視化し、今後の取組方針を明確化しました。

セキュリティ製品や規程類の運用と情報資産の可視化

本事業の専門家によるヒアリングの結果、UTM（Unified Threat Management）などのセキュリティ対策は一通りできているという評価を受けました。一方、ログを活用した運用管理については、「UTMから取得するネットワークログに関する情報を把握できていない」、「ネットワーク機器のアップデート管理が行われていない」などの課題が明確になったため、本事業の専門家からアドバイスを受け、優先的に着手することにしました。また、セキュリティ規程については、新たな規程を盛り込む際のルールや定期的な見直しタイミングが定められていなかったため、四半期に一度見直しを行うことをルール化し、運用面での対策を強化しました。情報資産管理台帳の作成については、本事業のセミナーやワークショップでの取組を活かして着手し始めましたが、他部門の協力を得ながら情報資産の洗い出しを進めていく必要があるため、まずは自部門の整理から進め、来年度以降も継続して作成していくことにしました。
さらに、「情報資産の整理」、「インシデント対応フローの作成」といった今回の取組で新たに顕在化した課題や、「ISMS認証取得」といった中長期で取り組むことが必要な課題に継続して対応するために、「セキュリティ実装計画」も作成しました。

04 結果と今後

今後はISMS認証取得も視野に計画を推進

本事業でのさまざまな取組により、「セキュリティ実装計画」を作成できたことは大きな成果となりました。
大手の取引先や官公庁からは高い基準でのセキュリティ対策を求められることも多く、セキュリティ製品やセキュリティ規程の実効性を高めるためにも、運用管理の徹底などの取組を強化していきます。将来的なISMS認証取得を視野に入れ、セキュリティ対策強化を継続していきます。

経営層の声

セキュリティ対策については、インシデントが起こらない状況こそが正常な状態であるため、ともすればセキュリティに対する意識が低くなりがちです。本事業終了後も取引先にとっての信頼材料となるように、セキュリティ対策の強化に取り組んでいきたいと考えています。

参加者の声

基本的なセキュリティ対策を整備した後の取組が不明確でしたが、具体的な対策が見えてきました。自分自身もセキュリティ対策について考える機会が増えてきており、今後は本事業を通じて得られた知見を組織全体に共有するため、継続して取り組んでいきます。

ベンダー依存型のセキュリティ対策から脱却
全従業員で取り組むセキュリティ管理体制を構築

取り組んだ支援テーマ：ネットワークセキュリティ / エンドポイントセキュリティ / モバイルデバイス / データ保護 / セキュリティ意識と教育 / 外部パートナーとの関係

企業プロフィール

業種 / 従業員数：人材サービス業 / ～100 名
セキュリティ体制：1名体制 兼務

事業内容

高度専門人材を活用し、企業のブランド向上や製品の販促といったBPO業務を担当する企業です。ショールームやオフィスといった常設施設、博覧会・イベントコンベンション・各種プロモーションなどが活動領域です。運営管理、人材育成・研修、コンサルティング業務を行っています。ニーズに沿ったキャスティングに強みがあります。

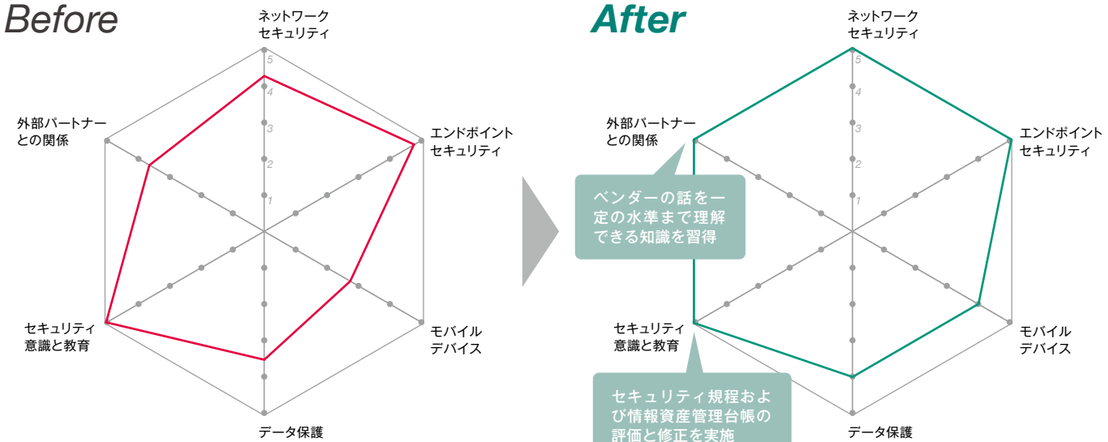
01 背景と状況
担当者にセキュリティに関する専門的な知識がない

02 課題
ベンダー任せの保守運用に不安あり

03 取組内容
課題を解決しつつセキュリティ対策の知識を習得

04 結果と今後
ベンダーの提案を理解し意見を述べることが可能に

Before After 取組を通じたビフォーアフター



01 背景と状況

セキュリティの専門知識がなく不安なままベンダー任せのセキュリティ対策を実行

- セキュリティの専門的な知識がない
- 保守運用はベンダーに一任
- セキュリティ規程の運用が不十分

ベンダーに保守運用を一任していますが、セキュリティ担当者にその内容を精査・検証する知見がなく、正しい対策ができているのか不安を感じています。セキュリティ規程は作成されていますが、十分に運用されていません。従業員教育としては、年間計画の従業員研修にセキュリティ対策の内容を盛り込んでいます。

02 セキュリティ課題

担当者の知識不足から生じるベンダーへの依存を懸念

当初の課題

- ベンダーへの依存度が高すぎることに不安を感じる
- セキュリティ規程が十分に運用されていない
- 従業員へのセキュリティ教育と知識の共有が不十分

専門家派遣支援で明らかになった課題

- クラウドサービス利用時の多要素認証が未導入
- 情報資産管理台帳の整理ができておらず見直しが必要
- ネットワークログを取得していないためリスクがある

03 取組内容

STEP 1　課題の可視化

本事業の専門家派遣において、セキュリティ対策の現状を確認し、「保守運用に関してベンダーへの依存度が高い」、「セキュリティ規程および情報資産管理台帳の運用が行われていない」、といった課題を洗い出しました。

STEP 2　課題解決に向けた優先順位の決定

洗い出した課題をリスト化して、解決に向けた優先順位を決定しました。当初、セキュリティ担当者は体系的な知識を得るというステップを経てから実務的な対策に移行することを考えていましたが、本事業の専門家のアドバイスにより、早期の解決が必要なセキュリティ対策を優先することとしました。

STEP 3　リスクの大きい実務的な課題から一つずつ改善

まず、ベンダーに一任していた脆弱性情報の能動的な収集を行いました。社内に向けて定期的に脆弱性情報を提供するようになると、従業員の危機意識が高まり担当者への問い合わせが増えました。また、ネットワークログの収集・監視を開始し、多要素認証の導入についても前向きに検討し始めました。

STEP 4　セキュリティ規程と情報資産管理台帳の評価と修正に着手

長期間メンテナンスしていなかったセキュリティ規程に関しては、独立行政法人情報処理推進機構（IPA）のひな型と照らし合わせて評価・修正を開始しました。また、情報資産管理台帳に関しては、本事業のワークショップで学んだ内容を参考に、不足している部分を追加する形で少しずつ修正作業を進めています。

リスクの大きい課題から改善に着手しつつ知識を吸収

本事業の専門家派遣において、課題の洗い出しを実施しました。「セキュリティ担当者に専門的な知識がなく不安を感じている」、「ベンダーに一任している保守運用で正しい対策ができているか否かの判断がつかない」、「SECURITY ACTION（二つ星）の宣言時にプライバシーマーク（Pマーク）の規程と照らし合わせて作成したセキュリティ規程がメンテナンスできていない」、といった課題を可視化し、一つ一つのテーマごとに解決に向けた方策を練っていきました。担当者は当初セキュリティに関する体系的な知識を吸収しなければ課題を解決できないと考えていましたが、「リスクの大きい課題から実務的に解決すべき」と本事業の専門家に指摘され、すぐに着手できる課題から改善を目指すことにしました。ベンダーから提供されている脆弱性情報を自社で能動的に収集するようになったほか、サーバ入替時にアクセスログの取得を開始するとともに、クラウドサービス利用時の多要素認証の導入も検討しました。セキュリティ規程に関しては、現状の規程を点検した上で、将来的に全従業員を巻き込んで運用していくことを決定しました。情報資産管理台帳についても、各部の担当者による記入項目の漏れなどを確認した上で、全社的に運用していく方向性を定めました。

04 結果と今後

全従業員でセキュリティ対策に取り組む企業へ

本事業の専門家派遣やセミナー・ワークショップを通じて専門的な知識を身につけたことで、ベンダーからの提案を正しく理解し、意見を述べたり疑問を呈したりすることができるようになりました。セキュリティ規程および情報資産管理台帳の評価・修正については、来年度よりさらに本格的に着手する予定です。将来的には、全従業員を巻き込む形で運用していくことを目指しています。

経営層の声

当社の事業において必要な情報セキュリティ管理体制・対策づくりを組織的に推進していく機会となりました。取組から運用に移行し、結果が出るのはこれからですが、変化し続ける環境に対応しながら、今後も継続的に取り組んで参ります。

参加者の声

本事業のセミナーやワークショップは、回を重ねるごとに専門用語などがわかるようになり、とても勉強になりました。他社の参加者と交流し、当社と同様に他業務との兼務で悩みながら努力している方たちがいることを知り、モチベーションの維持と向上につながりました。

インシデント対応フローを明確化し、自社の業務内容に合わせて再整備

取り組んだ支援テーマ：ネットワークセキュリティ / **エンドポイントセキュリティ** / モバイルデバイス / データ保護 / **セキュリティ意識と教育** / 外部パートナーとの関係

企業プロフィール
業種 / 従業員数：サービス業 / ～300名
セキュリティ体制：1名体制 兼務 経営者

事業内容
創業当初からソフトウェア開発事業を展開しており、高い技術を持つエンジニアが幅広い業種でソフトウェア開発やサービス構築を行っています。また、培ってきた経験や技術力のある人材を活用し、IT分野における人材派遣事業も展開しています。さまざまな企業のIT運用を総合的にサポートする企業です。

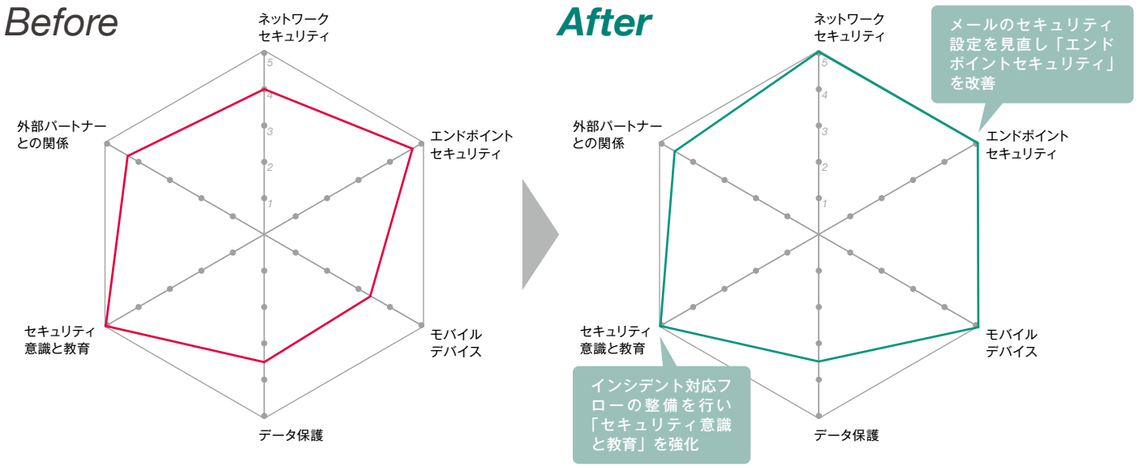
01 背景と状況
セキュリティ対策を実施しているが見直しが必要

02 課題
インシデント発生時の対応手順が初動に限定

03 取組内容
インシデント対応手順を具体化、業務に合わせて整備

04 結果と今後
セキュリティ対策をさらに改善しつつ教育にも注力

Before ***After*** 取組を通じたビフォーアフター



01 背景と状況

ISMS認証を取得しセキュリティ対策を推進しているが見直しが必要

基本的なセキュリティ対策は実施 / セキュリティ担当が1名の管理体制 / セキュリティ対策を評価したい

ISMS認証を取得し基本的なセキュリティ対策は実施していますが、対策の妥当性を判断できておらず、インシデント発生時の具体的な対応手順もありませんでした。本事業の専門家に現在のセキュリティ対策を評価してもらい、不足している部分や強化すべき点を明確化したいと考え、本事業に参加しました。

02 セキュリティ課題

インシデント発生時の対応手順が整備されていない

当初の課題
- 現状のセキュリティ対策の妥当性を評価できていない
- インシデント発生時の対応手順が決まっていない
- 担当者のセキュリティ知識の向上を図りたい

専門家派遣支援で明らかになった課題
- UTM の設定に関する管理はベンダー任せ
- メールのセキュリティチェック設定の見直しが必要
- 従業員向けの研修は行っているが確認テストは未実施

03 取組内容

STEP 1 本事業の専門家とともに課題の洗い出しと優先順位づけを実施
本事業の専門家派遣により、セキュリティ対策の現状評価と課題の洗い出しを行いました。課題対応の優先順位を決め、優先度の高い「インシデント対応フローの作成」に着手しつつ、UTM（Unified Threat Management）の設定確認やメール関連のセキュリティ対策を強化することにしました。

STEP 2 IPAの手引きを参考にしながらインシデント対応フローを検討
インシデント発生時の対応については、初動のみ決まっており、その後の具体的な対応が決まっていませんでした。そこで、本事業の専門家から提供を受けたIPAの「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」を参考にしながら、具体的な対応内容を検討しました。

STEP 3 インシデント発生時の具体的な対応作業の検討や担当者のアサインを実施
手引きをもとに自社に合わせたインシデント対応フローを作成しました。フローの作成に伴い、インシデント対応時の具体的な対応作業を検討し、対応する担当者を決定しました。あわせて、ハードウェアとソフトウェアの復旧責任者を決定し、社内窓口や関連するベンダーの連絡先の確認も実施しました。

STEP 4 UTMのアップデート状況やメールのセキュリティチェック設定の確認を実施
UTMのアップデート状況やメールのセキュリティチェック設定の確認を実施しました。ベンダーに確認したところ、UTMのアップデート管理は実施されていましたが、暗号化されたメールや添付ファイルについてはセキュリティチェックができていなかったため、直ちに設定の変更を依頼し、完了しました。

インシデント対応フロー作成とセキュリティ対策強化

本事業に参加した目的は「インシデント対応フローを構築する」ことでしたが、本事業の専門家のヒアリングにより、現状のセキュリティに関する課題の洗い出しを網羅的に行いました。明確になった複数の課題に対し、本事業の専門家からアドバイスを受けながら優先順位をつけました。最も重要度の高かった「インシデント対応フローの構築」については、独立行政法人情報処理推進機構（IPA）が公開している「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」を参考にしながら、スムーズに文書化することができました。あわせて、インシデント発生時に実施する具体的な対応作業や担当者の検討に加え、ハードウェアとソフトウェアの復旧責任者と関係連絡先の確認を実施しました。また、本事業の専門家からの指摘により、メールのセキュリティチェックの設定の確認も行いました。ベンダーに確認したところ、初期設定から変更しておらず、必要なセキュリティチェックができていない状況だったため、直ちに修正を依頼し完了しました。従業員のセキュリティ教育の強化については、新入社員向けの研修に取り入れるため、本事業の専門家から紹介されたIPAの「中小企業の情報セキュリティ対策ガイドライン」を参考にしながら、内容の精査を進めています。

04 結果と今後

インシデント対応の継続的な見直し、社内教育に注力

本事業の参加目的としていたインシデント対応フローの文書化を推進することができました。本事業のセミナーで学んだ「インシデント対応」に関する知識を活用し、継続的な見直しを行うとともに、社内のセキュリティ教育にも注力していく予定です。また、担当者1名によるセキュリティ管理体制を強化していくため、今後はセキュリティ業務を担務できる人材の育成にも取り組んでいきます。

経営層としての声
本事業でセキュリティ対策の見直しができたことにより、主要な取引先が毎年実施しているセキュリティに関するアンケートでは高い評価が得られると考えています。インシデント対応フローの作成が完了したため、今後は従業員のセキュリティ教育にも注力していきます。

参加者としての声
インシデント対応フローの文書化が実現できたため、本事業への参加目的は概ね達成することができました。今後もISMS認証取得の継続とともに、本事業で得た知識や経験を社内で共有することにより、社内のセキュリティ意識のレベルを向上させていきたいと考えています。

令和5年度中小企業サイバーセキュリティ対策継続支援事業 事例集

発行者
東京都産業労働局商工部経営支援課
新宿区西新宿二丁目8番1号
電話番号: 03-5320-4770

発行年月
令和6年3月