令和6年度版　中小企業サイバーセキュリティ社内体制整備事業　事例集

東京都産業労働局

中小企業サイバーセキュリティ社内体制整備事業

事例集

40社の
対策事例を掲載

令和６年度版

東京都産業労働局

令和6年度
中小企業サイバーセキュリティ社内体制整備事業　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: 03-5320-4773

発行年月
令和7年3月

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社内体制整備事業」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6年度の本事業の参加企業40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。

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6年度

中小企業サイバーセキュリティ社内体制整備事業

事例集

目次

中小企業サイバーセキュリティ社内体制整備事業について

社会におけるDX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。

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。

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。

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。

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と中小企業に求められるセキュリティ対策	企業経営に必要なIT活用とサイバーセキュリティ対策の実践	ISMSなどのフレームワークの種類と活用法の紹介	ISMSの構築と対策基準の策定と実施手順	ISMSの管理策に基づいた対策とセキュリティ対策状況の有効性評価	情報システム構築時に参考となる各種ガイドラインの紹介と必要な工程の説明	ガイドラインを参考にした情報システム導入におけるセキュリティ対策の実装と運用ポイントの紹介	サイバーセキュリティ対策を実践するための知識とスキルの認定制度	セキュリティ対策のための人材育成カリキュラムの計画と実施方法	全体総括 振り返りと今後のアクションについて
自社のIT活用状況とトレンドや知識向上を見据えた今後の対策を整理する	最新のインシデント事例やガイドラインを参考にした対策基準を検討する	リスクアセスメントの実施に必要な情報資産を洗い出し、リスクレベルを算出する	リスクアセスメントの結果をもとに対策基準および適用宣言書を作成する	サイバー攻撃から自社を守るため、対策の実施優先度や社員の教育・トレーニングの取組や効果を検討する	自社の特性から想定される脅威に対し、実施手順や課題の洗い出しと解決手段を立案する	新システム導入時に必要なセキュリティ機能や運用上のセキュリティ課題と解決策を考える	理想的なセキュリティ人材育成のための教育プランや社内体制（評価制度）を策定する	セキュリティ教育を学ぶための学習方法やツールをピックアップし重要なトピックを考える	これまでのワークを振り返り、企業間での共通点や差異をもとに新たなアイデアや気づきを得る

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、4～5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。

3 専門家派遣 1社につき全4回

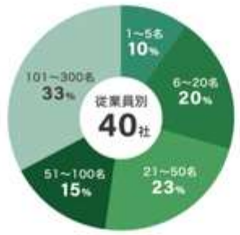
参加企業の皆様がワークショップで洗い出した課題や、企業が直面しているセキュリティ上の問題点解決へ向け、多様な得意分野を持つ専門家（ネットワーク設計・構築などの技術分野での経験、リスク分析、セキュリティ事故対応や再発防止策の検証、監査、セキュリティ教育、各種セミナー・支援の講師経験など）が、セミナー・ワークショップで得た気づきや知識を活かし、参加企業の皆様が自ら対策を立案できるようサポートしました。

1. 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の網羅的なヒアリングを実施。
2. 第1回のヒアリング結果をもと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。
3. 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。
4. 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。

参加企業・参加者の属性

支援対象企業の属性

様々な業種や規模の都内中小企業40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40名の方にご参加いただきました。

※構成比の数値を四捨五入しているため、個々の集計値の合計は必ずしも100%とならない場合がございます。

参加企業のセキュリティ体制と支援テーマ

卸売・小売	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
電子機器製造販売業A社	~5名		●		●		●				●	
OA機器販売・運用保守業B社	~20名		●		●		●				●	
機械製造・卸売業C社	~50名	●			●		●				●	
飲食関連備品販売業D社	~50名		●		●		●			●	●	
アパレル用品製造販売業E社	~100名	●			●			●		●	●	
塗料販売業F社	~100名	●			●					●	●	
化粧品販売業G社	~100名		●		●		●				●	
オフィス機器製造販売業H社	~100名		●		●		●			●		
アパレル用品製造販売業I社	~300名	●			●		●				●	
繊維・化成品製造販売業J社	~300名	●		●			●			●	●	

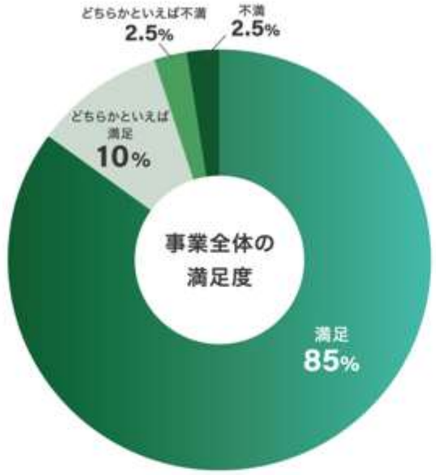
建設・製造	従業員数	セキュリティ体制					支援テーマ					
		1名体制	複数	専任	兼務	経営者	ネットワークセキュリティ	エンドポイントセキュリティ	モバイルデバイス	データ保護	セキュリティ意識と教育	外部パートナーとの関係
システム機器製造業A社	~5名		●		●	●	●			●	●	
管工事業B社	~20名	●			●			●		●	●	
精密機器製造業C社	~50名	●		●			●	●			●	
印刷業D社	~50名	●			●				●		●	
専門工事業E社	~50名		●		●		●				●	●
電子部品製造業F社	~100名		●		●			●			●	
電気機器製造業G社	~300名	●			●					●	●	●
通信機器販売業H社	~300名	●		●						●	●	
精密部品製造業I社	~300名		●	●			●			●	●	
医療機器製造業J社	~300名		●		●			●			●	●

サービス・その他	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
テスト支援ツール開発・販売業A社	~5名	●			●	●	●			●	●	
社会保険労務士業B社	~5名	●			●	●				●	●	●
薬事支援サービス業C社	~20名	●			●	●	●	●			●	
マーケットリサーチ業D社	~20名	●			●		●	●			●	
ITコンサルティング業E社	~20名	●			●		●				●	
臨床試験支援サービス業F社	~20名	●			●	●		●		●	●	
不動産仲介業G社	~20名	●			●	●		●			●	
ITインフラサービス業H社	~20名		●		●	●		●	●		●	
経営コンサルティングサービス業I社	~50名	●			●		●				●	
証券金融業J社	~50名	●			●					●	●	
人事総務アウトソーシング業K社	~50名		●		●		●				●	●
産業廃棄物処理業L社	~50名		●		●	●	●	●			●	
広告業M社	~100名		●		●		●		●		●	
人材支援サービス業N社	~300名	●			●				●	●	●	
飲食サービス業O社	~300名	●			●			●		●	●	
その他サービス業P社	~300名		●		●		●			●	●	
総合コンサルティングサービス業Q社	~300名		●		●					●	●	
不動産売買業R社	~300名		●		●			●			●	
システムインテグレーション業S社	~300名		●		●			●		●	●	
金融商品取引業T社	~300名		●		●	●			●		●	

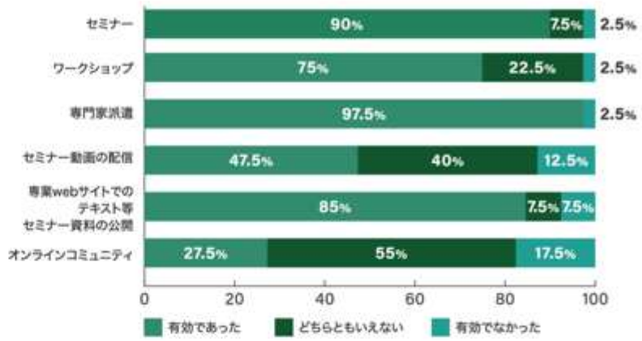
アンケート

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。

本事業への総合的な満足度



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、85%の参加者が「満足」を、10%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、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。

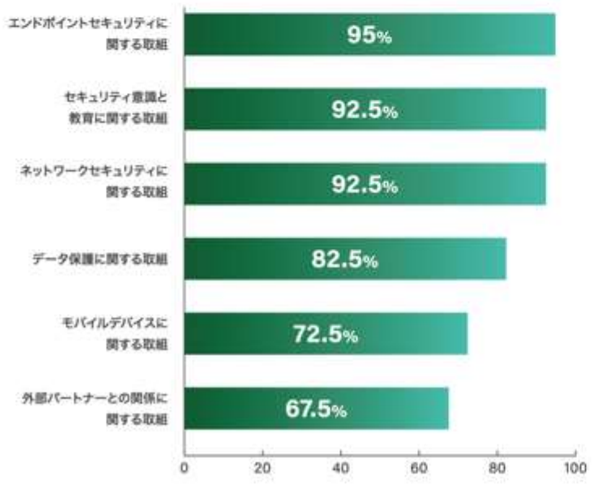
本事業を通じて、事業参加前と比べて貴社の情報セキュリティレベルに変化はありましたか？

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	77.5%
2	セキュリティ体制を強化できたから	62.5%
3	従業員に対して教育を実施したから	50.0%
4	規程類が整備できたから	40.0%
5	その他	7.5%

事業に参加した企業の92.5%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、続いてセキュリティ体制の強化や従業員への教育が挙げられた。また、その他として「今後の指針としての資料を得たから。」、「経営層に（セキュリティ対策の重要性を）アピールができたから。」という回答などがあった。

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、参加企業の95%が「エンドポイントセキュリティに関する取組」を行っている。この項目ではウイルス対策ソフトウェアの運用強化やパスワードに関する新たなルールの策定などを行い、利用する端末のセキュリティ強化を図った。

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」と「ネットワークセキュリティに関する取組」(92.5%)だった。「セキュリティ意識と教育に関する取組」では、定期的なセキュリティ教育や標的型攻撃メール訓練の計画策定・実施、セキュリティポリシーの整備や具体的なルール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。

また、「ネットワークセキュリティに関する取組」ではUTMなど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いる。参加企業の多くが本事業を通じてセキュリティ対策の向上につなげることができたと言える。

事例の見方

卸売・小売　塗料販売業　F社

新設間もない情報システム課から始まる、ゼロからのセキュリティ管理体制の構築

背景と課題

新設された情報システム課が社内のセキュリティ強化を担うことになりましたが、1人体制のため相談できる相手がおらず、不安を感じていました。

取組内容

本事業の専門家と協力して既存のセキュリティ対策を見直し、時代に即した対策を実行することで、全社のセキュリティレベルを向上させました。

背景と課題

背景

新設された情報システム課は1人体制のため、セキュリティ対策の実行が難航

昨今の社会情勢を踏まえ、社内でセキュリティ対策を推進する機運が高まり、情報システム課が新設されました。しかし、担当者が一人しかおらず、専任でもなかったため、セキュリティ対策が思うように進みませんでした。さらに、社内に相談できる人がいないこともあり、本事業の専門家からのアドバイスが必要でした。

課題

1 セキュリティに関する知識が不足しているため

2 セキュリティポリシーやガイドラインが最新の

3 経営層を含めた全従業員のセキュリティに対す

取組内容

取組1　本事業の専門家のアドバイスをもとに、自社で取り組むべきセキュリティ対策を抜本的に見直し

自社で取り組んでいるセキュリティ対策が事業規模や業務内容に適しているか判断できなかったため、本事業の専門家からアドバイスを受けました。現状を評価し、自社に必要なセキュリティ対策をリスト化して具体的なタスクに落とし込み、順次対応していきました。

取組2　本事業で提供された最新のサイバー攻撃事例をもとに、セキュリティポリシーとガイドラインを更新

古くなったセキュリティポリシーやIT利用に関するガイドラインを更新しました。本事業のセミナーやワークショップ、専門家から提供されたフォーマットをもとに、最近のサイバー攻撃事例を反映した内容にしました。

取組3　全従業員を対象に、セキュリティ知識の習得と意識向上を目的とした教育プログラムを実施

経営層を含めた全従業員のセキュリティ知識を向上させるべく、実際に発生した事例などを用いて教育、啓蒙の機会をつくりました。MDM(※1)の活用などの技術的対策と並

※1　Mobile Device Management（モバイル端

※2　令和6年度中小企業サイバーセキュリティ社内

1 背景
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。

2 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。

3 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。

4 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。

企業プロフィール

事業内容

塗料の専門会社として、自動車、建築機械、鋼材、建築向けの塗料を提案・販売しています。一般的な塗料に加え、電磁、防錆、環境対策に優れた特殊塗料も提供しています。また、塗料事業から発展し、塗料関連の設備エンジニアリング事業も展開しています。

結果と今後

自社に必要なセキュリティ対策をリスト化し、順次取り組んでいます。セキュリティポリシーと
更新に際しては、実際のサイバー攻撃事例をもとに具体的な対策を組み込みました。今後も
セキュリティ意識を向上させるため、定期的な情報共有に努めます。

5 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。

結果と今後

1 セキュリティ対策の見直しにあたり、ベンダーの変更から検討しました。しかし、大規模なサーバー環境の変更が必要となり、推定以上のコストがかかるため、計画自体を再検討しています。まずは、重要データの定期的なバックアップなど、できることから着手しています。 → 継続

2 作成したドキュメント類は、本事業の
視点をセキュリティポリシーやガイドラ
更新に取り組みます。

3 セキュリティ知識向上のため、グルー
から提供されたサイバー攻撃事例を
教育を予定しています。

6 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。

取り組んだ支援テーマ　データ経営　セキュリティ意識と教育

Before（取組前）

ネットワークセキュリティ 4.3
内部ルールへの浸透 3.7
セキュリティ組織と運営 4.0
データ保護 2.5

今後の展望

経営層の理解を得ながら、セキュリ
セキュリティポリシーやガイドライン
また、従業員へのセキュリティ教育も
段階的な見直しも進めています。

7 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。

経営層の声

本事業に参加することで、セキュリティの重要性が会社の信用問題にも関わる重大な課題であることを再認識しました。リソース面での支援を受けて対策を拡大し、経営層を含めた全従業員のセキュリティ意識と
として取り組んでいます。

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、同等規模の会社の担当者と交流する中で、自分では考えつかなかったセキュリティ対策やITツールを知ることができ、非常に有

8 経営層／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。

卸売・小売

電子機器製造販売業　A社

少数精鋭で挑むセキュリティ強化
VPN導入で実現する通信保護と柔軟な働き方の両立

企業プロフィール
- 業　　種：卸売業・小売業
- 従業員数：～5名

セキュリティ体制　複数名体制/兼務

事業内容　高視認性を誇る電子ペーパーサイネージや薄型TV用タッチセンサーフレームなどの製品を公共施設、商業施設、オフィスなど幅広い領域に提供しています。環境に優しいソリューションを通じて、受託開発やカスタマイズにも対応し、アイデアを形にするサービスを展開しています。

背景と課題
クラウドサービス化した製品をリリースし、取引先からセキュリティ関連の問い合わせが増えたことからセキュリティ対策の強化を模索していました。

取組内容
現在のセキュリティ状況を再検討し、セキュリティ関連規程を改訂しました。また、多様な働き方に合わせて通信セキュリティを強化しました。

結果と今後
セキュリティソフトの機能追加によりシステム環境を強化しました。本事業で学んだセキュリティ情報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の向上を実感しています。将来的なPマーク(※1)取得を見据えた準備が整い、セキュリティ確保とビジネスの発展の両立を推進します。

背景と課題

背景

取引先が求めるセキュリティ対策の水準が高度になり、セキュリティ対策の強化を検討

専門的なセキュリティ対策の知識がない中で、取引先が求めるセキュリティ対策の水準は高まっており、対策の強化を模索していました。また、アフターコロナの影響を踏まえ、自社のセキュリティ対策を客観的に見直すことにより、多様な働き方に対応できるセキュリティ管理体制に進化させたいと考えていました。

課題

1. 現状のセキュリティ対策の妥当性を判断できず、実施すべきことが明確でない
2. セキュリティ関連規程の見直しが必要だが、着手が遅れている
3. リモート業務など多様な働き方を実現するためのセキュリティ対策が整備されていない

取組内容

取組1

本事業の専門家とともに現在のセキュリティ状況を客観的に捉え、必要なツールを見直し

本事業の専門家とともに自社で講じているセキュリティ対策について見直しを行いました。その結果、ネットワークの入り口に脆弱性があることが判明しました。そこで、ファイアウォール機能としてUTM(※2)など新たに導入すべきセキュリティ機器について検討しました。

取組2

セキュリティ関連規程を業務に則した内容に改訂、従業員に展開しセキュリティ知識の強化を図る

改訂したセキュリティ関連規程を社内に展開しました。規程にはPCやスマートフォンの適切なアップデートの運用を盛り込み、従業員への周知を徹底しました。また、インシデントやシステム障害に関する情報を定期的に共有して、従業員のセキュリティ知識の向上を図りました。

取組3

通信セキュリティを保護するためにVPN(※3)を導入し、多様な働き方の実現に向けて準備

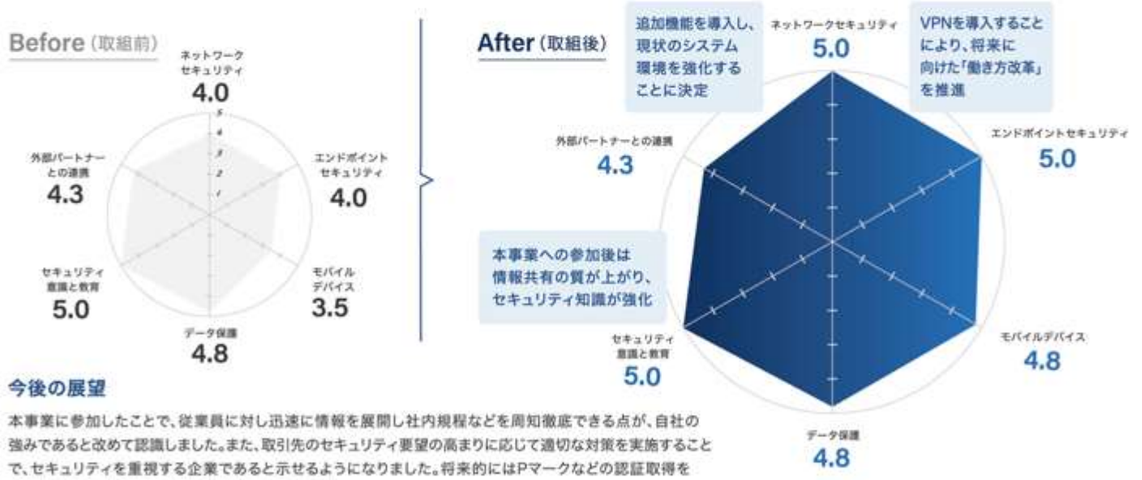
社外における通信セキュリティを担保するためにVPNを導入しました。また、PCやスマートフォンの位置検索機能やロック機能などを設定し、置き忘れや盗難に備えました。外部での営業活動やリモート業務にも対応できるよう、セキュリティ管理体制の強化を図りました。

※1　プライバシーマーク(個人情報を適切に取扱う体制を整備していると認定された事業者に付与)　※2　Unified Threat Management 統合脅威管理(複数のセキュリティ機能を統合した管理システム)
※3　Virtual Private Network(仮想専用通信網)　※4　独立行政法人情報処理推進機構

結果と今後

1. 取組の結果、自社で利用しているセキュリティソフトの機能をアップグレードしたり、導入しているルータの設定を見直すことでファイアウォール機能にも対応できることが判明しました。セキュリティ対策強化のために、今後も製品の導入検討は継続していきます。　→ 解決
2. かねてよりIPA(※4)が公開している動画を従業員が視聴していましたが、本事業のセミナーで得た知識を朝礼で共有することにより、以前より情報共有の質が向上しました。今後、継続的な意識づけのため、定期的な理解度テストの実施を検討しています。　→ 継続
3. 定期的に社内端末の一斉チェックを行い、OSのバージョンや各種機能の設定など、セキュリティ規程に則しているか確認するフローを構築しました。また、VPN導入もあわせて実施したことにより、多様な働き方に合わせた環境を構築できました。　→ 解決

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連携



今後の展望

本事業に参加したことで、従業員に対し迅速に情報を展開し社内規程などを周知徹底できる点が、自社の強みであると改めて認識しました。また、取引先のセキュリティ要望の高まりに応じて適切な対策を実施することで、セキュリティを重視する企業であると示せるようになりました。将来的にはPマークなどの認証取得を検討しており、その下準備ができたと考えています。

経営層の声

セミナー・ワークショップ開催翌日の朝礼で担当者が情報共有することが定例となり、学んできたことが自社に還元されていると感じています。本事業を通じて従業員のセキュリティ知識を強化することができました。引き続きセキュリティ対策を実施し、取引先から信頼を勝ち取れる企業を目指します。

参加者の声

漠然としていたセキュリティについて体系的に学べ、他社の取組事例に触れられたことは大きな収穫でした。学んだ知識を共有することで従業員のセキュリティ意識も一層向上し、主体的に取組に協力してくれています。中小企業ならではの機動力を活かし、今後もセキュリティ対策を推進してまいります。

卸売・小売

OA機器販売・運用保守業 B社

老朽化が進む機器の入替を目指した予算確保と情報発信による従業員意識の向上で、信頼を勝ち取る

企業プロフィール
- 業　　種：卸売業・小売業
- 従業員数：～20名

セキュリティ体制　複数名体制/兼務

事業内容　知的財産や専門性の高い業務を手掛ける企業に対する管理システムの構築支援やDX推進のコンサルティング、OA機器・什器の販売など多岐にわたる事業を展開しています。創業以来蓄積している知見やネットワークを活かし、取引先の事業成長を推進し、企業価値の向上を支援します。

背景と課題
ISMS認証は取得していましたが、従業員のセキュリティ意識には個人差があり、導入済みの機器は老朽化が進むなど対策の強化が必要でした。

取組内容
教育内容の再検討とセキュリティ情報の発信を実施、老朽化が進む機器の入替とクラウドサービス利用に関するルールの策定を進めました。

結果と今後
朝礼時にセキュリティ情報の共有を行い、従業員のセキュリティ意識が向上しました。また、従業員が利用しているクラウドサービスについてはルールを設け、遵守してもらうための仕組みづくりを行います。
また、経営層にインシデント発生のリスクを説明し、最新機器などの導入予算案を提出する予定です。

背景と課題

背景

導入済のセキュリティ機器の老朽化に加え、従業員への教育も不十分

ISMS認証は既に取得していました。しかしセキュリティ教育は年に1回のみと、従業員の意識を強化できていませんでした。また、導入済みのセキュリティ機器は老朽化が進み、インシデント発生のリスクが懸念されていました。そのため、入替を行うとともに、新たな運用ルールの策定が必要でした。

課題

1. 年1回の研修だけでは従業員のセキュリティ意識は個人差があり、教育の再検討が必要
2. 保守期限切れの機器が一部存在し、インシデント発生リスクを抱えるも予算の確保に苦戦
3. クラウドサービスを利用する際の選定基準がなく、サービスの利用可否を判断できない

取組内容

取組1

従業員へのセキュリティ教育を再検討、朝礼や掲示板を活用してセキュリティ情報を共有

以前より、セキュリティ研修を年に1回実施していましたが、意識向上のためには頻度や内容の再検討が必要でした。そこで、本事業のセミナーで得た知識やテキストを活用し、朝礼や社内掲示板で共有する取組を開始しました。また、標的型メール訓練の実施も検討中です。

取組2

老朽化が進むセキュリティ機器を入れ替えるため、経営層に取組の必要性と予算化を上申

保守期限が切れているルータの入替とUTM(※1)の導入を検討しました。併せて、経営層の理解と予算確保のために、保守期限切れによるインシデント事例や入替の必要性を根拠とした資料を作成し、経営層へセキュリティ対策の重要性を具体的に説明しました。

取組3

利用するクラウドサービスについて利用状況を確認、新たに選定基準を設けることでルールを明確化

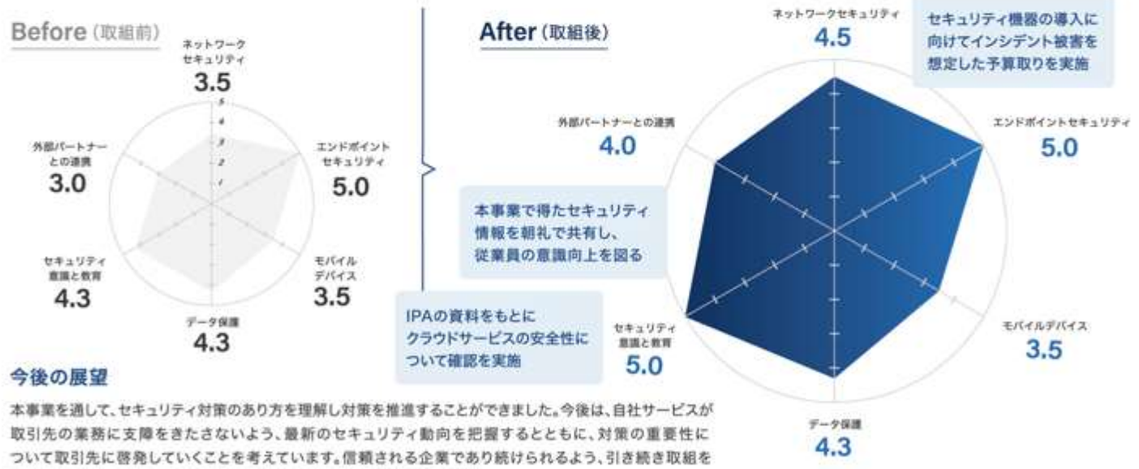
IPA(※2)の「中小企業のためのクラウドサービス安全利用の手引き」をもとに、現在利用するクラウドサービスについて、選定方法、運用時の管理体制、サービスに付帯するセキュリティ対策を確認しました。また選定基準として具体的な評価項目を設定し、運用ルールを定めます。

※1 Unified Threat Management 統合脅威管理（複数のセキュリティ機能を統合した管理システム）　※2 独立行政法人情報処理推進機構
※3 Endpoint Detection and Response（端末のセキュリティ脅威を検知・分析・対応するセキュリティ技術）

結果と今後

1. 特に、本事業のセミナーで学んだインシデント事例と実際の対応方法を社内で共有したことは、自社のリスク管理に当てはめて考える良い機会となりました。さらに、従業員のセキュリティレベルを把握するため、メール訓練を実施する方向で計画しています。　→ 継続
2. 予算の確保に向け、インシデント発生によって想定される被害額を伝えながら、経営層と議論をしています。予算の確保ができれば、ルータやUTMの導入に加え、既存のEDR(※3)のアップグレードを実施し、定期的にログ確認が行えるよう設定を強化します。　→ 継続
3. 複数導入しているクラウドサービスのうち、一つのサービスの利用状況を確認しました。この確認作業をもとに、他のサービスもあわせて順次確認していきます。さらに、セキュリティポリシーと照合してクラウドサービスの利用ルールの策定を進めていきます。　→ 継続

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連携



今後の展望
本事業を通して、セキュリティ対策のあり方を理解し対策を推進することができました。今後は、自社サービスが取引先の業務に支障をきたさないよう、最新のセキュリティ動向を把握するとともに、対策の重要性について取引先に啓発していくことを考えています。信頼される企業であり続けられるよう、引き続き取組を前進させ、セキュリティ対策の有識者としての立場を確立していきます。

経営層の声
本事業への参加を通じて、セキュリティ知識やノウハウを習得することができ、従業員のセキュリティ意識向上を実感しています。サイバー攻撃の手法は日々進化し、巧妙化しているため、最新の情報を入手し、セキュリティ対策や教育に今後も継続的に取り組むことで、自社の資産を保護していきます。

参加者の声
本事業の専門家派遣による個別支援、セミナー・ワークショップに無償で参加できる機会は大変貴重でした。サイバー攻撃の事例が増える中、今回進めたセキュリティ対策は自信を持って取引先にも明示することができます。また、本事業で得た知識を社内に展開することで、全社的な意識向上を実感しました。

卸売・小売

機械製造・卸売業　C社

アフターコロナ時代の働き方にマッチしたセキュリティ対策の見直しと管理体制の強化が重要課題に

企業プロフィール
- 業　　種：卸売業・小売業
- 従業員数：～50名

セキュリティ体制　1名体制/兼務

事業内容　長年培ってきた高度な技術と豊富な経験を活かし、製造業の取引先を中心に幅広く事業を展開しています。搬送機器や自動組立機に使用する産業用ロールや自動搬送システムなど、工場に必要なさまざまな機械・機器の製造・販売を行っています。

背景と課題

コロナ禍に情報システム部門は多様な働き方に対応してきましたが、現状のセキュリティ対策について改めて見直しを行いたいと考えていました。

取組内容

本事業の専門家からアドバイスを受け、従業員へのセキュリティ研修、Webサイトのセキュリティ強化、UTM(※1)の見直しなどに取り組みました。

結果と今後

セキュリティ研修を通じて従業員のセキュリティリテラシーが向上し、技術的な対応によって全体的なセキュリティ対策が強化されていることを実感しています。しかし、本事業で明らかになったセキュリティ課題はまだ多く残っているため、引き続き危機感を持ち、一つ一つ確実に対応していきます。

背景と課題

背景

コロナ禍で対応したさまざまなセキュリティ対策について、改めて見直しを行いたい

コロナ禍に情報システム部門として多様な働き方に対応してきました。コロナの終息により、従業員のセキュリティ意識や対策実施レベルに差があることが判明しました。
また、自社のセキュリティ対策を第三者の評価をもとに把握し、さらに強化するためのアドバイスを得たいと考えました。

課題

1. 従業員への定期的なセキュリティ教育を行っておらず、セキュリティ意識が浸透していない
2. Webサイトのセキュリティ対策を十分に把握できておらず、今後リニューアルも検討
3. UTMが導入されているものの、効果的な活用方法を理解していない

取組内容

取組1　従業員に対して定期的なセキュリティ研修を実施し、学習意欲を高める評価制度の導入も検討

令和7年1月から、毎月行われる営業会議に従業員向けのセキュリティ研修を盛り込む予定です。各従業員の業務内容に合わせた教育内容を検討するとともに、学習意欲を高めるために、ゲーム要素を取り入れたり、評価制度の導入も検討しています。

取組2　Webサイトのセキュリティリスク調査および開発言語のバージョンアップを実施

Webアプリケーションへの攻撃を防ぐためにWAF(※2)を導入しており、ログの管理状況にも問題がないことを確認しました。また、現在使用している開発言語のバージョンが古く、セキュリティリスクがあると本事業の専門家から指摘され、バージョンアップを実施しています。

取組3　UTMの設定について現状を調査し、自社の運用に適した使い方への見直しを実施

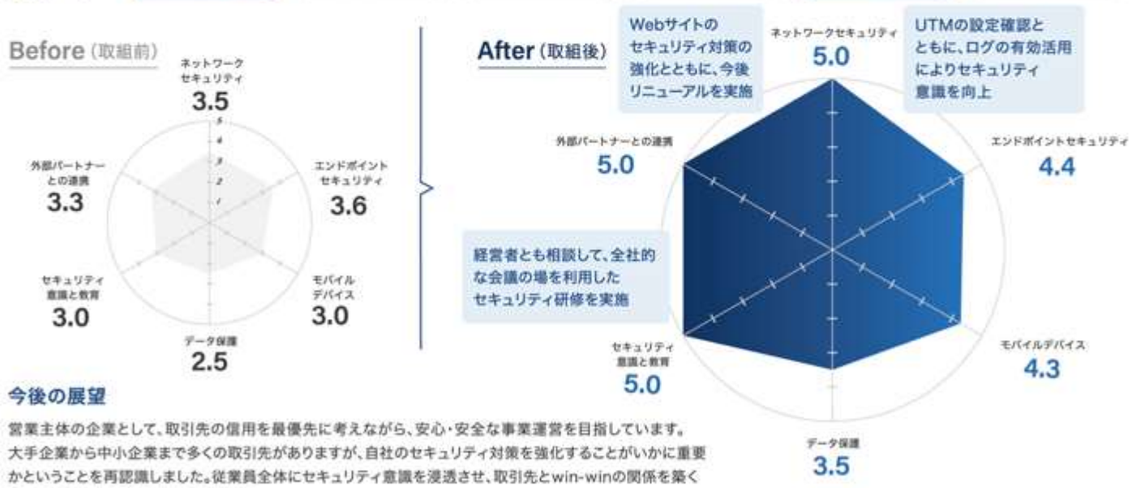
UTMの設定仕様書をベンダーから入手し、本事業の専門家に協力を得て、設定内容の検証を行いました。自社に必要なセキュリティ対策レベルを確保しつつ、従業員の日常業務に支障をきたさない設定となっていることを確認しました。

※1　Unified Threat Management 統合脅威管理（複数のセキュリティ機能を統合した管理システム）　※2　Web Application Firewall（ウェブアプリケーションを攻撃から守るための仕組み）

結果と今後

1. 毎月行われる営業会議後に、セキュリティ研修を実施する予定です。また、本事業のセミナーやワークショップ、各ベンダーで開催している展示会などで得た情報を随時共有し、継続的にリテラシー向上に向けた取組を進めていきます。　→ 継続
2. Webサイトの重要データの保護も問題ないことが確認できたため、現在のシステム環境で実施できるセキュリティ対策は、ほぼ完了しました。今後、Webサイトのリニューアルを検討しており、より強固なセキュリティ環境への移行を進める予定です。　→ 解決
3. UTMの設定が確認できたことで安心は得られましたが、セキュリティ状況レポートが十分に活用されていませんでした。そこで、外部サイトへのアクセスをブロックしたログ情報などを社内に共有し、セキュリティ意識の向上に取り組んでいきます。　→ 解決

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連携



今後の展望

営業主体の企業として、取引先の信用を最優先に考えながら、安心・安全な事業運営を目指しています。大手企業から中小企業まで多くの取引先がありますが、自社のセキュリティ対策を強化することがいかに重要かということを再認識しました。従業員全体にセキュリティ意識を浸透させ、取引先とwin-winの関係を築くことができるよう取り組んでいきます。

経営層の声

本事業に参加することで、セキュリティ対策に不備があると取引先にも影響を与える可能性があることに気づきました。この気づきは経営の意思決定に大きな影響を与え、自社のセキュリティ管理体制を見直すきっかけとなっています。今後は、リスクに備えるためにサイバー保険への加入も検討していきます。

参加者の声

事業開始前と現在では、セキュリティに対する意識が大きく変わりました。しかし、自分だけが高い意識を持っていても意味がなく、全従業員の関心を引き、どのようにして高いセキュリティ意識を維持していくかが課題です。今後もこのようなセキュリティ関連事業があれば、積極的に参加したいと思います。

卸売・小売

飲食関連備品販売業　D社

知恵と技術による仕掛けや仕組みづくりで、セキュリティ体制強化と人材育成を実践

企業プロフィール
- 業　　種：卸売業・小売業
- 従業員数：～50名

セキュリティ体制　複数名体制/兼務

事業内容　お客様が安心して使うことができる、食文化に貢献する高品質な食器・厨房備品を提供しています。和食器、洋食器、グラス、厨房備品など幅広い商品ラインアップを取り揃え、ホテル・ダイニング、飲食店から病院・福祉施設まで多様なシーンに最適な商品を提案しています。

背景と課題

セキュリティ体制は高まってきているが、バックアップ方式や教育体制、ネットワーク強化に改善の余地があり、効率的な運用体制を必要としていました。

取組内容

バックアップ方式の再検討、従業員教育の整備、ネットワーク安定化などに取り組み、「自然とセキュリティ知識が身につく運用体制」を構築しました。

結果と今後

NAS(※1)とクラウドサービスを併用したバックアップの二重化や、無線から有線への切替によりネットワークの安定性の向上を図りました。従業員向けにはクイズ形式の教育資料を作成中です。
今後はVPN(※2)やルータのバージョンアップデート、脆弱性診断を検討し、体制強化を目指します。

背景と課題

背景

社内のシステム環境の改善が進む中、教育環境の整備と運用の効率化に課題

情報システム部門の設立を令和6年11月に控えており、基幹システムの入替に伴うシステム改善が進む一方、従業員へのセキュリティ教育に課題を感じています。セキュリティ対策は一定の効果があるものの、バックアップ体制の変更を検討するなど、さらなる仕組み化と効率化が求められています。

課題

1. バックアップ体制や運用フローが未整備で、基幹システムの入替に伴い対策が急務
2. セキュリティ教育の受講に抵抗感を示す従業員が多く、体系的な教育ができていない
3. ネットワークの安定性に不安がある上、ハードウェアのバージョンの更新ができていない

取組内容

取組1　バックアップ体制の再検討と運用フローの整備を行い、事業の継続性を確保できる具体策を協議

NASを利用して社内でバックアップを取得していますが、円滑なデータ復旧に懸念があります。そのため、令和6年度に予定していた基幹システム入替に伴い、より安全性の高い方式への変更を検討します。また、事業の継続性を確保するため、冗長性を高める具体策を協議します。

取組2　従業員の学習への抵抗感を軽減するセキュリティ教育方法を模索し、知識強化を狙う

学習に抵抗感を持つ従業員が多く、「セキュリティ研修」や「教育プログラム」といった、堅苦しさを感じる取組では、積極的な参加が期待できません。そのため、従業員が抵抗なくセキュリティ知識を身につけられる、柔軟で親しみやすい教育プログラムを検討します。

取組3　業務を安定して行うためにネットワークの安定化と機器のバージョンアップデートを計画

以前よりネットワークの安定に課題を感じており、より安定した業務運営を実現するためのネットワーク構成について考えます。また、社内で利用しているハードウェアが最新バージョンになっているかを確認し、古い機器についてはバージョンアップデート計画を作成します。

※1　Network Attached Storage(ネットワークに接続された記憶装置)　※2　Virtual Private Network(仮想専用通信網)
※3　Solid State Drive(フラッシュメモリを使った高速記憶装置)

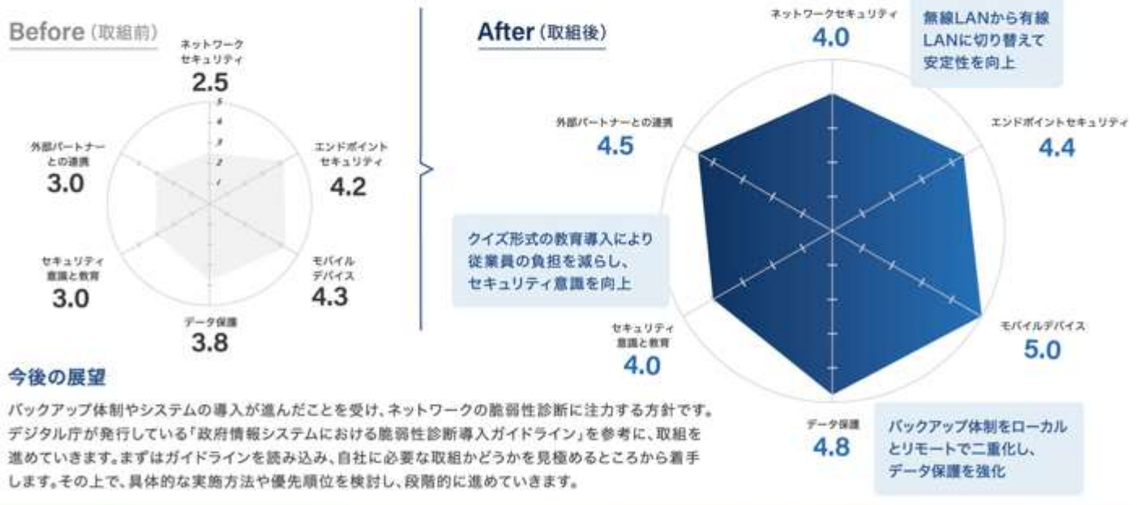
結果と今後

1　NASとクラウドサービスによるバックアップの二重化を実現しました。また、システム接続はローカルとリモートの併用に変更し、冗長性の高い環境を構築しました。さらに、SSD(※3)も物理的に二重化し、データ保護と業務の安定性を強化しました。　→　解決

2　従業員が無理なく学べる環境を目指し、新人教育マニュアルにセキュリティ項目を追加しました。また、教育プログラムにはクイズ形式を取り入れ、従業員の負担を軽減しつつ、楽しみながらセキュリティリテラシーが向上する仕組みを構築中です。　→　継続

3　基幹システムの入替を契機に、ネットワークの一部を無線から有線に切り替え、業務の安定化を図りました。ネットワーク診断については適用範囲を含め、今後検討していきます。また、機器のバージョンアップデート計画は途上であり、具体的な計画を作成中です。　→　継続

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連携



今後の展望

バックアップ体制やシステムの導入が進んだことを受け、ネットワークの脆弱性診断に注力する方針です。デジタル庁が発行している「政府情報システムにおける脆弱性診断導入ガイドライン」を参考に、取組を進めていきます。まずはガイドラインを読み込み、自社に必要な取組かどうかを見極めるところから着手します。その上で、具体的な実施方法や優先順位を検討し、段階的に進めていきます。

経営層の声

本事業を通じて、バックアップ体制の整備やネットワーク冗長化などの改善が進みました。また、経営層においてもセキュリティ対策の重要性を再認識し、コスト面を考慮しながら現実的な施策を推進する方向性が明確になりました。今後はこれらの取組を仕組み化し、セキュリティ管理体制を強化していきます。

参加者の声

ワークショップで他社の実践例や意見を聞けたことで、自社の課題と強みを客観的に把握することができました。
今後は従業員教育に注力し、従業員の負担を軽減しながらセキュリティ意識を向上させる仕組みづくりを進めたいと考えています。学んだ内容を取り入れながら、対策を改善していきます。

卸売・小売

アパレル用品製造販売業　E社

セキュリティ担当者1名から全従業員へ拡げる、強固なセキュリティ体制構築に向けた取組

企業プロフィール
- 業　　種：卸売業・小売業
- 従業員数：～100名

セキュリティ体制　1名体制/兼務

事業内容　アウターや帽子、アクセサリーといったアパレル用品の輸入・販売を主な事業として展開しています。
また、グローバルな展開を行っており、本社の歴史は創業から100年を超えています。
実店舗だけではなく、ECサイトの運営も行っています。

背景と課題

本社の管理部門がセキュリティ対策を主導する一方で、ECサイトで個人情報を取扱うこともあり、従業員のセキュリティ意識の向上が必要でした。

取組内容

セキュリティ情報の社内への積極的な共有やアクセス権限の管理ツールの導入、シャドーIT(※1)の利用に関するルールの策定に取り組みました。

結果と今後

標的型攻撃メール訓練などの定期的な教育を通じて、従業員のセキュリティ意識を高め、全員が同じレベルの意識を持てるよう浸透を図ります。また、重要データの保護体制や社内の情報資産管理の強化により、万が一のインシデント発生にも対応できる強固なセキュリティ体制を構築していきます。

背景と課題

背景

本社の管理部門がセキュリティ対策を主導、従業員のセキュリティ意識に課題

セキュリティ対策は本社の管理部門が主導しており、セキュリティ担当者は知識を持っているものの、他の従業員にはセキュリティ意識や危機感が不足していました。また、自社のセキュリティ体制を第三者の客観的な視点で評価し、必要な対策を講じるため、本事業に参加しました。

課題

1. セキュリティポリシーが浸透しておらず、従業員のセキュリティ意識が不足している
2. アクセス権限の管理ツールを活用できておらず、個人管理に委ねられている
3. 会社の情報が私用のクラウドサービスに保存され、シャドーITの利用が常態化している

取組内容

取組1　セキュリティに関する情報を従業員に共有するとともに、メール訓練などの実践的な教育も計画

IPA(※2)が提供するセキュリティ情報や、本事業のセミナー・ワークショップで得た知識を社内で積極的に共有しました。また、従業員のセキュリティ意識向上のため、標的型攻撃メール訓練を計画しました。さらに、セキュリティポリシーの公開方法についても検討しました。

取組2　サーバの不具合を契機に新たな管理ツールを導入。重要情報へのアクセス権限の管理を強化

以前より導入していたアクセス権限の管理ツールは、サーバの不具合により十分に活用されていなかったため、新たな管理ツールの導入を決定しました。導入準備として、自社の情報資産を整理し、重要情報に対する現在のアクセス権限の付与状況を確認しました。

取組3　シャドーIT利用に関するセキュリティルールを定め、全従業員に対する注意喚起も行う

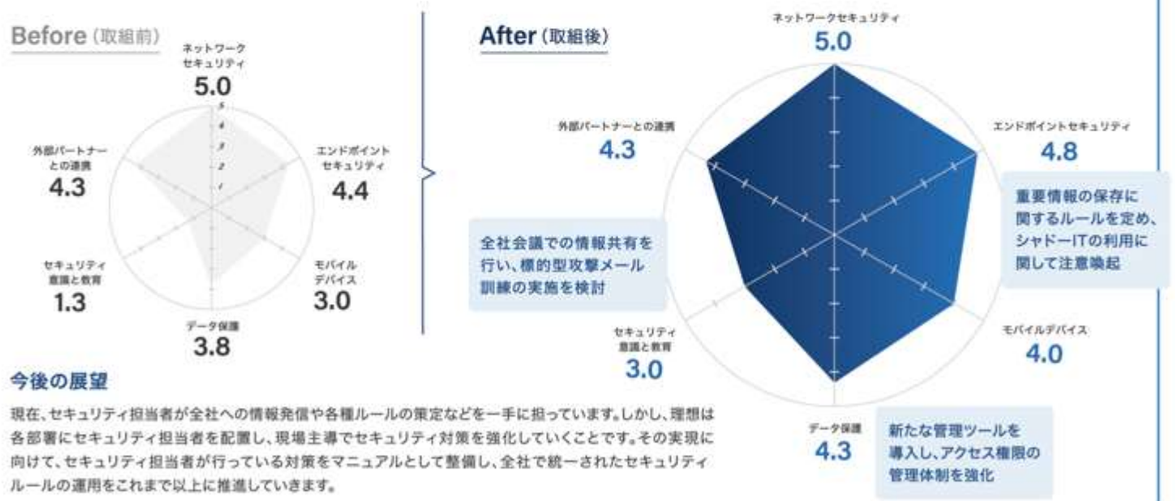
やむを得ず私用端末を使用する場合には事前申請を義務付け、MDM(※3)を活用したデバイスの管理を行い、EDR(※4)で脅威を検知するなど、セキュリティルールを定めました。また、シャドーITの危険性については、メールや月1回の全社会議を通じて注意喚起を行いました。

※1　企業の管理部門が把握していないIT機器やソフトウェア、クラウドサービスのこと　　※2　独立行政法人情報処理推進機構
※3　Mobile Device Management（モバイル端末を一元的に管理する仕組み）　　※4　Endpoint Detection and Response（端末のセキュリティ脅威を検知・分析・対応するセキュリティ技術）

結果と今後

1. 標的型攻撃メール訓練は、令和7年度に全従業員を対象に実施する予定で、予算の確保を進めています。従業員のセキュリティ意識には個人差があり、定期的な教育が必要です。今後も月1回の全社会議などを通じて、セキュリティに関する情報を発信していきます。　→　継続
2. 新たな管理ツールは、令和7年度中に導入する予定です。導入に向けて、アクセス権限の全体像を把握できたことで、統一的な管理体制構築の第一歩を踏み出しました。今後はPCのディスク暗号化にも取り組み、重要データの保護体制を強化します。　→　継続
3. 取組の結果、シャドーITの利用は減少しています。今後は、情報資産管理台帳を作成し、利用中の情報資産を把握します。また、退職者が利用していたアカウントの削除やPCの取扱いに関するチェックリストを作成し、管理外の資産が残らないよう徹底します。　→　継続

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連携



今後の展望

現在、セキュリティ担当者が全社への情報発信や各種ルールの策定などを一手に担っています。しかし、理想は各部署にセキュリティ担当者を配置し、現場主導でセキュリティ対策を強化していくことです。その実現に向けて、セキュリティ担当者が行っている対策をマニュアルとして整備し、全社で統一されたセキュリティルールの運用をこれまで以上に推進していきます。

経営層の声

本事業の専門家派遣を通して、自社のセキュリティ課題が明確になりました。従業員のセキュリティ意識の向上には時間を要しますが、現在の取組が数年後に成果として現れることを期待しています。今後も盤石な体制構築を進めるため、長期的な視野でセキュリティ対策を進めていきます。

参加者の声

本事業を通じて、自社のセキュリティ体制の現状を把握し、セキュリティ知識や対策を強化できたことは非常に有意義でした。また、経営層やマネージャーに判断を仰ぐだけでなく、まずは自分ができるセキュリティ対策から実践することが、セキュリティ強化の第一歩であると感じています。

卸売・小売

塗料販売業　F社

新設間もない情報システム課から始まる、ゼロからのセキュリティ管理体制の構築

企業プロフィール
- 業　　種：卸売業・小売業
- 従業員数：～100名

セキュリティ体制　1名体制/兼務

事業内容　塗料の専門商社として、自動車、建築機械、建材、建築向けの塗料を提案・販売しています。一般的な塗料に加え、電着、防腐、環境対策に優れた特殊塗料も提供しています。また、塗料事業から発展し、塗料関連の設備エンジニアリング事業も展開しています。

背景と課題

新設された情報システム課が社内のセキュリティ強化を担うことになりましたが、1人体制のため相談できる相手がおらず、不安を感じていました。

取組内容

本事業の専門家と協力して既存のセキュリティ対策を見直し、時代に即した対策を実行することで、全社のセキュリティレベルを向上させました。

結果と今後

自社に必要なセキュリティ対策をリスト化し、順次取り組んでいます。セキュリティポリシーとガイドラインの更新に際しては、実際のサイバー攻撃事例をもとに具体的な対策を組み込みました。今後も全従業員のセキュリティ意識を向上させるため、定期的な情報共有に努めます。

背景と課題

背景

新設された情報システム課は1人体制のため、セキュリティ対策の実行が難航

昨今の社会情勢を踏まえ、社内でセキュリティ対策を推進する機運が高まり、情報システム課が新設されました。しかし、担当者が一人しかおらず、専任でもなかったため、セキュリティ対策が思うように進みませんでした。さらに、社内に相談できる人がいないこともあり、本事業の専門家からのアドバイスが必要でした。

課題

1. セキュリティに関する知識が不足しているため、現行の対策が妥当かどうか判断できない
2. セキュリティポリシーやガイドラインが最新のセキュリティ動向に追いついていない
3. 経営層を含めた全従業員のセキュリティに対する知識が不足している

取組内容

取組1　本事業の専門家のアドバイスをもとに、自社で取り組むべきセキュリティ対策を抜本的に見直し

自社で取り組んでいるセキュリティ対策が事業規模や業務内容に適しているか判断できなかったため、本事業の専門家からアドバイスを受けました。現状を評価し、自社に必要なセキュリティ対策をリスト化して具体的なタスクに落とし込み、順次対応していきました。

取組2　本事業で提供された最新のサイバー攻撃事例をもとに、セキュリティポリシーとガイドラインを更新

古くなったセキュリティポリシーやIT利用に関するガイドラインを更新しました。本事業のセミナーやワークショップ、専門家から提供されたフォーマットをもとに、最近のサイバー攻撃事例を反映した内容にしました。

取組3　全従業員を対象に、セキュリティ知識の習得と意識向上を目的とした教育プログラムを実施

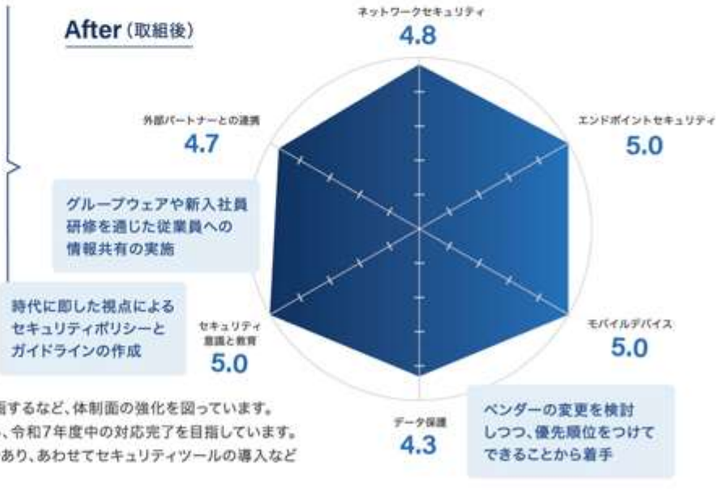
経営層を含めた全従業員のセキュリティ知識を向上させるべく、実際に発生した事例などを用いて教育、啓蒙の機会をつくりました。MDM(※1)の活用などの技術的対策と並行して、人的リスクを軽減する施策に取り組んでいます。

※1　Mobile Device Management（モバイル端末を一元的に管理する仕組み）

結果と今後

1. セキュリティ対策の見直しにあたり、ベンダーの変更から検討しました。しかし、大規模なサーバー環境の変更が必要となり、想定以上のコストがかかるため、計画自体を再検討しています。まずは、重要データの定期的なバックアップなど、できることから着手しています。　→ 継続
2. 作成したドキュメント類は、本事業の専門家によるチェックを受けて見直しを行いました。自社だけでは気づけなかった視点をセキュリティポリシーやガイドラインに加えられたのは大きな収穫です。今後も時代に即した内容となるよう、継続して更新に取り組みます。　→ 継続
3. セキュリティ知識向上のため、グループウェアでの情報共有や新入社員研修での教育を行いました。また、本事業の専門家から提供されたサイバー攻撃事例をもとに、経営層への説明の機会を設けました。今後も継続的に全従業員へのセキュリティ教育を予定しています。　→ 継続

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連携



今後の展望

経営層の理解を得ながら、セキュリティ対策の人員補強を計画するなど、体制面の強化を図っています。セキュリティポリシーやガイドラインの整備は継続的に実施し、令和7年度中の対応完了を目指しています。また、従業員へのセキュリティ教育も継続して展開する計画であり、あわせてセキュリティツールの導入など技術的な面の見直しも進めています。

経営層の声

本事業に参加することで、セキュリティの重要性が会社の信用問題にも関わる重大な課題であることを再認識しました。リソース面での支援を受けて対策を拡大し、経営層を含めた全従業員のセキュリティ意識と知識の向上を全社的な課題として取り組んでいきます。

参加者の声

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、同等規模の会社の担当者と交流する中で、自分では考えつかなかったセキュリティ対策やITツールを知ることができ、非常に有益でした。特に、セキュリティ対策の事例やフォーマットの提供は、自社の対策の効率化に役立っています。

卸売・小売

化粧品販売業　G社

オリジナル教材によるセキュリティ教育とテストを実施
従業員のセキュリティ意識の変化を実感

企業プロフィール
- 業　　種：卸売業・小売業
- 従業員数：～100名

セキュリティ体制　複数名体制/兼務

事業内容　化粧品や美容機器、サプリメントの卸売、通信販売を主な事業としています。自社でも化粧品、美容機器、サプリメントなど製品の開発を行い、医療機関やドラッグストアへの卸売事業と自社ECサイトや大規模事業のECサービスを利用した小売事業を展開しています。

背景と課題

情報セキュリティに対して全社的に危機意識が不足していると感じています。セキュリティ担当もリソースが不足しており、人材の育成が急務でした。

取組内容

オリジナル教材によるセキュリティ教育、情報資産管理台帳の再作成による重要情報の管理強化、ベンダーへのセキュリティ対策状況の把握を行いました。

結果と今後

従業員向けのセキュリティ教育と確認テストを実施した結果、従業員の意識に変化が見られています。
情報資産管理台帳を再作成し、社内に点在している重要情報を整理・評価して、管理の強化を図ります。
将来的なIPO(※1)を見据え、セキュリティ対策の強化と環境整備をさらに進めていきます。

背景と課題

背景

担当者不在時のインシデント対応やセキュリティに対する危機意識の薄さに不安がある

全社的にセキュリティへの危機意識の不足を感じています。
担当者不在時のインシデント対応方法も明確に定まっておりません。
ECサイトのセキュリティ対策はベンダーが主導しており、自社としても現状把握が必要です。また担当者が新任のため本事業に参加することで知識を習得したいと考えています。

課題

1. セキュリティ教育を行っていないため、従業員のセキュリティに関する危機意識が不足
2. 情報資産管理台帳の作成は数年前に着手したが、重要情報の区分が明確でないため見直しが必要
3. ECサイトやコーポレートサイトのセキュリティ対策状況の把握と対策強化を検討

取組内容

取組1　自社の業務とセキュリティ運用ルールに基づくオリジナル教材と確認テストを作成し、全社に展開

IPA(※2)が提供する動画や資料を参考に、自社の業務やセキュリティ運用ルールに合わせたオリジナル教材やそれに準拠した確認テスト（全10問）を作成しました。作成後、社内のイントラネットで従業員に共有しました。テスト結果のフィードバック方法も検討しています。

取組2　情報資産管理台帳の再作成と運用の見直しを行い、保護・管理するべき情報資産を明確化

数年前から情報資産管理台帳の作成に着手しております。IPAの提供する「リスク分析シート」を活用して、改めて情報資産の洗い出しと分類を行いました。これまで自社の重要情報の区分が不明確であったため、今回の見直しでは管理対象を広げて対応しています。

取組3　ECサイトのセキュリティ対策状況の把握と懸案となっていたバックアップ運用の見直し

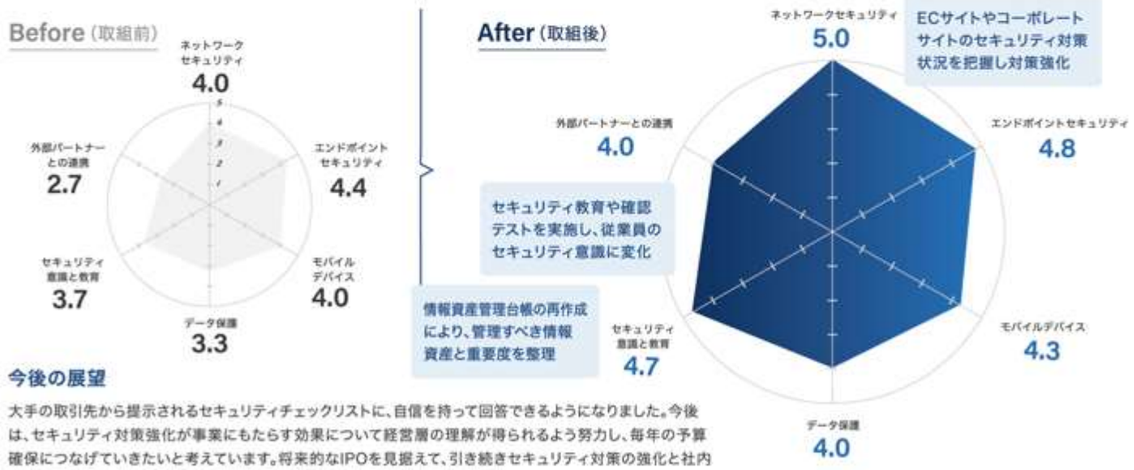
ECサイトを保守運用するベンダーに本サイトのセキュリティ対策について確認したところ、問題はありませんでした。一方懸案となっていたバックアップ運用については、技術的な対策を協議しながら、運用の安定性を向上させていきます。

※1　Initial Public Offering（新規株式公開）　※2　独立行政法人情報処理推進機構

結果と今後

1. オリジナル教材の作成により担当者自身の知識が向上しただけでなく、自社業務で特に注意すべき点が明確になりました。これまで実施していなかったセキュリティ教育ですが、最近はセキュリティに関する問い合せも増え、従業員の意識に変化が見られています。　→ 解決
2. 情報資産管理台帳の更新にあたり、まず自部門の台帳を整備し、その後順次他部門へ展開しました、最終的な更新はほぼ完了し、顧客情報や製品の成分情報など、重要な情報の保存場所が明確となりました。今後は各情報の重要度を評価し、適切に管理していきます。　→ 解決
3. ECサイトについては、過去に脆弱性診断を行い、問題がないことを確認していますが、今後は内部監査の対象となることも想定され、定期的な診断の実施を検討しています。現在再構築中のコーポレートサイトについても、リリース前に脆弱性診断を行う予定です。　→ 解決

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連携



今後の展望

大手の取引先から提示されるセキュリティチェックリストに、自信を持って回答できるようになりました。今後は、セキュリティ対策強化が事業にもたらす効果について経営層の理解が得られるよう努力し、毎年の予算確保につなげていきたいと考えています。将来的なIPOを見据えて、引き続きセキュリティ対策の強化と社内体制の整備を進め、ビジネス面でも良い影響を与えるように推進していきます。

経営層の声

本事業への参加をセキュリティ対策の妥当性の確認と担当者の知識向上の良い機会と捉えておりました。そのため、課題と対策、今後の計画立案に役立ち、有意義な経験でした。特に従業員のセキュリティ意識向上は、経営上のリスク対策として重要なポイントであり、経営層を含めて展開していきます。

参加者の声

本事業への参加により、ITリテラシーを高めセキュリティ知識を習得することができました。また、第三者の視点から評価を受け、自社のセキュリティ対策を見直す良い機会になったと考えています。ワークショップで行った情報資産管理台帳の作成は、自社の対策強化に直結し、非常に参考になりました。

卸売・小売

オフィス機器製造販売業 H社

「効率的にセキュリティ施策を展開できるロードマップ」を作成し優先順位の可視化を実現

企業プロフィール
- 業　　種：卸売業・小売業
- 従業員数：～100名

セキュリティ体制　複数名体制/兼務

事業内容　オフィス家具を中心にEC事業、卸販売を展開し、自社でデザイン設計から製造、品質管理まで一貫して行っています。日本の繊細さと海外の斬新さを融合した商品開発に注力し、顧客ニーズを反映した製品を生産しています。国内外にOEM工場を持ち、徹底した品質管理が特徴です。

背景と課題

情報システム部門では多くのセキュリティ課題を認識しているものの、リソース不足や優先順位の未設定などにより、順調に進められていない状況でした。

取組内容

セキュリティロードマップの作成により優先順位の可視化を行い、クラウドサービスのアカウント管理の整理および権限付与について協議しました。

結果と今後

クラウドサービスのアカウントの現状を把握して、追加が必要な個人アカウントを洗い出しました。今後はルールに基づいてアカウントを付与し、適切なアクセスレベルの設定を行います。また、Wi-Fiの冗長化や切り分けを行うとともに、将来に向けたセキュリティ施策の優先度を設定していきます。

背景と課題

背景

アカウント管理や権限付与など基本的なセキュリティ対策に不安を抱えている

社内で取り組むべきセキュリティ課題は認識しているものの、日々の業務に追われ、未着手の項目が多々あります。新社屋移転に伴うネットワーク再構築も並行して行っていますが、アカウント管理や権限付与など基本的な課題が未解決で、セキュリティ教育の整備やアクセス管理の強化も課題です。

課題

1. 担当者のセキュリティ知識不足により、課題の洗い出しと優先順位づけができていない
2. 目標に掲げたセキュリティ水準に達しておらず、ネットワーク強化が進んでいない
3. アカウントの管理が不適切で、アクセス権限の適正な管理・運用ができていない

取組内容

取組1　本事業の専門家のアドバイスをもとにしたセキュリティロードマップの作成

社内にセキュリティの知見が蓄積されておらず、人的・金銭的リソースにも限りがあったため、まずは本事業の専門家とともに、セキュリティ対策を効率よく進めるためのロードマップを作成しました。その後、タスクの細分化や優先順位の明確化を進める取組を行いました。

取組2　IPO(※1)企業と同等のセキュリティ水準を目指し、新社屋移転を機にネットワーク強化を推進

新社屋への移転に伴い、移転前よりもセキュリティを強化する必要があると考え、技術的な対策を検討しました。特に、ネットワークの冗長化やWi-Fi環境の見直しを計画し、将来的なIPOを見据えた高度なセキュリティ水準を確保することを目指しました。

取組3　アカウント管理の見直しや適切な権限付与のため、ライセンスとその利用状況を整理

契約中の一部のクラウドサービスでは、複数の従業員で1つのアカウントを共有していました。そのため、ライセンスと従業員の利用状況を整理して可視化する取組を行いました。また、アクセス権限が適切に管理されていなかったため、ルールに基づく権限の割り当て方を設定します。

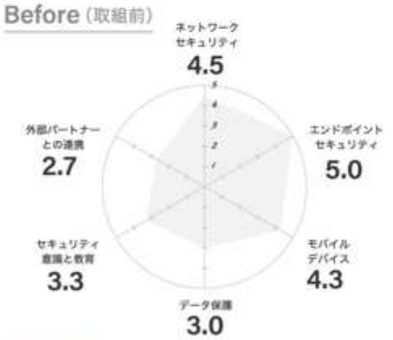
※1　Initial Public Offering(新規株式公開)

結果と今後

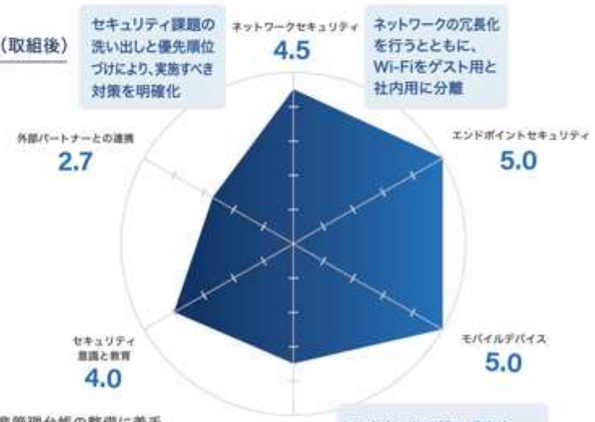
1. 本事業の専門家とともに、従業員教育やインシデント対応、クラウドサービスのセキュリティ対策などのタスクを細かく洗い出し、それぞれの優先順位を明確化しました。今後は作成したロードマップに沿って、優先度の高いタスクから段階的に実施していきます。　→ 継続
2. Wi-Fiのアクセスポイントを2箇所に増設し、ゲスト用と社内用の接続を物理的に切り分け、ゲストが社内のネットワークに侵入できないような仕組みを構築しました。これにより外部からの侵入リスクの低減と通信速度の安定性を向上させることができました。　→ 解決
3. 社内の利用状況を明確化しました。これを受け、全従業員に1人1つのアカウントを付与するために必要な予算を計算し、適切なアカウント利用体制の確立を進めています。また、各業務に応じた適切なアクセスレベルを設定する仕組みを導入予定です。　→ 継続

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連携

Before（取組前）



After（取組後）



セキュリティ課題の洗い出しと優先順位づけにより、実施すべき対策を明確化

ネットワークの冗長化を行うとともに、Wi-Fiをゲスト用と社内用に分離

アカウントの洗い出しとアクセス状況の明確化により、不正利用リスクを低減

今後の展望

アクセス権限を適切に付与するため、今後はセキュリティ対策の基盤となる情報資産管理台帳の整備に着手します。また、本事業の専門家からのアドバイスを受け、やるべきことが明確になりました。これにより課題に優先順位をつけ、着手しやすい粒度までタスクを分解することで、リソース不足を補いながら継続的に対策を進めます。IPOの基準に適合したセキュリティレベルの実現を目指します。

経営層の声

社内でセキュリティ担当者を育成するのは容易ではないため、本事業を通じて専門知識を一から学び、人材を育成できたことは非常に有意義でした。また、本事業への参加を契機に、セキュリティ対策を一層強化することができました。今後もさらなる対策を少しずつ実行に移し、効果的な体制を構築します。

参加者の声

セミナー講師の説明が毎回わかりやすく、フィッシング被害に関連する最新の手口など、トレンドを押さえた情報を得ることができ、非常に有益でした。ワークショップでは他社のセキュリティ担当者の方とも情報交換することができました。今回の経験を活かして社内のセキュリティを一層強化していきます。

卸売・小売

アパレル用品製造販売業　I社

関連会社のランサムウェア被害により対策が加速、多層防御で自社のインシデント発生に備える

企業プロフィール
- 業　　種：卸売業・小売業
- 従業員数：～300名

セキュリティ体制　1名体制/兼務

事業内容　ウィメンズ・メンズウエアや服飾雑貨、アクセサリーなどの企画、生産、販売、卸売を行っています。ものづくり、買い付け、販売、店舗表現までをすべて自分たちで手掛けており、オリジナルブランドショップからセレクトショップ、飲食店の経営にも携わっています。

背景と課題

関連会社がランサムウェアの被害を受け、自社のセキュリティ対策を見直しました。しかし、知識不足から必要な対策がわかりませんでした。

取組内容

セキュリティポリシーの作成、インシデント発生時の対応マニュアルの整備に取り組みました。また、詳細なネットワーク構成図の作成を行いました。

結果と今後

業務運用に適したセキュリティ関連規程を作成しました。その上で、最低限守るべきルールを従業員に教育し、セキュリティリテラシーの向上を図ります。また、詳細なネットワーク構成図の完成により、ネットワークセキュリティの強化も進みました。引き続き、セキュリティ管理体制の強化を目指します。

背景と課題

背景

関連会社がランサムウェア被害を受け、本格的なセキュリティ対策強化が急務に

本格的なセキュリティ対策は行っておらず、セキュリティ担当者も不在でした。そのような中、関連会社がランサムウェアの被害を受け、業務が一時停止しました。それを契機に、経営層からセキュリティ対策の強化を指示され、EDR(※1)を導入しましたが、それ以上にどのような対策が必要かわかりませんでした。

課題

1. セキュリティポリシーの作成を進めていたが、簡易的な内容であるため見直しが必要
2. ネットワーク構成図には、各拠点間の関連図しか記載がなく、詳しい状況の把握が困難
3. 実際のインシデント発生時に、どのような対応をすべきか決まっていない

取組内容

取組1　簡易的だったセキュリティポリシーを自社の業務運用に則した内容に見直し

簡易的なセキュリティポリシーは作成済みですが、自社の業務運用には合っていませんでした。そのため、IPA(※2)が提供する「情報セキュリティ関連規程」を参考に、自社に合った内容に見直し、原案を作成しました。本事業の専門家と確認しながら、修正作業を行っています。

取組2　本事業の専門家からアドバイスを受け、ベンダーと協力し詳細なネットワーク構成図を作成

本事業の専門家から、ネットワークトラブル発生時の早期復旧には、ネットワーク構成図が必要とアドバイスを受け、ベンダーと協力し作成を進めました。ベンダーが作成した拠点間の構成図に加え、社内のネットワーク環境を反映させた詳細な構成図の完成を目指しています。

取組3　インデント発生時の対応方針を策定、具体的な行動マニュアルを作成し運用を目指す

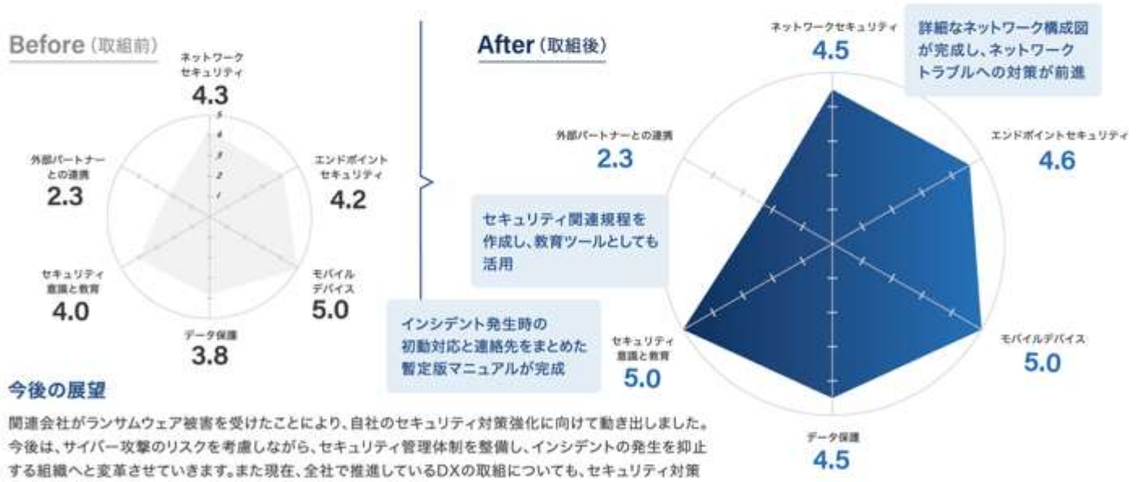
インシデント発生時の対応方針を策定し、具体的な対応フローを作成しています。インシデントの一次発見者がどこに連絡するか、初動対応として何を実施するか（例：PCのLANケーブルを抜線、フルスキャンを実施）を具体的に文書化しています。

※1　Endpoint Detection and Response（端末のセキュリティ脅威を検知・分析・対応するセキュリティ技術）　※2　独立行政法人情報処理推進機構

結果と今後

1. セキュリティ関連規程が完成し、セキュリティ体制強化に向けた基盤が整いました。その内容を従業員が最低限守るべきルールとして、教育を行いました。セキュリティリテラシーは、業務や従業員によって個人差があり、教育を通じて全体的な底上げを図ります。　→　解決
2. ネットワーク構成図が完成し、インシデントやネットワークトラブルへの対策が前進しました。一方で、現在導入している複数のエンドポイントセキュリティツールの管理が煩雑という課題が明らかになりました。令和7年度以降、ツールの見直しを予定しています。　→　継続
3. これまで文書化されていなかったインシデント発生時の対応について、具体的な対応方針が決まり、暫定版マニュアルが完成しました。組織的対策、人的対策、技術的対策の多層防御による対応フローの整備を進め、セキュリティ管理体制を強化していきます。　→　継続

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連携



今後の展望

関連会社がランサムウェア被害を受けたことにより、自社のセキュリティ対策強化に向けて動き出しました。今後は、サイバー攻撃のリスクを考慮しながら、セキュリティ管理体制を整備し、インシデントの発生を抑止する組織へと変革させていきます。また現在、全社で推進しているDXの取組についても、セキュリティ対策の進捗を確認しながら、バランスよく両輪で進めていく予定です。

経営層の声

漠然とセキュリティ対策を行うべきだと考えていましたが、社内にセキュリティの有識者がおらず悩んでいました。本事業の専門家からアドバイスを受けたことで、自社が具体的に取るべき対策について知見を得ることができました。今後は自社のセキュリティ対策をより加速させようと決意を新たにしました。

参加者の声

本事業に参加したことで、セキュリティに関する多くの知識が得られました。セミナー・ワークショップでは、他社のセキュリティ担当者と意見交換し、切磋琢磨できた点も大きな収穫でした。事業参加後の成果として報告書を作成し、社内で学びを共有しました。今後もセキュリティ対策を強化していきます。

卸売・小売

繊維・化成品製造販売業　J社

ランサムウェア被害をきっかけにセキュリティ対策を強化、各拠点の推進リーダによる強化を推進

企業プロフィール
- 業　　種：卸売業・小売業
- 従業員数：～300名

セキュリティ体制　1名体制/専任

事業内容　繊維事業や化成品事業などを取扱う専門商社です。繊維事業では繊維素材の企画・開発からメーカーへの資材提供など、化成品事業では高機能シリコーンゴムロールの設計や開発を行っています。さらに産業分野から生活雑貨まで活用できる、ゴム・エラストマー素材も手掛けています。

背景と課題

ランサムウェア被害の経験からUTM(※1)などのセキュリティ機器は導入していたものの、費用面とセキュリティ対策の両立に課題を感じていました。

取組内容

NAS(※2)活用やIT担当設置、ガイドブック作成を行いました。また、サイバーセキュリティ対策促進助成金(※3、以下助成金)を申請しました。

結果と今後

各拠点のセキュリティ推進リーダとしてIT担当者を設置したことで、新たに作成したセキュリティガイドラインの浸透やセキュリティ対策の徹底が進んでいます。バックアップ運用の見直しやUTMの入替の検討などの技術的な対策強化も進めており、セキュリティ対策を大きく前進させることができました。

背景と課題

背景

関係会社がランサムウェアの被害を受け、セキュリティ対策強化の必要性に迫られている

ランサムウェアの被害を受け、セキュリティ対策の強化が急務となっていました。セキュリティポリシーは作成済ですが、まだ運用には至っていません。また、従業員のセキュリティ意識が低いため、全社的な意識の向上が必要です。さらに、バックアップの見直しやUTMの入替など、具体的な課題も山積みでした。

課題

1. バックアップの運用ルールが確立していないため、データ量の増加や復旧時間に懸念
2. セキュリティ対策を全従業員に徹底させるための社内体制が整備されていない
3. セキュリティ対策の基本的なルールが定められておらず、全従業員の認識レベルが不安

取組内容

取組1　サーバのデータバックアップ運用を見直し、保存領域の確保や復旧時間の短縮を実現

サイバー攻撃を受けた場合の復旧時間を短縮するためには、バックアップ運用の見直しが重要だと、本事業の専門家からアドバイスを受けました。そのため、NASにバックアップを行い、バックアップサーバには全社共通のデータのみを保存する運用を確立しました。

取組2　セキュリティ対策を推進するIT担当者を各拠点に設置し、確実なセキュリティ対策への取組を目指す

全従業員がセキュリティ対策を確実に取り組むために、セキュリティ対策の推進リーダとしてIT担当者（他業務と兼務）を各拠点に設置しました。マニュアルを渡して従業員に任せきりにするのではなく、IT担当者が業務の中で具体的なセキュリティ対策の方法を指導しています。

取組3　セキュリティガイドブックを作成し従業員に配布、UTM入替のための助成金申請の準備を進める

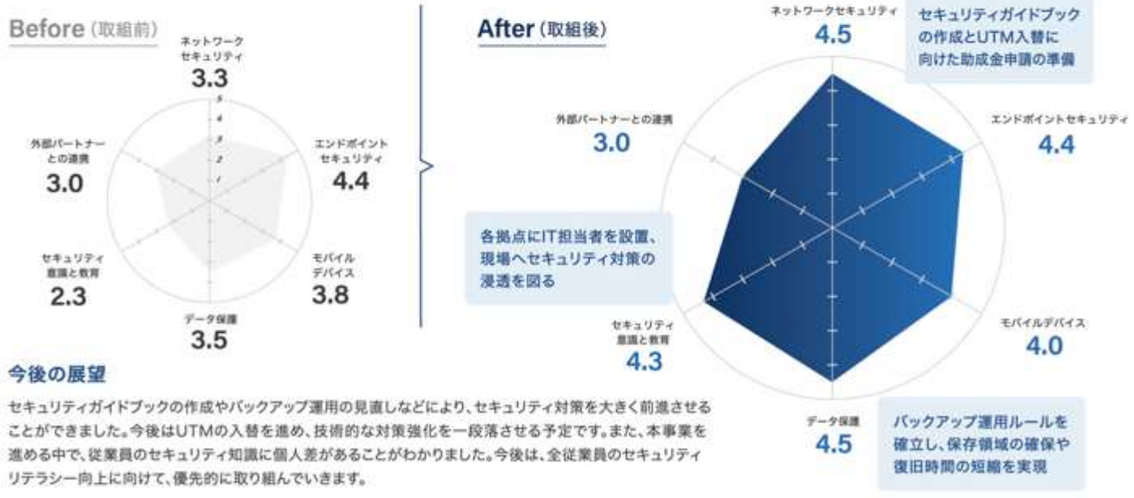
IPA(※4)の「中小企業の情報セキュリティ対策ガイドライン」をもとに、業務に活用するセキュリティガイドブックを作成し、従業員に配布しました。また、「情報セキュリティ基本方針」をWebサイトに掲載し、「SECURITY ACTION（二つ星）」を宣言しました。

※1　Unified Threat Management 統合脅威管理（複数のセキュリティ機能を統合した管理システム）　※2　Network Attached Storage（ネットワークに接続された記憶装置）
※3　公益財団法人東京都中小企業振興公社 サイバーセキュリティ対策促進助成金　※4　独立行政法人情報処理推進機構

結果と今後

1. これまで個人任せとなっていたバックアップの運用ルールを確立し、バックアップデータの保存領域の整理とデータ量の削減が実現しました。一方で、サーバ内には長い期間使用されていないデータが多く存在しており、これらの整理が新たな課題となりました。　→　解決
2. IT担当者は、バックアップ方法やパスワードの強化対策についても、各拠点の従業員に説明しています。この体制でPCのOS入替作業を行いましたが、特に問題なく完了しました。今後は、セキュリティに関する啓蒙活動も担当してもらう予定です。　→　解決
3. ネットワークセキュリティの強化のために、助成金を活用したUTMの入替を検討しています。本事業の専門家に、今回の取組で助成金申請に必要な要件が満たされたことを確認するとともに、申請書の具体的な記入項目についてもアドバイスを受けました。　→　解決

取り組んだ支援テーマ：ネットワークセキュリティ／データ保護／セキュリティ意識と教育



今後の展望

セキュリティガイドブックの作成やバックアップ運用の見直しなどにより、セキュリティ対策を大きく前進させることができました。今後はUTMの入替を進め、技術的な対策強化を一段落させる予定です。また、本事業を進める中で、従業員のセキュリティ知識に個人差があることがわかりました。今後は、全従業員のセキュリティリテラシー向上に向けて、優先的に取り組んでいきます。

経営層の声

本事業に参加した報告を受け、従業員のセキュリティ意識の向上が最も重要だと感じました。どれほど知識やノウハウがあっても、各自がセキュリティ意識を持たなければ意味がありません。そのため、今後は経営層を含む全従業員に対し、実際の被害やリスクを理解してもらうための取組を行います。

参加者の声

本事業のセミナーや専門家のアドバイスを受け、継続的に学ぶことの重要性を改めて実感しました。自分自身の知識レベルとしては十分足りていると思っていましたが、まだ学ぶべき内容が多いことを認識させられました。令和6年をセキュリティ対策強化の元年として、取組を継続していきます。

建設・製造

システム機器製造業　A社

医療業界からの高まるセキュリティ要求に対し、「技術」・「組織」両面の対策強化で安全性を確保

企業プロフィール
- 業　　種：製造業
- 従業員数：～5名

セキュリティ体制　複数名体制/兼務/経営者

事業内容　医療事務機器の製造、販売、運用保守を行う企業です。ソフトウェアとハードウェアを組み合わせた受付業務の効率化システムを提供し、医療現場の事務的負担を軽減するとともに、患者様のスムーズな受診を支援しています。

背景と課題

主要な取引先である医療業界のセキュリティ要求が高まる中、自社の対策が十分であるか、また、どの程度対応できるのか、不安を感じていました。

取組内容

セキュリティポリシー更新と現場の運用ルールとの関連付け、バックアップ運用の見直し、UTM(※1)の追加導入、ディスク暗号化などを行いました。

結果と今後

セキュリティポリシーの更新により、従業員の意識が向上しました。また、バックアップ運用の見直しやリモート接続のセキュリティ強化を行い、取引先のセキュリティ要求にも自信を持って対応できる体制を整えました。将来的には、ISMS認証の取得も視野に入れ、セキュリティ対策の強化に努めます。

背景と課題

背景

医療業界でのセキュリティ要求が格段に高度化し、自社のセキュリティ対策に不安

近年のサイバー攻撃の事例を受けて、主な取引先である医療業界のセキュリティ要求が高まっており、自社のセキュリティ対策に対して不安に感じていました。また、万が一サイバー攻撃を受けた場合でも、取引先の業務が止まらないようなセキュリティ対策が必要であると強く認識するようになりました。

課題

1. セキュリティポリシーを更新できておらず、日々の業務で留意すべきルールが曖昧
2. 社内データへのセキュリティ体制が脆弱なため、インシデント発生時の対応に不安
3. 保守メンテナンス用ネットワークにはUTMが未導入で、事業運営の安全性に不安あり

取組内容

取組1　セキュリティポリシーを更新、現場の運用ルールと関連付けることで社内への浸透を図る

IPA(※2)が提供する「中小企業の情報セキュリティ対策ガイドライン」などの資料を参考にして、セキュリティポリシーを更新しました。また、具体的なセキュリティ運用ルールと関連付けて整理し、社内のセキュリティ教育の基本となる内容を目指しました。

取組2　現行のデータバックアップの運用を見直し、多層的なセキュリティ対策を実施

これまで手動で行っていたデータのバックアップを、週2回自動で実施することにしました。また、バックアップデータの保存先をネットワークから切り離した場所にも確保しました。万が一サイバー攻撃を受けても業務に支障が出ないよう、多層的なセキュリティ対策を講じています。

取組3　保守メンテナンス用ネットワークにもUTMを導入し、リモート接続におけるセキュリティを確保

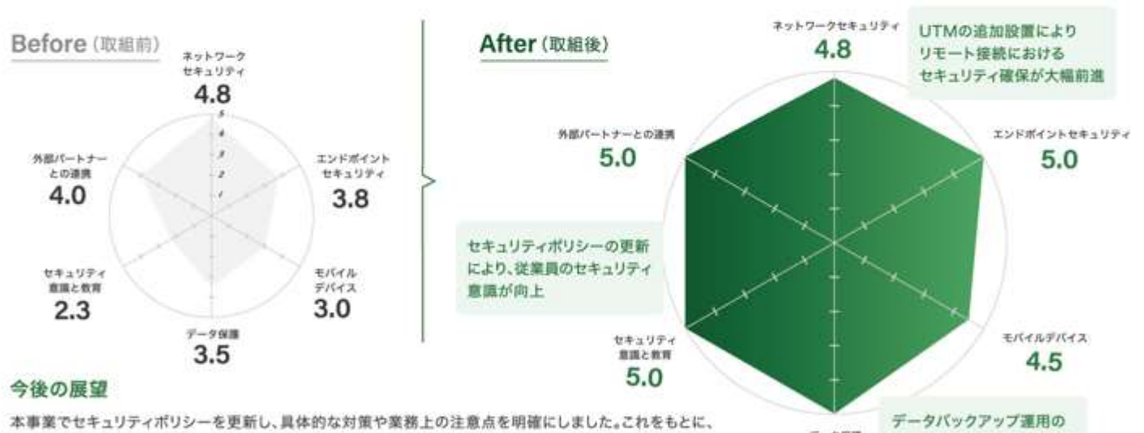
本事業の専門家にアドバイスを受け、保守メンテナンス用ネットワークにもUTMを導入しました。また、デバイスのディスク暗号化やスマートフォンへの生体認証も適用しました。これにより、社外から保守メンテナンスを行う際もセキュリティを確保でき、事業の安全性を高めました。

※1　Unified Threat Management 統合脅威管理（複数のセキュリティ機能を統合した管理システム）　※2　独立行政法人情報処理推進機構

結果と今後

1. セキュリティポリシーを自社のWebサイトに掲載し、社外にも公開しています。これにより、従業員は守るべき事項が明確になり、日々の業務でのセキュリティ対策の根拠として、セキュリティ意識の向上に役立っています。今後も定期的に更新を行う予定です。　→　解決
2. 多層的なデータバックアップの体制を整備したことにより、事業の安定性と取引先からの信頼感を確保できたと考えています。また、バックアップ体制が確立されたことにより、インシデント発生時の報告手順や対応体制についても定めることができました。　→　解決
3. リモート接続のセキュリティ対策を強化したことで、事業をより安定して運営できるようになりました。また、取引先からセキュリティ対策の調査があった場合でも、自信を持って対応ができると考えています。今後とも、対策を定期的に見直していきます。　→　解決

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連携



今後の展望

本事業でセキュリティポリシーを更新し、具体的な対策や業務上の注意点を明確にしました。これをもとに、従業員へのセキュリティ教育を行い、意識の向上を図ります。また、整備したドキュメントや規程類を活用して、将来的にはISMS認証の取得にも取り組む予定です。今後も取引先から定期的にセキュリティ対策状況の調査が行われるため、引き続きセキュリティ強化に務めます。

経営層としての声

本事業を通じて、自社のセキュリティ対策に対する認識の曖昧さを解消し、確信を持ってセキュリティ対策を進めることができています。また、これまで進められなかった文書の更新やインシデント発生時の対応についても、本事業の専門家の支援により取り組むことができ、大きな成果だと考えています。

参加者としての声

本事業の専門家の支援により、これまで漠然としていたセキュリティ対策が明確になりました。また、技術的な対策強化が必要なことはもちろんですが、それ以上に従業員のセキュリティ意識の向上が重要だと実感しました。また、他社のセキュリティ担当者との情報交換ができたことも、非常に有意義でした。

建設・製造

管工事業　B社

前任者が構築したセキュリティ対策を総点検 事業参加により知識が向上し体制強化に向け前進

企業プロフィール
- 業　　種：建設業
- 従業員数：～20名

セキュリティ体制　1名体制/兼務

事業内容　東京都内、多摩地域を中心に建築設備工事の施工管理を行っています。水回り工事や給排水・衛生設備工事、空調換気設備を専門とし、水漏れや排水口詰まり等のリフォーム・改修工事も対応しています。地域とのつながりを大切にしながら、お客様の快適な住環境をサポートしています。

背景と課題
自社システムの現状を前任者から引き継ぐことができず、知識や予算などのリソースが限られる中、セキュリティ体制をどう整備していくかが課題でした。

取組内容
情報資産を把握する手法およびバックアップ方法を検討しました。また、既存の対策状況を精査し、EDR(※1)の導入を検討しました。

結果と今後
情報資産管理台帳を作成することにより情報資産を可視化し、運用ルールも検討しました。また、EDRの導入を正式決定し、サービスも選定できたため、令和7年度の導入を目指して準備を進めています。さらに、バックアップ方式をクラウド環境へ移行する方針を固めました。

背景と課題

背景

社内のシステムや情報資産を把握しきれておらず、必要なセキュリティ対策が不明瞭

前任の担当者が休職後に業務を引き継いだため、セキュリティ体制を十分に把握できておらず、現担当者はセキュリティ知識を学びながら手探りで対応している状況でした。EDR未導入や情報資産管理台帳の未整備、インシデント発生時の対応フローが決まっていないなど、多くの課題が残されていました。

課題

1. 自社の情報資産について把握しておらず、データ管理の運用方法も決まっていない
2. 導入しているシステムを把握できていない上、コストに見合う最適な対策がわからない
3. 万が一のインシデント発生への備えが不十分であり、バックアップ方式の再検討が必要

取組内容

取組1　情報資産管理台帳を作成することにより自社の情報資産を可視化しつつ、運用ルールを策定

IPA(※2)のリスク分析シートを参考にして、情報資産管理台帳を作成しました。これにより、自社が保有する情報資産が可視化され、重要情報のリスクアセスメントが可能となりました。また、この取組をきっかけにデータの管理方法や運用体制の見直しをする予定です。

取組2　コスト面と機能面を考慮しつつ、ベンダーと協議を重ねEDRの導入を検討

本事業の専門家派遣後、EDRが未導入であることが判明しました。そこで、エンドポイントセキュリティを強化するため、EDRの導入を決定しました。コスト面と機能面のバランスが取れた、自社の事業規模に合ったEDRサービスをベンダーと連携し、検討を進めています。

取組3　自社のバックアップ方式を見直し、万が一のインシデント発生にも耐えられる体制構築を推進

社内サーバに保存しているデータの種類や取得頻度、バックアップ先について、現状のバックアップ方式における課題を洗い出し、今後の運用についてより堅牢で効率的な方法を模索しました。インシデント発生時にも迅速にデータを復元できる体制の構築を目指します。

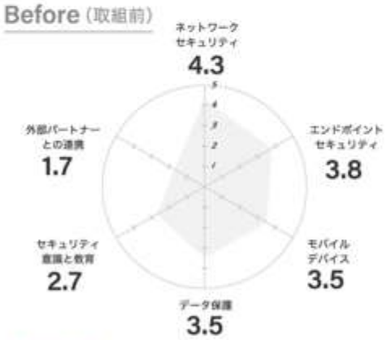
※1　Endpoint Detection and Response(端末のセキュリティ脅威を検知・分析・対応するセキュリティ技術)　※2　独立行政法人情報処理推進機構

結果と今後

1. 情報資産管理台帳を完成させたことで、リスク管理の基盤が整いました。今後はリスクの「低減」や「回避」などの方策を講じて、情報資産のリスクマネジメントを行います。また、情報資産ごとの運用方法についてドキュメント化することを予定しています。　→ 解決
2. 自社に合ったEDRサービスを絞り込むことができました。令和7年度の導入に向けて、ベンダーと詳細の運用方法や設定について協議を行っています。また、この機会に導入済みの他のセキュリティ対策についてもベンダーと話し合い、再検討していきます。　→ 継続
3. 現在、バックアップ方式はオンプレミスを採用していますが、本事業をきっかけにバックアップ方式をクラウドに変更することを検討しています。今後は、クラウドサービスの選定を進めつつ、バックアップデータの対象範囲や運用ルールを定めていく予定です。　→ 継続

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連携

Before（取組前）



After（取組後）

IPAのリスク分析シートを参考にしながら、情報資産管理台帳を作成

導入するEDRを選定しつつ、ベンダーとの協力関係を築く

クラウドサービスを選定するとともに、バックアップデータの対象範囲を検討

今後の展望
自社のセキュリティ運用ルールを従業員が遵守するためには教育やルールの簡素化を適じた歩み寄りが必要だと考えています。業務上必要なクラウドサービスについてはWebフィルタリングの利用を検討し、対策が業務の負担とならないよう工夫していきます。さらに、生成AIの利活用を社内で進めるため、利用範囲の制限やデータの漏えい防止を含めた運用ルールを確立していきます。

経営層の声

今回の事業を適じて、情報資産管理台帳の作成やシステム対策の見直しといった具体的な成果が出たことを嬉しく思っています。作成したドキュメントを本格運用することになり、いよいよ実行のフェーズに入ります。今後も対策を進めて、組織全体でセキュリティレベルを高めていきたいと考えています。

参加者の声

セキュリティ対策について専門用語も含め、体系的に学べたことが一番の収穫でした。ベンダーと対等に話ができるレベルまで成長できたと実感しています。今後は、経営者も加えた全従業員がセキュリティ対策への足並みを揃えつつ業務効率化も実現し、盤石なセキュリティ管理体制を構築してまいります。

建設・製造

精密機器製造業　C社

古いOSのPC利用や従業員の意識の課題を解消、特許を扱う企業としてセキュリティ強化を加速

企業プロフィール
- 業　　種：製造業
- 従業員数：～50名

セキュリティ体制　1名体制/専任

事業内容　特殊なレーザーを用いた測定機器を開発しており、自動車部品の検査に広く使われています。複雑な形状の部品を高速で検査できる技術を駆使して、自動車部品などで多い中型・大型の部品の検査を容易にしています。また、センサーや検査装置に加え、ソフトウェアも販売しています。

背景と課題

過去にフィッシングメールの被害を受けたものの、PCのパスワードを何年も変更しないなどセキュリティ対策の重要性が理解されていませんでした。

取組内容

標的型メール訓練を計画し、ネットワークセキュリティ強化のためのツールを導入しました。また、OSが未更新のPCに対する対策にも取り組みました。

結果と今後

セキュリティ教育は従業員のレベルに合わせて行い、意識と知識の両面で強化を図る予定です。
また、ネットワークセキュリティの強化により、外部からの攻撃に備え、重要情報を守るセキュリティ体制が整いつつあります。今後も費用対効果を考慮しながら、最適な対策を検討していきます。

背景と課題

背景

インシデント発生によりセキュリティ対策強化が求められるが、従業員の意識が低い

パスワードの変更を10年以上行っていない従業員がいるなど、セキュリティ意識の低さが課題でした。また、過去にはフィッシングメールによって情報漏えいが発生しているものの、ウイルスの侵入に気づかない状況でした。そのため、経営層の理解を得ながら、全社的にセキュリティ対策を強化する必要がありました。

課題

1. 過去にフィッシングメールの被害を受けたものの、従業員のセキュリティ意識が低い
2. ネットワークの監視体制が不十分で、アカウント管理や拠点間通信のセキュリティに不安
3. 古いOSのPCやウイルス対策ソフトウェアが未更新のPCがあり、脆弱性に懸念あり

取組内容

取組1　定期的なセキュリティチェックと標的型攻撃メール訓練を行い、セキュリティ意識の向上を図る

過去に自社の従業員がフィッシングメールの被害を受け、情報漏えいが発生した経験を踏まえ、全従業員が定期的に行うセキュリティのセルフチェックリストを配布しました。また、令和7年中に、全従業員を対象とした標的型攻撃メール訓練を実施する計画を立てました。

取組2　SSO(※1)やVPN(※2)の導入でネットワークセキュリティを強化、外部からの攻撃を防御

アカウント管理やパスワード保護の強化のため、SSOの導入についてベンダーと協議しています。また、UTM(※3)から転送されるログの確認方法を把握し、監視体制の改善に取り組みました。さらに、拠点間通信のセキュリティ強化のため、VPNの導入を決定しました。

取組3　古いOSのPCをネットワークから切り離し、最新のウイルス対策ソフトウェアをインストール

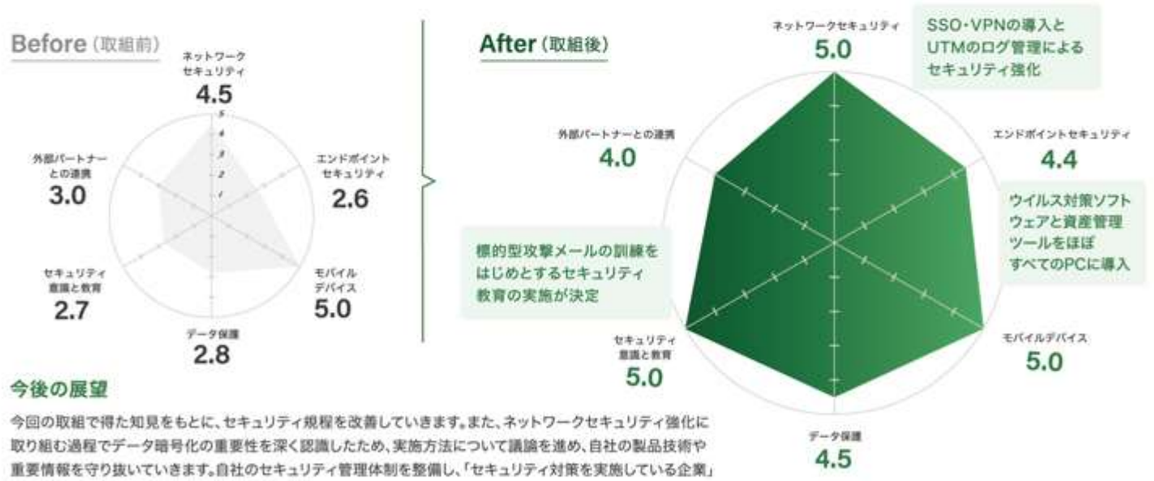
まず、セキュリティ上の安全を確保するため、古いバージョンのOSを使用しているPCをネットワークから切り離し、最新のウイルス対策ソフトウェアをインストールしました。また、全社的なOSのバージョン管理を効率化するため、資産管理ツールの導入を進めました。

※1　Single Sign On(一度のユーザー認証で複数のシステムやサービスを利用できる仕組み)　※2　Virtual Private Network(仮想専用通信網)
※3　Unified Threat Management 統合脅威管理(複数のセキュリティ機能を統合した管理システム)　※4　Endpoint Detection and Response(端末のセキュリティ脅威を検知・分析・対応するセキュリティ技術)

結果と今後

1. 標的型攻撃メール訓練を委託するベンダーの選定を行いました。また、訓練を実施した後に結果を分析し、自社のセキュリティ意識における課題を把握します。テスト結果に基づき、問題をカスタマイズするなど、自社の課題に合ったセキュリティ教育を行います。　→ 継続
2. UTMのログは必要に応じてベンダーから提供を受ける体制が整いました。これにより、インシデント発生時には迅速に原因の調査ができます。今後は、ドメインセキュリティサービスの導入を検討し、アクセス管理やメールセキュリティの強化を進めていきます。　→ 継続
3. ウイルス対策ソフトウェアに加え、資産管理ツールをほぼすべてのPCに導入したため、社内のIT資産の一元管理が可能となりました。これを受け、エンドポイントセキュリティをより強化するため、EDR(※4)の導入について本格的に議論を進める予定です。　→ 解決

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連携



今後の展望

今回の取組で得た知見をもとに、セキュリティ規程を改善していきます。また、ネットワークセキュリティ強化に取り組む過程でデータ暗号化の重要性を深く認識したため、実施方法について議論を進め、自社の製品技術や重要情報を守り抜いていきます。自社のセキュリティ管理体制を整備し、「セキュリティ対策を実施している企業」としての信頼を築いていきたいと考えています。

経営層の声

本事業への参加により、自社のセキュリティ対策を見直すことができました。また、最新のセキュリティ動向を把握できた点も非常に有益でした。特許を扱う企業として、ハッキングや情報漏えいといったリスクを少しでも減らしていくために、今後さらにセキュリティ対策を強化していきます。

参加者の声

取組を通じて、従業員の業務効率も考慮しながら、セキュリティに対する意識を適切に把握することの重要性を実感しました。現場の負担を最小限に抑えながら、自社に最適な対策を講じていきます。また、今後は、社内の情報資産を重要度に応じて整理し、より効果的なセキュリティ対策を進めていきます。

建設・製造

印刷業　D社

個人情報や機密情報を多く取扱う印刷業として、全社を巻き込んだ意識改革と体制強化を断行

企業プロフィール
- 業　　種：製造業
- 従業員数：～50名

セキュリティ体制　1名体制/兼務

事業内容　小ロット印刷、デジタルオンデマンド印刷、パッケージ制作、スキャニングサービスなど、多彩なソリューションを提供する印刷会社です。また、販促ツールの制作やカスタマイズにも強みを持ち、製本やアッセンブリまでシームレスに対応しています。

背景と課題

取引先からセキュリティ対策に対する要求が年々高まる中、セキュリティ対策の更新と全社的なセキュリティ意識の向上が課題となっていました。

取組内容

既設の「Pマーク(※1)委員会」を拡充し、「情報セキュリティ委員会」を組織しました。また、経営層を巻き込んで教育計画の見直しを図りました。

結果と今後

「情報セキュリティ委員会」の発足により、現場の実情に即したセキュリティルールの策定や教育プログラムの拡充に取り組みやすくなりました。今後は、現場の従業員に寄り添った形でセキュリティ対策を強化し、セキュリティ意識の浸透を図ります。

背景と課題

背景

個人情報を多く取扱う印刷業に求められるセキュリティ強化を目指し、全社体制を構築

個人情報や取引先の機密情報を多く取扱っているため、取引先からのセキュリティ対策に対する要求が年々高まっています。Pマークの取得やUTM(※2)の導入など、一定の取組は進めていますが、セキュリティ担当者1名では対応に限界があるため、全社を巻き込んだ対応が必要です。

課題

1. 担当者が他の業務と兼任する「1人情報システム体制」でセキュリティ対策が進まない
2. 担当業務により意識に差があり、従業員がルールを守らない場面が散見される
3. 全社的なセキュリティ意識の向上には、経営層の理解や従業員への教育が必要

取組内容

取組1　既存の社内体制を拡充し、「情報セキュリティ委員会」を設置して、セキュリティ管理体制を強化

既に設置されていた「Pマーク委員会」を拡充し、新たに「情報セキュリティ委員会」として組織しました。従来より広く現場部門を巻き込んで議論を進めることが可能となり、現場部門の実情や抱えている課題、要望を洗い出すことができる体制ができました。

取組2　従業員のリテラシーにあわせて、全従業員が理解できるようにセキュリティ教育を実施

セキュリティ教育の資料内に、社内で私物のデバイスを利用する際の運用ルールやインシデント発生時の初期対応などについて盛り込みました。この資料は全従業員を対象としたものであるため、普段PCを使用しない現場従業員にもわかりやすい内容にすることを心掛けました。

取組3　経営層の理解を深めるために、セキュリティ教育の方針を明確化

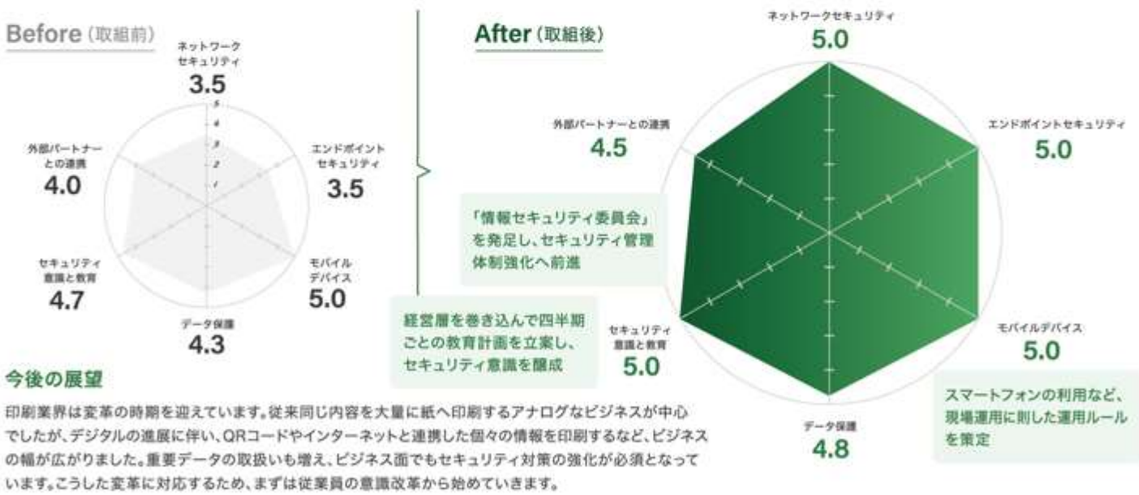
取引先が求めるセキュリティ対策を経営層と共有して、セキュリティ教育の方針について話し合いました。この議論により教育を年1回から四半期に1回行うなどの方針を明確にできました。従業員がセキュリティ対策を自分事として捉え、より具体的な理解を深めることを目指しました。

※1　プライバシーマーク（個人情報を適切に取扱う体制を整備していると認定された事業者に付与）　※2　Unified Threat Management 統合脅威管理（複数のセキュリティ機能を統合した管理システム）

結果と今後

1. 「情報セキュリティ委員会」の発足により、組織全体としてセキュリティ対策への取組を進める機運が芽生えてきています。今後は他部門との連携を強化し、現場の課題や要望に地道に対応していきながら、さまざまな運用ルールの見直しにも着手していきます。　→　継続
2. セキュリティ教育により運用ルールが現場に浸透したことから、ルールに違反する従業員はほぼいなくなり、教育の成果を実感しています。今後も、教育内容を定期的に見直し、現場の変化や新たなリスクに対応したプログラムを導入していく予定です。　→　継続
3. 経営層がセキュリティ対策のための予算化や体制強化の必要性を認識するようになり、長期的な投資計画と予算確保、体制の議論を行っています。今後も、経営層を含めた全社レベルでのセキュリティ意識の強化を目指して、議論を進めていきます。　→　継続

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連携



今後の展望

印刷業界は変革の時期を迎えています。従来同じ内容を大量に紙へ印刷するアナログなビジネスが中心でしたが、デジタルの進展に伴い、QRコードやインターネットと連携した個々の情報を印刷するなど、ビジネスの幅が広がりました。重要データの取扱いも増え、ビジネス面でもセキュリティ対策の強化が必須となっています。こうした変革に対応するため、まずは従業員の意識改革から始めていきます。

経営層の声

取引先からの要望を踏まえたセキュリティ課題を明確化できました。セキュリティ管理体制の構築や社内教育の重要性を再認識したため、来年度に向けた予算の検討や全社的な意識改革を進めます。また、セキュリティ対策に注力している企業だと周知することで、企業競争力を高める取組を推進していきます。

参加者の声

他社の取組や本事業の専門家からのアドバイスを受け、自社のセキュリティ課題を整理することができました。また、社内教育に必要な取組の道筋も見えてきました。セミナーやワークショップで得た知識は現場で役立っており、今後も継続して学びを深めていきたいと考えています。

建設・製造

専門工事業　E社

ベンダーとの役割分担と責任範囲を明確にし、自社の運用ルールに合わせたセキュリティ体制を確立

企業プロフィール
- 業　　種：建設業
- 従業員数：～50名

セキュリティ体制　複数名体制/兼務

事業内容　建造物のコンクリート内部探査や耐震診断調査から耐震補強工事、地中探査や埋設物探査などを行っています。産業廃棄物収集運搬業や産業廃棄物処分業の認可を取得しており、環境に配慮した作業プロセスを提供しています。

背景と課題

セキュリティ規程の整備を行い「SECURITY ACTION（二つ星）」を宣言しましたが、規程に準じた具体的な活動は積極的にできていません。

取組内容

ベンダーとの役割分担や責任範囲を確認しました。また、セキュリティハンドブックの作成やクラウドサービスへの移行の検討などに取り組みました。

結果と今後

ベンダーの責任範囲を整理し、自社で対応するべきセキュリティ対策が明確になったことで、自立した体制への一歩を踏み出しました。今後は、ベンダーとの連携を強化し、必要なセキュリティレベルに応じた対策を検討していきます。また、従業員教育を通じて、セキュリティ意識の向上を図っていきます。

背景と課題

背景

ベンダーにセキュリティ対策を任せていたため、自社として十分な検討ができていない

セキュリティ規程を整備し、「SECURITY ACTION（二つ星）」を宣言しましたが、セキュリティ対策はベンダー任せで、自社として十分に検討できていません。また、大手取引先からのセキュリティ調査が増加しており、対策の見直しや強化、従業員へのセキュリティ教育の重要性が高まっています。

課題

1. 運用はベンダー主体で行っており、ベンダーとの役割分担や責任範囲が把握できていない
2. 自社の運用に合ったセキュリティ運用ルールの策定と文書化が必要
3. 今後のシステム構想として、オンプレミス環境からクラウドサービスへの移行を検討

取組内容

取組1　各ベンダーの責任範囲を把握するとともに、自社で実施するべき内容を確認し、具体的な対応を行う

ネットワークやサーバ、業務システムなど、ベンダーと連携して運用しているシステムを整理し、ベンダーとの役割分担と責任範囲を確認しました。例えば、バックアップデータはベンダーが保有しているものの、復旧は自社で行うことが確認されたため、復旧手順をまとめました。

取組2　具体的なセキュリティ運用ルールを定めた「セキュリティハンドブック」を作成し、社内に展開

IPA(※1)の提供する「情報セキュリティハンドブック」をもとに、自社の運用に合わせて「セキュリティハンドブック」を作成しました。従業員の職種ごとの運用の違い、PCとスマートフォンの使用に関する説明の精査、テレワーク利用時の注意点などを盛り込みました。

取組3　営業外出時や現場作業時のテレワークの増加に伴い、セキュリティ確保と利便性向上を検討

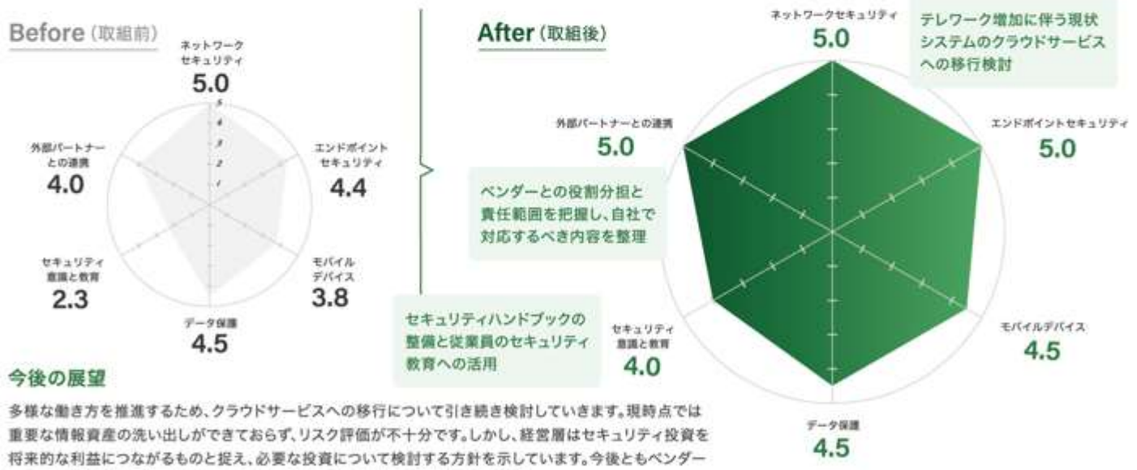
営業外出時や現場作業時のテレワークの増加に伴い、社外からのアクセスが増加していることから、セキュリティの確保と利便性の向上を目指して、クラウドサービスへの移行を検討しています。まずは、取引先とのファイル共有を目的に、クラウド型ファイル共有サービスを検討しました。

※1　独立行政法人情報処理推進機構

結果と今後

1. ベンダーとの役割分担や責任範囲を確認する過程で、ベンダーへの相談や依頼の方法について、本事業の専門家から学ぶことができました。現在は、社内システムの今後の展開（クラウドサービスへの移行や再構築など）について、ベンダーと協議を進めています。　→　継続
2. 作成したセキュリティハンドブックを活用し、従業員教育を実施します。従業員の職種ごとに教育資料を整備し、共通事項と個別事項をわけるなど、現場の従業員が理解しやすい内容に見直します。将来的にはセキュリティ事故事例なども追加する予定です。　→　継続
3. 今後のシステム構想として、現在のオンプレミス中心のサーバ環境を再構築するか、クラウドサービスに移行するかを、令和7年度中に決定することになりました。現在のファイルサーバが入替時期を迎えているため、早期に決定し、移行を進めていく予定です。　→　継続

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連携



今後の展望

多様な働き方を推進するため、クラウドサービスへの移行について引き続き検討していきます。現時点では重要な情報資産の洗い出しができておらず、リスク評価が不十分です。しかし、経営層はセキュリティ投資を将来的な利益につながるものと捉え、必要な投資について検討する方針を示しています。今後ともベンダーとの連携を強化し、必要なセキュリティレベルに応じた対策を検討していきます。

経営層の声

本事業に参加したことで、セキュリティ対策の重要性を再認識しました。特に、公共Wi-Fiなど社会のサービスに潜む危険性について認識を深めることができました。今後はセキュリティに関する最新情報を社内に周知していきます。自社の規模に合った対策を講じ、セキュリティ意識の向上を図ります。

参加者の声

本事業を通じて、費用対効果を重視しながらセキュリティ対策を進めることができました。ワークショップで他社の担当者から「経営層にセキュリティ費用をどのように説明するか」という話を聞きました。今後は経営層にセキュリティ対策の重要性を粘り強く説明し、予算の確保を目指していきます。

建設・製造

電子部品製造業　F社

東京都の支援事業を活用したセキュリティ対策強化、早期の脅威検知とインシデント調査を可能に

企業プロフィール
- 業　　種：製造業
- 従業員数：～100名

セキュリティ体制　複数名体制/兼務

事業内容
電子機器、産業機器、情報機器向けに電子部品の製造・加工を行っています。
多品種・小ロットに対応できる先端技術と豊富な設備を活かし、高品質で短納期の製品を提供しています。

背景と課題
取引先からセキュリティ状況の調査依頼があり、現在のセキュリティ対策における課題を確認し、不十分な部分を強化していきたいと考えました。

取組内容
EDR(※1)の導入や規程に則した教育コンテンツの作成、インシデント対応マニュアルの整備を進め、セキュリティ管理体制を強化しました。

結果と今後
EDRの導入により、早期の脅威検知と効率的なインシデント調査が可能になりました。また、普段PCを使わない工場の従業員のセキュリティ意識の向上にも取り組みました。さらに、事業継続の観点から、システム面での対策強化を検討し、インシデント発生に備えた体制を整えています。

背景と課題

背景

取引先からのセキュリティ調査をきっかけに、セキュリティ管理体制の強化を検討

取引先のセキュリティ要望の高まりに対応するため、セキュリティ規程の作成やUTM(※2)導入などの対策を進めています。規程の更新と従業員の意識向上が必要な一方で、現在の対策状況の課題が明確になっておらず、次に取り組むべき対策がわからない状態でした。そのため、本事業に参加することにしました。

課題

1. サイバー攻撃を受けた際の早期の脅威検知と原因特定を行いたい
2. 従業員のセキュリティ意識の向上が急務、特に工場に勤務する従業員を底上げしたい
3. 上長へのエスカレーションルールなど、インシデント対応フローが確立されていない

取組内容

取組 1

東京都の支援事業(※3)を活用してEDRを試験導入し、セキュリティ対策を強化

出口対策としてセキュリティ機器は導入していました。先般脅威が検出されたためフォレンジック調査を行いましたが、原因が特定できませんでした。そこで、東京都の支援事業を活用し、EDRを試験導入しました。EDRの機能と効果を確認した上で、本導入について検討しました。

取組 2

セキュリティ規程に則した教育コンテンツとフィッシング詐欺メール事例を題材に、意識向上を図る

セキュリティ規程をもとに、普段PCを使用しない工場の従業員にも理解しやすいように、業務に則した教育コンテンツを作成しています。IPA(※4)が提供する動画も活用します。また、実際に届いたフィッシング詐欺メールを題材にして情報発信を行い、注意喚起を促します。

取組 3

従業員ごとに、自社の運用に適した使いやすいインシデント対応マニュアルを作成

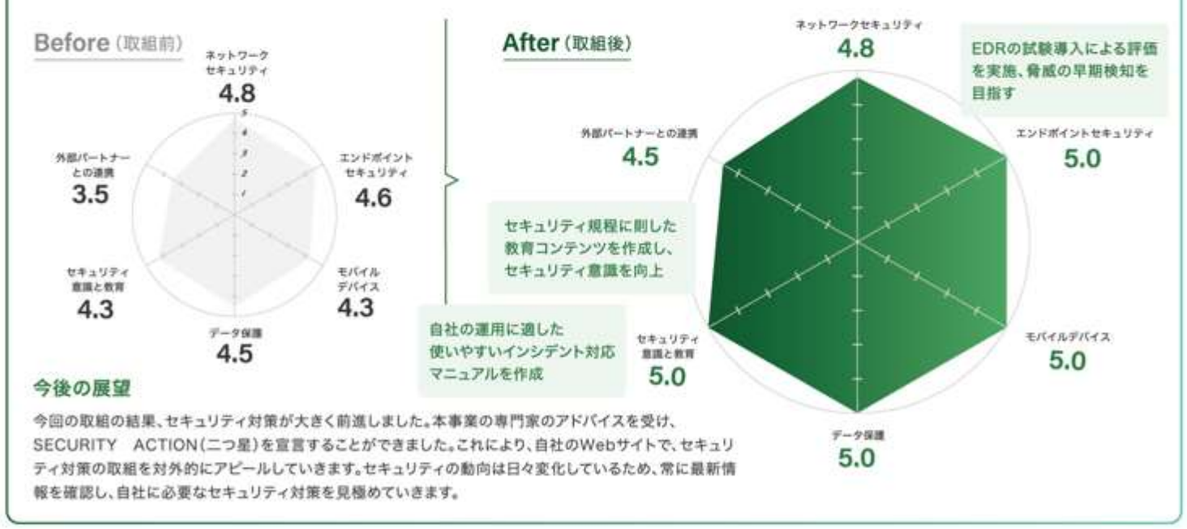
インシデント発生に備え、従業員ごとにインシデント対応マニュアルの作成を進めています。また、管理者側の対応も含め、連絡先や対応フローを整備しています。本事業の専門家に紹介された対応フローのサンプルを確認しながら、自社の運用に適した使いやすい資料を作成しています。

※1 Endpoint Detection and Response(端末のセキュリティ脅威を検知・分析・対応するセキュリティ技術)
※2 Unified Threat Management 統合脅威管理(複数のセキュリティ機能を統合した管理システム)　※3 東京都「令和6年度中小企業サイバーセキュリティ基本対策事業」
※4 独立行政法人情報処理推進機構　※5 Computer Security Incident Response Team(セキュリティインシデント対応の専門チーム)

結果と今後

1. EDRの試験導入では、特に脅威は検知されませんでした。EDRのサポートベンダーからは、定期的に端末の状況やログなどのレポートが提供されています。今後は、早期の脅威検知や効率的なインシデント調査のために、レポートの活用を進めていきます。　→ 解決
2. 工場に勤務する従業員についてはまだ意識の浸透に課題が残りました。そこで、教育コンテンツをPDF変換し、メールマガジンとして定期的に配信しています。また、社内サイトにはセキュリティの最新情報や事故情報を掲示し、全社的な意識の浸透を図ります。　→ 継続
3. 今後は、サーバダウン時の代替手段やシステムダウン時間に応じた復旧対応策を整理して、事業継続の観点からも対策を検討していきます。将来的には、インシデントに対応する組織(CSIRT※5)の設置も視野に入れ、検討を進めていきます。　→ 継続

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連携



今後の展望

今回の取組の結果、セキュリティ対策が大きく前進しました。本事業の専門家のアドバイスを受け、SECURITY　ACTION(二つ星)を宣言することができました。これにより、自社のWebサイトで、セキュリティ対策の取組を対外的にアピールしていきます。セキュリティの動向は日々変化しているため、常に最新情報を確認し、自社に必要なセキュリティ対策を見極めていきます。

経営層の声

セキュリティ対策は進めていましたが、システムやセキュリティ機器に関する対策をどこまですべきか不明なところがあり、参加しました。本事業に参加できたことは非常に価値があり、感謝しています。今後も、常に最新情報を確認しつつ、社内全体での運用と教育を行っていきたいと思います。

参加者の声

本事業を通じて、セキュリティ知識を体系的に習得することができました。学習が進むにつれて、セキュリティ対策は最初から完璧を目指すのではなく、できるところから始めることが大切だと実感しました。他社の取組事例と比較することで、自社のセキュリティ状況を見直す良い機会になりました。

建設・製造

電気機器製造業　G社

クラウドサービスの選定基準を明確化、また社内の意識向上のためフィッシングメール訓練を活用

企業プロフィール
- 業　　種：製造業
- 従業員数：～300名

セキュリティ体制　1名体制/兼務

事業内容　家庭用・業務用電化製品の輸入販売を行っています。小型調理家電製品や空調機器などを取扱っており、製品の販売、サポート、会員向けサービスを通じて、上質なライフスタイルを提案しています。

背景と課題

基本的なセキュリティ対策は実施していましたが、専門知識を持った担当者が不在のため、現在の対策に問題があるかどうかの判断ができませんでした。

取組内容

モバイルデバイスやデータ保護の対策強化、利用中のクラウドサービスの点検、従業員への継続的な啓蒙を通じて、セキュリティ全般の対策を改善します。

結果と今後

MDM(※1)の導入やデータバックアップのクラウドサービス活用などの検討を進めており、令和7年度内に対策を実行する予定です。また、今後新たにクラウドサービスを選定する際の基準も明確になりました。
従業員への研修や情報発信を通じて、セキュリティ意識の向上も実感しています。

背景と課題

背景

基本的なセキュリティ対策は実施しているが、リソース不足により運用体制が不十分

セキュリティ対策の専任担当者がいないため、IT管理者が兼任で対応しており、管理体制が十分ではありません。
基本的なセキュリティ対策は実施していますが、現在の対策に問題があるのか、漏れがないか、また対策を進める際にどの程度のコストや人的リソースを投入すべきかが不明で、判断ができていません。

課題

1. 重要データ保護のため、モバイルデバイスの対策強化やバックアップ運用の見直しが必要
2. クラウドサービスの利用状況を把握しておらず、セキュリティ面の評価ができていない
3. フィッシングメール訓練の結果を踏まえ、従業員のセキュリティ意識向上が急務

取組内容

取組1　これまで管理ができていなかったモバイルデバイスの対策強化のため、MDM導入を検討

業務で使用するスマートフォンやタブレット端末の管理が以前から不十分であることが課題でした。パスコードや生体認証が設定されていることは確認できましたが、OSのパッチやアップデートの対応、リモートでの消去やロックの対策を強化するため、MDMの導入を検討しています。

取組2　チェックリストによる評価基準を明確化し、利用中のクラウドサービスについて契約内容を点検

利用状況を調査した結果、約20種類のクラウドサービスを利用していることがわかりました。そこで、IPA(※2)が提供する「委託先情報セキュリティ対策状況確認リスト」を活用し、サービス提供事業者に協力を依頼して、セキュリティ対策の観点から点検を行いました。

取組3　従業員への定期的なセキュリティ対策訓練と注意喚起によりセキュリティの重要性を啓蒙

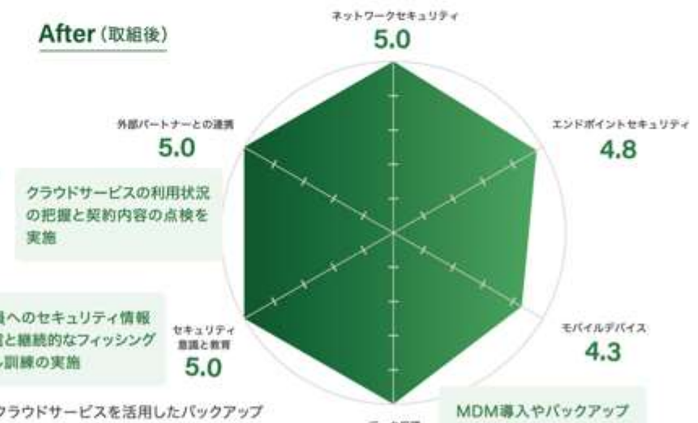
先般実施したフィッシングメール訓練で、一定数の従業員がURLをクリックしたため、今後は定期的な訓練と継続的な注意喚起を行っていきます。
IPAの最新情報や東京都「中小企業サイバーセキュリティフォローアップ事業」から提供されるメールマガジンを活用します。

※1　Mobile Device Management（モバイル端末を一元的に管理する仕組み）　※2　独立行政法人情報処理推進機構

結果と今後

1. MDMは令和7年度に導入する予定です。その他に、PCのディスク暗号化設定とデータバックアップの運用見直しを行いました。バックアップについては、複数のサーバを集約することで効率的に運用するとともに、オフライン保存の実施も検討しています。 → 継続
2. セキュリティ対策のチェックリストを活用することで、将来新たなクラウドサービスを選定する際の基準が明確になりました。個人情報の取扱い状況が可視化され、現状を正確に把握できるようになり、信頼性を確保した上でサービスを利用できるようになりました。 → 解決
3. 従業員を対象にセキュリティ関連の研修や情報発信を行うことで、少しずつ社内にセキュリティ意識が浸透してきていると感じています。セキュリティの重要性を理解し、インシデントが発生しても取引先に迷惑をかけないような社内体制の構築を目指します。 → 継続

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連携



クラウドサービスの利用状況の把握と契約内容の点検を実施

従業員へのセキュリティ情報の発信と継続的なフィッシングメール訓練の実施

MDM導入やバックアップ運用の見直しにより、重要データの保護対策を強化

今後の展望

令和7年度に向けて必要な予算を確保したので、MDMの導入やクラウドサービスを活用したバックアップ運用の確立を進め、セキュリティ対策を強化していきます。今後も、新たなサイバー攻撃手法の登場が予想されますが、最新情報を収集し、自社のセキュリティ対策を持続的に運用していくことをIT管理部門の目標に定め、安全で効率的な運用体制を実現します。

経営層の声

本事業を通じて、社内の運用体制の現状と課題が明確になり、改善の方向性を把握できました。また、本事業の専門家からのアドバイスを受けることで、経営層の中でセキュリティ投資に対する合意形成が進みました。今後も全社的に高いセキュリティ意識を持ち、運用体制の効率化と強化を推進していきます。

参加者の声

本事業のワークショップを通じて他社の取組を参考にすることで、自社の課題を客観的に見直すことができました。特に、少人数で効果的なセキュリティ運用を実現している事例に刺激を受け、今後の体制強化に役立つ知見を得ることができました。これらの知見を社内に持ち帰り、改善を進めていきます。

建設・製造

通信機器販売業　H社

令和7年度のISMS認証取得を目指し、実効性のあるセキュリティ管理体制を構築

企業プロフィール
- 業　　種：製造業
- 従業員数：～300名

セキュリティ体制　1名体制/専任

事業内容　産業用通信機器や映像通信機器の販売を行っています。産業用通信機器においては、海外から製品を輸入し、国内で使用できるように認定も取得しています。無線機器では、電波干渉が起きにくい商品ラインナップを揃え、それぞれの環境に合わせた商品提案を行っています。

背景と課題

令和7年度のISMS認証の取得を目指し、セキュリティ文書の見直しや運用整備、従業員のセキュリティリテラシーの向上を図りたいと考えていました。

取組内容

自社の運用に則した情報管理要領を作成し、eラーニングを行いました。また、重要データの分類を再定義し、保管ルールを明確にしました。

結果と今後

ISMS認証取得に向けて、セキュリティ対策の強化や従業員のセキュリティ意識が向上しました。
重要データの管理強化や外部サービス利用時の確認・申請方法の見直しを行い、セキュリティ面での信頼性が確保されました。これにより、取引先からの安心が得られる環境が整ったと感じています。

背景と課題

背景

セキュリティ方針や運用ルールを策定しているものの、従業員への浸透ができていない

セキュリティワーキンググループを設立し、週に1回活動しています。この中でセキュリティ方針や運用ルールを策定しましたが、従業員への周知が不足しており、まだ十分に浸透していません。令和7年度にはISMS認証の取得を目指しており、セキュリティ対策の強化と従業員のセキュリティ意識の向上が必要です。

課題

1. 自社のセキュリティルールを盛り込んだ実効性のある教育が出来ていない
2. 重要データの取扱いが適切に行われておらず、保管ルールも整備されていない
3. クラウドサービスなどの外部サービスの利用ルールや確認項目が明確になっていない

取組内容

取組1　情報管理要領などISMSに準拠したドキュメントを整備、従業員向けにeラーニングを実施

ISMSの管理文書を参考に、情報管理要領を整備しました。また、自社のセキュリティルールや一般常識を盛り込むとともに、社長のメッセージや最近の事故事例、関連法令などを加えて教育コンテンツを作成し、eラーニング形式の教育を提供しました。

取組2　重要データの分類を再定義し、重要度に応じた情報の保管ルールやフォルダ分類を整備

重要データの取扱いにおいて、多くのデータが「極秘」に分類されており、重要度に応じた適切な取扱いができていませんでした。そこで、重要データを「関係社外秘」「社外秘」「他社秘」「個人データ」という4つの分類に再定義し、情報の保管ルールやフォルダ分類を整備しました。

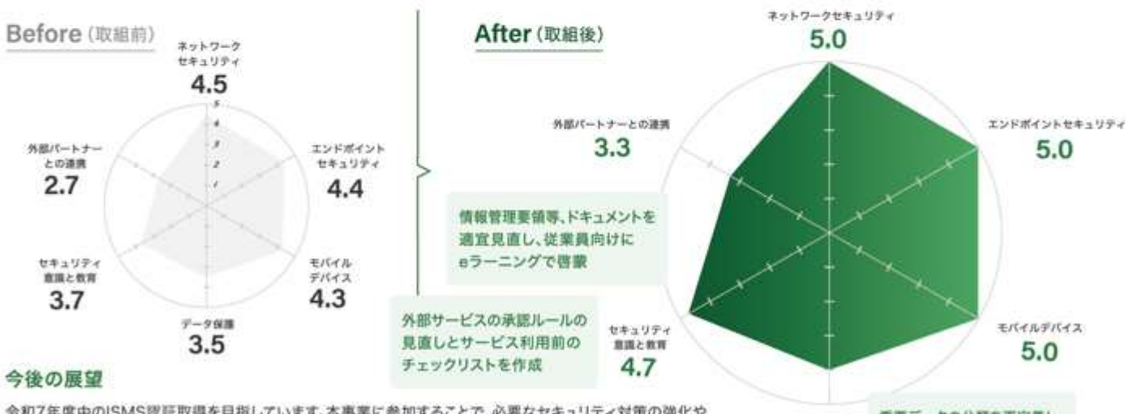
取組3　外部サービスの承認ルールを、業務内容や取扱う情報の重要度に応じて見直し

クラウドサービスなどの外部サービスを利用する場合には承認が必要ですが、インターネット検索や動画視聴などの機密情報を取扱わないサービスも申請の対象となっていました。そこで、業務委託や機密情報を保管するような外部サービスに限定して申請を行うように見直しました。

結果と今後

1. eラーニングの受講率は約85％で、理解度テストではすべての受講者が合格点に達しています。未受講の従業員には再度受講を促し、不合格者には再テストを実施しています。今後は定期的にeラーニングを実施し、全社的なセキュリティ意識の向上を図ります。　→ 解決
2. 重要データを共有サーバに保存する際は暗号化、PC内に保存することは禁止というルールがありますが、十分に守られていませんでした。今後は、重要データの取扱いについて周知徹底し、データ暗号化ツールを導入して、データ保護の強化を進めます。　→ 解決
3. 今後は、生成AIやショッピングサイトなどのクラウドサービスの取扱いについて、検討を進めます。クラウドサービスのセキュリティ対策状況については、確認すべき最低限の項目を整理し、利用前にチェックリストとして活用する方法を検討しています。　→ 解決

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連携



今後の展望

令和7年度中のISMS認証取得を目指しています。本事業に参加することで、必要なセキュリティ対策の強化や従業員のセキュリティ意識の向上など、実効性のある社内体制を構築することができ、認証取得に向けて大きく前進したと感じています。情報システム部門が一元管理している、従業員のPC設定やパスワード管理の運用方法など、課題は残っていますが、今後も継続的に取り組んでいきます。

経営層の声

本事業に参加することができて、大変感謝しています。本事業の専門家による支援を通じて、セキュリティ担当者の知識とスキルが向上し、自社に活かされていることを実感しています。今後も取引先のセキュリティ要件を満たすことができるよう、引き続きセキュリティ対策を進めていきます。

参加者の声

セキュリティを体系的に学べたことが一番の収穫でした。また、他社の取組を知ることにより、視野が広がり、刺激を受けられたことも有意義でした。まずは、令和7年度のISMS認証取得を目指し、社内で教育や啓蒙を進め、全社的にセキュリティ意識を向上させていきます。

建設・製造

精密部品製造業　I社

航空・宇宙分野の機密情報保護を目的に、インシデントに備えた復旧計画を策定し体制を強化

企業プロフィール
- 業　　種：製造業
- 従業員数：～300名

セキュリティ体制　複数名体制/専任

事業内容　精密部品の製造、加工を主な事業としています。金属加工を得意とし、厳格な品質要求にも高い技術力で対応しています。また、技術革新にも力を注いでいます。

背景と課題

ISMS認証に沿ったセキュリティ対策を実施していますが、インシデントが発生した際に、迅速な復旧ができるか不安に感じていました。

取組内容

実際のインシデント発生時を想定し復旧手順を明確化するとともに、バックアップ方法の見直しや地方拠点含めたセキュリティ対策の向上を図りました。

結果と今後

フォレンジック業者の選定と復旧手順の整備を進め、令和7年度には訓練を実施予定です。
また、データ保全を考慮したバックアップの導入や地方拠点へのセキュリティ製品の導入は前向きに検討しています。今後は、拠点間の多層防御の強化を通じ、全社的なセキュリティ向上を目指していきます。

背景と課題

背景

機密情報を取扱うため、ISMS認証を取得し、各種のセキュリティ対策を実施

取引先の技術情報を取扱うことから、ISMS認証を取得するとともにUTM(※1)などのセキュリティ製品を積極的に導入してます。しかし、現行の対策でインシデントに対応できるか不安があり、自社の強化ポイントを知りたいと考えていました。

課題

1. ISMS認証の取得時にインシデント発生時の対応を定めたが、具体的な内容が不明確
2. データバックアップは実施済みだが、復旧を前提とした強化が必要
3. 本社のセキュリティ対策を進める一方で、地方拠点のセキュリティ対策ができていない

取組内容

取組1　インシデント発生時の復旧対応について、手順の明確化と訓練実施計画の策定

従来より策定していたセキュリティインシデント発生時の復旧手順において、具体的な対応内容や対応者などが明確ではないことが判明しました。そこで各復旧手順における対応者を決定し、責任範囲を明確にしました。また、フォレンジック業者の選定も行いました。

取組2　バックアップ方式や保護対象となるデータを再検討し、クラウドバックアップシステムを導入

インシデント発生時の復旧を想定し、データバックアップの方式、周期、対象データ、保存場所などを改めて精査しました。ベンダーから業務復旧を前提に複数の案を提示されており、コストも考慮しながらクラウドバックアップシステムの導入に向けた議論を行いました。

取組3　地方拠点のセキュリティ対策を再検討し、全社単位でセキュリティレベルの向上を目指す

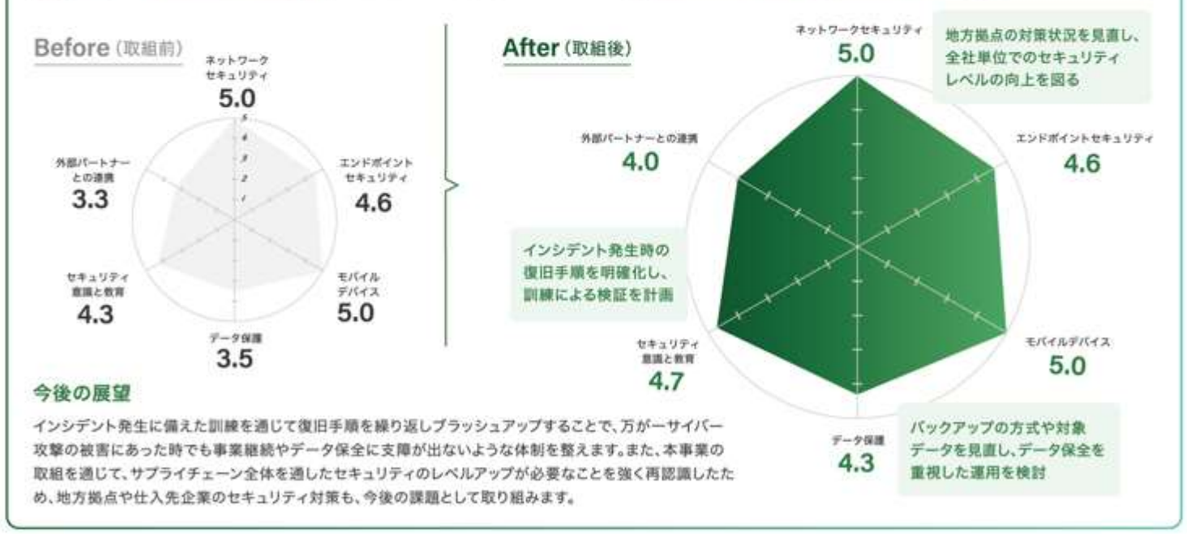
本社のセキュリティ対策を進める一方で、本社とVPN(※2)接続を行っている地方拠点のセキュリティ強化が課題になっていました。そこで、UTMやEDR(※3)の入替や新規導入を検討し、全社としてセキュリティレベルの向上を目指しました。

※1 Unified Threat Management 統合脅威管理（複数のセキュリティ機能を統合した管理システム）　※2 Virtual Private Network（仮想専用通信網）
※3 Endpoint Detection and Response（端末のセキュリティ脅威を検知・分析・対応するセキュリティ技術）

結果と今後

1. フォレンジック業者の選定は令和6年度中には完了する見込みであり、復旧手順は整備が進んでいます。令和7年度には、この復旧手順を用いたインシデント対応訓練を計画しており、手順の妥当性や不足部分を確認しながら実際のインシデントに備えます。　→ 解決
2. ベンダーからの提案を受け、社内で最適なバックアップの運用方法を検討しています。事業の特性上、復旧だけではなく、データ保全も重視する必要があることを本事業の専門家から指摘されており、この点も考慮したバックアップシステムを導入していきます。　→ 継続
3. 地方拠点におけるセキュリティ強化は、どのレベルまで担保するべきか社内で協議を進めています。また、全社のセキュリティレベルを向上させるという点で、VPNの多層防御についても今後取り組む必要があると認識しています。　→ 継続

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連携



今後の展望

インシデント発生に備えた訓練を通じて復旧手順を繰り返しブラッシュアップすることで、万が一サイバー攻撃の被害にあった時でも事業継続やデータ保全に支障が出ないような体制を整えます。また、本事業の取組を通じて、サプライチェーン全体を通したセキュリティのレベルアップが必要なことを強く再認識したため、地方拠点や仕入先企業のセキュリティ対策も、今後の課題として取り組みます。

経営層の声

本事業に参加したことで、社内メンバーだけでは気づけない課題を認識できたことが大きな成果でした。自社のセキュリティ対策を客観的な立場から評価いただき、貴重な機会となりました。セキュリティ対策は終わりのない、しかし、待ったなしの経営課題として、今後も注力してまいります。

参加者の声

本事業のセミナーで紹介されたセキュリティ関連の規程やドキュメントを、社内で展開し活用しています。ワークショップでは他社の事例を知り、自社の対策を考える上で参考になりました。また、本事業の専門家から自社の実態に即したアドバイスを受け、業務に活かすことができ、有意義に感じています。

建設・製造

医療機器製造業　J社

企業プロフィール
- 業　　種：製造業
- 従業員数：～300名

セキュリティ体制　複数名体制/兼務

事業内容　医療機器の製造および販売を行っています。機器のサポート体制は全国をカバーし、迅速に対応できることが強みです。院内のすべての環境を自社製品で快適に整えることがこだわりです。医療業界の現在のみならず、未来に向けた製品の開発を行っています。

情報は競争力を維持する最大の武器と捉え「情報を守るための攻めのセキュリティ対策」を目指す

背景と課題
セキュリティ対策の機器やツールは一通り導入していました。一方で、自社では十分に活用できず、ベンダーとの協力関係を築きたいと考えていました。

取組内容
インシデント発生時の対応の確認をベンダーと行いました。また、セキュリティポリシーの策定やPCのOSアップデートを自動化する検証を行いました。

結果と今後
本事業への参加をきっかけに、停滞していた自社のセキュリティ対策が大きく前進しました。
セキュリティポリシーを策定した後は、従業員に浸透させるための教育を実施し、意識の向上を図ります。
また、ベンダーとの対応範囲が明確になったことで、自社で行うべき対応の机上演習を行っていきます。

背景と課題

背景

ベンダー任せのセキュリティ対策と情報を整理し、ベンダーと伴走できる体制を目指す

UTM(※1)やEDR(※2)などのセキュリティ対策は実施していましたが、セキュリティポリシーがなく、運用担当者のセキュリティ知識不足もあって、導入したツールが十分に活用できていませんでした。そこで、ベンダーからの提案を評価した上で、最適な運用方法を自ら検討したいと考えました。

課題

1. セキュリティ関連の文書が未整備のため、従業員への教育ができず、意識浸透に課題
2. ベンダーとの責任分界点が曖昧で、インシデント発生時の迅速かつ適切な対応に不安
3. OSのバージョン管理は未実施で、パスワードも脆弱なためセキュリティリスクが高い

取組内容

取組1

IPA(※3)のひな型をもとにセキュリティポリシーを作成し、従業員のセキュリティ教育に活かす

セキュリティポリシーが策定されていないことから、従業員へのセキュリティ教育が実施できていませんでした。そこで、IPAの提供する「情報セキュリティハンドブック」をもとに、ポリシーの策定に着手しました。まずは自社が優先すべき項目を明確にし、作成を進めていきます。

取組2

インシデント発生時のベンダーとの役割分担を明確化するとともに機器の活用方法の理解を深める

インシデント発生時にベンダーに依頼する項目を洗い出し、その後、初動対応時の役割分担や対応範囲をベンダーと確認しました。さらに、自社で対応すべき範囲の具体的な手順を検討しました。また、自社で行うUTMのアップデートやログの活用方法についても確認しました。

取組3

OSを自動アップデートに設定変更。パスワードポリシーも策定し、パスワードを再設定

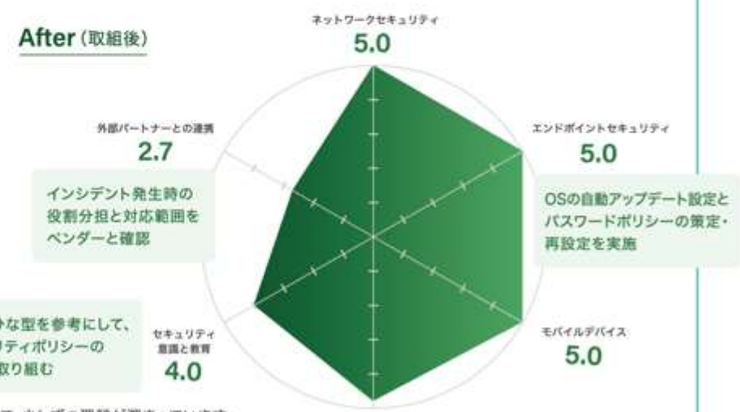
現状調査の結果、常にアップデートされているPCは半数にも満たない状況でした。そこで、一部のPCに更新プログラムを自動配布し、動作検証を行っています。また、桁数が少なく脆弱なPCのパスワードを強化するため、ポリシーを策定し、すべてのパスワードを変更しました。

※1 Unified Threat Management 統合脅威管理（複数のセキュリティ機能を統合した管理システム）
※2 Endpoint Detection and Response（端末のセキュリティ脅威を検知・分析・対応するセキュリティ技術）　※3 独立行政法人情報処理推進機構

結果と今後

1. セキュリティポリシーの基本的な方向性は定まり、担当部署内で共通認識が得られました。今後、完成に向けて協議を続け、令和7年度中には全社へ展開する予定です。展開にあわせて、従業員へのセキュリティ教育と理解度テストを実施します。　→ 継続
2. インシデント発生時の初動対応として、事象が発生したタイミングを正確に把握し、まず対象端末をネットワークから遮断することを決めました。また、ベンダーへの連絡と相談を迅速に行うことで、自社で解決できる問題も多いことに気づきました。　→ 解決
3. 動作検証が完了したため、自動アップデートを全社に導入する最終段階まで進んでいます。これにより、従業員の手間を減らしながら、脆弱性を防ぐことができます。また、全PCのパスワード変更が完了したことにより、不正アクセスの防止につながりました。　→ 継続

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連携**



今後の展望

インシデントが発生した際に重要となるUTMのログの仕組みについて、少しずつ理解が深まっています。一方で、ベンダーとの役割分担によって自社の対応範囲となった項目については、机上演習を通してインシデントに備えていきます。また、セキュリティ教育に終わりはないと考えており、今回の取組を活かした教育やテストの実施、最新のセキュリティ動向の共有などを継続して行っていきます。

経営層の声

自社のセキュリティ対策は、以前から進捗していませんでした。しかし、本事業を通じてセキュリティ対策の重要性を再認識し、パスワードポリシー策定やOS自動アップデートなど具体的な対策に取り組むことができました。今後は、「選択と集中」を念頭に置き、セキュリティ対策を推進してまいります。

参加者の声

「企業の当たり前」を守るためには、セキュリティ対策が重要であると再認識しました。自社が保有するデータは強みとなる一方で、リスクも伴います。今後は、リスクを最小化しながら企業の競争力を維持するために、従業員のセキュリティ意識の浸透がさらに重要になると考えています。

サービス・その他

テスト支援ツール開発・販売業　A社

従業員への運用ルールの徹底により意識変革、今後はセキュリティ監査で運用状況のチェック強化

企業プロフィール
- 業　　種：情報通信業
- 従業員数：～5名

セキュリティ体制　1名体制/兼務/経営者

事業内容　システム開発におけるテスト工程の効率化を通じて、品質と生産性の向上を支援する企業です。長年の経験を活かし、テストプラットフォームを中心にソリューションを提供しています。
テスト自動化、仕様書作成、テスト管理などの機能を連携させ、業務の効率化を実現します。

背景と課題

システム開発業務の特性上、取引先が求めるセキュリティ水準が非常に高いため、万全のセキュリティ対策を講じることが求められています。

取組内容

自社のセキュリティ対策について本事業の専門家による客観的な評価を受け、対策強化が必要な事項を洗い出し、改善策を実行していきました。

結果と今後

バックアップの運用方法を改善し、セキュリティ対策強化と業務効率化を実現しました。また、運用ルールの見直しにより、従業員のセキュリティ意識が向上しました。自社Webサイトの脆弱性も把握し、対策を進めています。
今後は定期的にセキュリティ監査を行い、継続的なセキュリティ対策の強化を目指します。

背景と課題

背景

人的リソースが限られる中で、効率的なセキュリティ対策強化を進めていきたい

従業員が5名と限られた人数の中で、セキュリティリスクの管理を進めていく必要がありました。現在は、自分自身の知識をもとにセキュリティ対策を講じていますが、その対策に漏れがないか不安です。本事業の専門家の意見を取り入れて、効率的にセキュリティ対策を強化したいと考えました。

課題

1. 定期的に自社のセキュリティ管理体制を評価し、必要なセキュリティ対策を見直したい
2. 重要データの保護強化と運用効率化の両面から見直しが必要
3. レンタルサーバで運用している自社Webサイトのセキュリティリスクを評価したい

取組内容

取組1　セキュリティ対策強化を進める上で、従業員が自分事として取り組むよう促す方法を検討

本事業の専門家によるセキュリティ対策の評価をもとに、改善が必要な点と不要な点を整理し、セキュリティ対策の強化内容を決定しました。
また、セキュリティ対策は経営者だけが実施しているという従業員の意識を変革し、従業員が自分事として取り組むよう促す方法を検討しました。

取組2　週次で行っていたバックアップ運用の見直しによる重要データ保護の強化と運用効率化の推進

重要データのバックアップ運用を見直し、週次でのバックアップに加え、差分データを毎日バックアップする運用としました。これにより、万が一のデータ損失インシデントにも迅速に対応できる運用を確立します。今後はさらに別サーバへの自動バックアップなどの検討を進めます。

取組3　ヒアリング結果に基づいたセキュリティ対策の再確認と将来を見据えた脆弱性への対策検討

自社Webサイトはレンタルサーバで運用し、自社のネットワークとは切り離されているため、運用保守も開発ベンダーに任せていました。しかし、本事業の専門家から指摘を受けたことで、自社Webサイトのセキュリティ対策を再確認し、安全性を向上させる取組を行います。

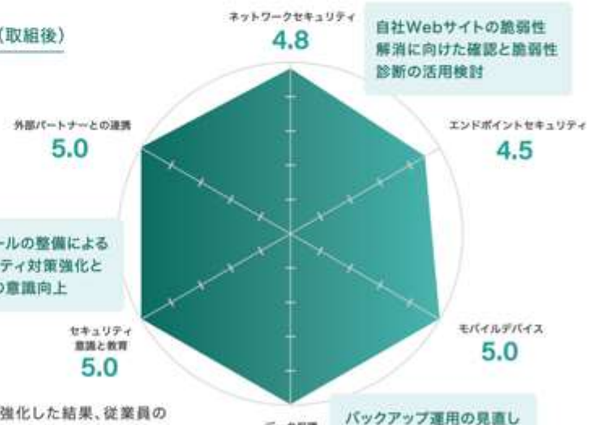
結果と今後

1. ファイル共有時には、ファイル共有サービスの使用と保存ファイルの暗号化、パスワードの別送信などのルールを明文化しました。また、今後はPCのスキャン結果を定期的に報告する運用を開始し、従業員のセキュリティ意識が向上するような取組を行います。　→ 継続
2. 今後は、サーバアクセス制限の見直しやデータの暗号化、デュプレックス（二重化）対応による信頼性向上にも取り組みます。データ保護を強化するとともに、従業員の業務負担を軽減する運用を実現し、セキュリティの維持と業務効率化を両立させます。　→ 継続
3. Webサイトの脆弱性を解消するため、契約中のレンタルサーバやWebサイトの設定、使用しているシステムのバージョンなどを確認しました。確認結果をもとに、必要な脆弱性対策を実施するとともに、脆弱性診断を活用してセキュリティ対策を強化します。　→ 継続

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連携

Before（取組前）

After（取組後）



自社Webサイトの脆弱性解消に向けた確認と脆弱性診断の活用検討

社内ルールの整備によるセキュリティ対策強化と従業員の意識向上

バックアップ運用の見直しによる重要データ保護の強化と運用効率化

今後の展望

セキュリティ運用ルールの整備や技術的な対応を通じて、セキュリティ対策を強化した結果、従業員のセキュリティ意識も向上しています。今後は社内で定期的にセキュリティ監査を実施し、従業員の日々のセキュリティ運用状況をチェックしていく予定です。また、自社の技術力を活かし、AIを活用したセキュリティ対策を検討し、従業員がアイディアを出し合いながら持続可能な対策を進めていきます。

経営層としての声

本事業を通じて、セキュリティ対策の重要性を再認識し、万が一のリスクに備える準備の必要性を改めて感じました。今後は、経営層を含む全従業員の意識向上に取り組むとともに、セキュリティ管理体制を継続的に改善し、より信頼される企業を目指していきたいと考えています。

参加者としての声

セミナーやワークショップを通じて他社の取組や工夫を知り、自社の課題を客観的に見直すきっかけとなりました。また、セキュリティの基礎知識を再確認し、見落とした点を再発見する貴重な機会となりました。参加者同士の意見交換も有意義で、新たな視点を得ることができました。

サービス・その他

社会保険労務士業　B社

多くの個人情報を取扱う企業として、「SECURITY ACTION（二つ星）」で対外的にアピール

企業プロフィール
- 業　　種：学術研究・専門・技術サービス業
- 従業員数：～5名

セキュリティ体制　1名体制/兼務/経営者

事業内容　企業の給与計算業務や人事労務管理業務を専門的に受託しています。人事や総務担当者への指導や、労働環境の整備も行っています。特に、行政官庁に提出する書類の作成や手続き、事務代理業務を中心に日々個人情報を取扱っています。

背景と課題

他社のランサムウェア被害を目の当たりにし、UTM(※1)などの基本的な対策だけではなく、セキュリティ対策全体の見直しが必要だと感じました。

取組内容

セキュリティポリシーの更新、デバイスの暗号化、クラウドサービスの運用方法の見直しなどを通じて、より体系的なセキュリティ対策を検討しました。

結果と今後

各種規程やガイドラインの整備、技術的な対策強化、ファイル共有などの業務運用方法の見直しを通じて、体系的なセキュリティ対策の強化を図ることができました。これらの取組を対外的にもアピールして、企業としての信頼を得るため、「SECURITY ACTION（二つ星）」を宣言する予定です。

背景と課題

背景

取引先から個人情報を預かる業種のため、体系的なセキュリティ対策の構築が急務

多くの個人情報を取扱うため、UTMやウイルス対策ソフトウェアなどのセキュリティ対策には積極的に取り組んできました。しかし、セキュリティに関する方針や規程など、組織としての対策は不十分でした。また、技術的な知識を持つ従業員が不在のため、第三者による評価と体系的な対策の検討が必要でした。

課題

1. セキュリティポリシー・規程が整備されておらず、インシデント発生時の対応ができない
2. 業務で使用するデータの暗号化やアクセス権限の管理ができていない
3. ファイル共有する際の脱PPAP(※2)を目指して、クラウドサービスを検討したい

取組内容

取組1　取引先の個人情報を多く取扱う会社としてセキュリティポリシーや規程類をブラッシュアップ

本事業の専門家にアドバイスを受け、過去に作成していたセキュリティポリシーをブラッシュアップしました。さらに、IPA(※3)が提供する「中小企業の情報セキュリティ対策ガイドライン」を参照しながら、セキュリティ規程の作成にも取り組みました。

取組2　ディスク暗号化ツールの導入とデータへのアクセス権限の見直しにより重要データの保護を強化

本事業の専門家からアドバイスを受け、まずPCのOSバージョンを確認し、標準搭載されているディスク暗号化機能の有効化を検討し、実施手順を確認しました。一部のPCではOSのバージョンアップが必要であることが判明しましたが、順次対応していく方針です。

取組3　チェックリストを活用してクラウドサービスの内容や安全性を評価し、自社に最適なサービスを選定

IPAが提供する「中小企業のためのクラウドサービス安全利用の手引き」を参考に、現在利用しているクラウドサービスをチェックしました。また、ファイル共有における「脱PPAP」を進めるため、一般的に利用されているクラウドサービスとの違いやメリットを確認しました。

※1：Unified Threat Management 統合脅威管理（複数のセキュリティ機能を統合した管理システム）　※2：パスワード付Zipファイルのメール送信手法の俗称
※3：独立行政法人情報処理推進機構

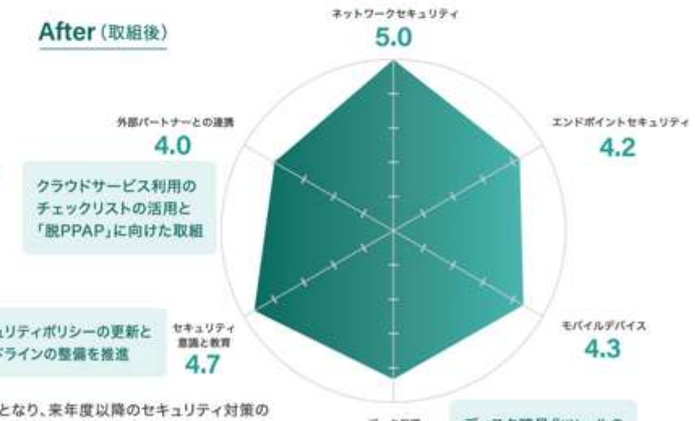
結果と今後

1　セキュリティ運用ルールが詳細に決まっていないため、まずは簡単なガイドラインを作成しました。この取組を社外にアピールするため、自社のWebサイトにセキュリティポリシーを掲載し、「SECURITY ACTION（二つ星）」を宣言することにしました。　→　解決

2　ディスク暗号化ツールは一部のPCに導入し、PCのレスポンスへの影響や運用上の注意点を確認した上で、順次展開する予定です。また、重要データの保護強化のため、データのアクセス権限の設定を見直し、部署ごとの管理方法に変更するなどの対策を講じます。　→　継続

3　本事業の専門家から、いくつかのクラウドサービスの事例を紹介されました。これらの情報を参考に、ファイル共有サービスを選定し、令和7年度の導入を予定しています。また、クラウドサービスのチェックリストは、今後のサービス選定にも活用していきます。　→　継続

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連携



クラウドサービス利用のチェックリストの活用と「脱PPAP」に向けた取組

セキュリティポリシーの更新とガイドラインの整備を推進

ディスク暗号化ツールの導入と重要データ保護強化に向けた検討実施

今後の展望

本事業は、これまで着手できなかった課題に取り組む貴重な機会となり、来年度以降のセキュリティ対策の方向性が明確になるという成果を得ることができました。今後は、本事業に非常に前向きに携わった従業員の中から1名をセキュリティの推進役として育成します。また、IPAが提供する動画コンテンツなどを活用して、全従業員のセキュリティ意識をさらに高めていきます。

経営層としての声

本事業を通じて、遅れていたセキュリティ対策が進展し、新たなセキュリティ担当者が決定したことで大きな変化を感じました。サイバー攻撃はいつ発生するか分からないため、全従業員が常にセキュリティ意識を持つよう促していきます。今後は継続的にセキュリティ教育を実施していきます。

参加者としての声

本事業の専門家派遣において、次回までに対応すべき課題が具体的に提示され、自社に不足しているセキュリティ対策と取り組むべき事項が明確になりました。また、IPAの提供する有益な情報やコンテンツを知ることができたため、今後はセキュリティ対策に積極的に活用をしていきます。

サービス・その他

薬事支援サービス業　C社

欧州のGDPRへの対応も見据えながら、取引先の機密情報を守る対策強化を実行

企業プロフィール
- 業　　種：学術研究・専門・技術サービス業
- 従業員数：～20名

セキュリティ体制　1名体制/兼務/経営者

事業内容　医薬品の開発や品質・安全性・供給に関わる戦略立案や当局への相談サポート、製造販売業許可取得・更新などのコンサルティングを行っています。薬事申請の助言や安全管理、製造販売後調査も取扱い、製薬企業などの医薬品の開発から市場への導入までをサポートしています。

背景と課題

医薬品開発に関わる極めて秘匿性の高い情報を取扱うことに加えて、海外の取引先も多く、どの程度までセキュリティ対策を講じるべきか悩んでいました。

取組内容

セキュリティ対策状況を整理し、優先順位を付けて対応していきました。セキュリティ製品の導入やインシデント対応ルールの明確化などを行いました。

結果と今後

自社のセキュリティ対策状況を把握し、セキュリティ製品の導入や運用ルールの明文化などが進んだことから、より強固なセキュリティ対策を講じることができました。今後はさらなるセキュリティ対策の充実を図り、国内外の取引先からの信頼を高めていきます。

背景と課題

背景

欧州のGDPR[※1]への対応も意識しながら、見えないセキュリティ対策のゴールに苦慮

製薬に関わる高度な機密情報を取扱うことに加え、欧州をはじめとする海外企業との取引も多いため、セキュリティは非常に重要視されています。ISMS認証は取得しており、基本的なセキュリティ対策は講じていますが、どのレベルまで対策を進めるべきか判断がつきませんでした。

課題

1. 自社のセキュリティ対策状況を把握し、対策強化項目の洗い出しと対応内容の検討が必要
2. PCレスポンスなどの現場運用を優先していたため、技術的なセキュリティ対策に躊躇
3. インシデント発生時の対応方法が曖昧なため、実効性に課題

取組内容

取組1　本事業の専門家派遣により、自社に必要なセキュリティ対策の洗い出しと優先順位付けを実施

本事業の専門家派遣により、自社のセキュリティ対策状況を評価し、強化すべき対策の洗い出しと優先順位付けを行いました。また、セキュリティ対策はベンダーと連携して対応していますが、導入機器のアップデートやトラブル時の対応などの役割分担も確認しました。

取組2　セキュリティ製品の導入と設定変更により、リモートワークやPCのセキュリティ対策を強化

リモートワークでの「セキュリティ強化」と「PCレスポンス確保」のため、現状のUTM(※2)をより高性能なものに入れ替え、VPN(※3)を利用できるように設定しました。また、「PCの紛失時の対策」や「USBの使用禁止の設定」のためにMDM(※4)を導入しました。

取組3　インシデント発生時の手順を洗い出し、明文化することで、実効性のあるルールを策定

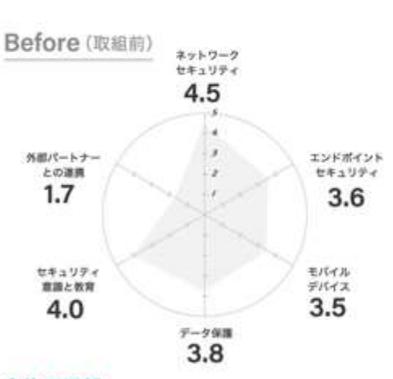
本事業の専門家からアドバイスを受け、「インシデント発生時の一次報告先」、「初動対応」、「社内外への連絡先」などを洗い出しました。
また、インシデント発生時の早期の原因究明のため、ベンダーとの連携によるEDR(※5)やMDMのモニタリングを開始しました。

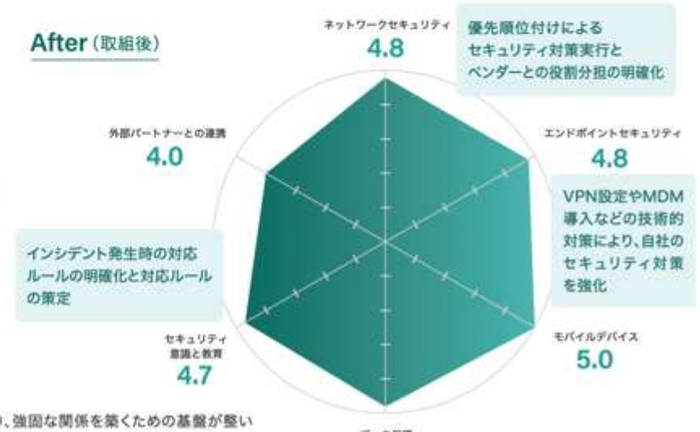
※1 General Data Protection Regulation（EU域内における個人情報の取扱いを定めたもの）　※2 Unified Threat Management 統合脅威管理（複数のセキュリティ機能を統合した管理システム）
※3 Virtual Private Network（仮想専用通信網）　※4 Mobile Device Management（モバイル端末を一元的に管理する仕組み）
※5 Endpoint Detection and Response（端末のセキュリティ脅威を検知・分析・対応するセキュリティ技術）

結果と今後

1. 本事業を通して得られた知識やノウハウにより、今後能動的にセキュリティ対策に取り組む目処が立ちました。
取引先に欧州の企業が多くGDPRの遵守が必須となっており、今後はコーポレートサイトのクッキー対策からGDPRへの対策を進めていく予定です。　→ 解決
2. セキュリティ製品の導入によりコストは増加しましたが、一定水準のセキュリティレベルが担保できたため、投資対効果は高かったと感じています。今後は運用状況を定期的に確認し、MDMのモバイル端末への展開などのセキュリティ対策を継続強化していきます。　→ 解決
3. 外資系企業から転職してきた従業員の多くは、厳格なセキュリティ教育を受けており、会社全体のセキュリティ意識は比較的高いと考えています。今回、技術的な対策の強化や運用ルールの明確化が進んだことで、全社的なセキュリティ対策がさらに強化されました。　→ 解決

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連携





今後の展望

セキュリティ対策の充実により国内外の取引先からの信頼が高まり、強固な関係を築くための基盤が整いました。今後も新たなサイバー攻撃が発生する可能性があるため、これらの脅威に対応できるよう情報収集を続け、定期的に対策を見直すことが重要だと考えています。また、海外企業との取引を拡大するために「品質マネジメントシステム ISO9001」の取得に向けた活動も進めていきます。

経営層としての声

本事業を通じて、セキュリティ対策は取引先から信用を勝ち取る上で欠かせないものであると再認識できました。経営上の重要課題ととらえ、予算を確保し継続的に取り組んでいきます。また、最新のセキュリティ動向を把握し、サイバー攻撃のトレンドを理解することも、経営層の努めだと考えています。

参加者としての声

本事業に参加し、自社に必要なセキュリティ対策を把握できました。選択肢も情報も多いなか、何を自社で取り組むべきか曖昧なままでしたが、現在は解決へと向かっています。また、経営者がセキュリティ担当者だからこそ、スピード感のある判断・取組が可能であるという、自社の強みも実感できました。

サービス・その他

マーケットリサーチ業　D社

独学でのセキュリティ対策やビルのWi-Fiネットワーク利用に危機感あり、本事業の活動で払拭

企業プロフィール
- 業　　種：学術研究・専門・技術サービス業
- 従業員数：～20名

セキュリティ体制　1名体制/兼務

事業内容　市場参入や成長戦略、ブランディングやポジショニングなどに向けたマーケットリサーチをグローバルに提供しており、日本以外にも複数の拠点を海外に持っています。消費者の意識を読み解き戦略・施策を立案することで、顧客の課題解決に貢献しています。

背景と課題

独学で行っているセキュリティ対策に不安がありました。入居するオフィスビルのWi-Fiを使用しており、セキュリティ上の危険性も認識しています。

取組内容

専用ネットワークの契約によりセキュリティを確保しつつ、UTM(※1)やEDR(※2)を導入しました。また、従業員へのセキュリティ教育も進めています。

結果と今後

ネットワークや機器を導入し、安心感を得ることができました。今後はログの管理や問題発生時の対応を徹底して行います。また、本事業の専門家によるアドバイスを活かし、従業員へのセキュリティ教育を進め、自社のセキュリティ対策をさらに向上させたいと考えています。

背景と課題

背景

独学で行っているセキュリティ対策と自社のネットワーク環境の脆弱性に不安

入居しているオフィスビルの備え付けWi-Fiネットワークを使用しているため、ネットワーク環境の脆弱性や情報漏えいなどのセキュリティリスクを認識していました。EDRは導入していますが、1名体制で独自に調査しながらセキュリティ対策を実施していることに、日頃から不安を感じていました。

課題

1. オフィスビルに備え付けのWi-Fiを使用しており、セキュリティ上の危険性を認識
2. EDRは導入されているが、ログを定期的に確認するなどの運用ができていない
3. 従業員に対するセキュリティ教育ができておらず、セキュリティポリシーも未更新

取組内容

取組1　自社専用のネットワークを契約するとともに、セキュリティ対策としてUTMを導入

本事業の専門家にアドバイスを受けて、自社専用のネットワークを契約しました。オフィスビルのWi-Fiネットワークが他社と共有されており、セキュリティ上の危険性がある状況を改善しました。また、セキュリティ対策をさらに強化する目的でUTMも導入しました。

取組2　EDR導入によりエンドポイントセキュリティを強化しつつ、ログの運用方法も検討

UTMの導入後、エンドポイントセキュリティの一元管理のためにEDRを見直し、セキュリティの堅牢性を強化しました。インシデントを迅速に検出する仕組みを導入し、盤石なセキュリティ管理体制の構築を目指しました。また、ログの定期的な確認にも取り組みました。

取組3　従業員へのセキュリティ教育の計画策定とセキュリティポリシーの抜本的な見直し

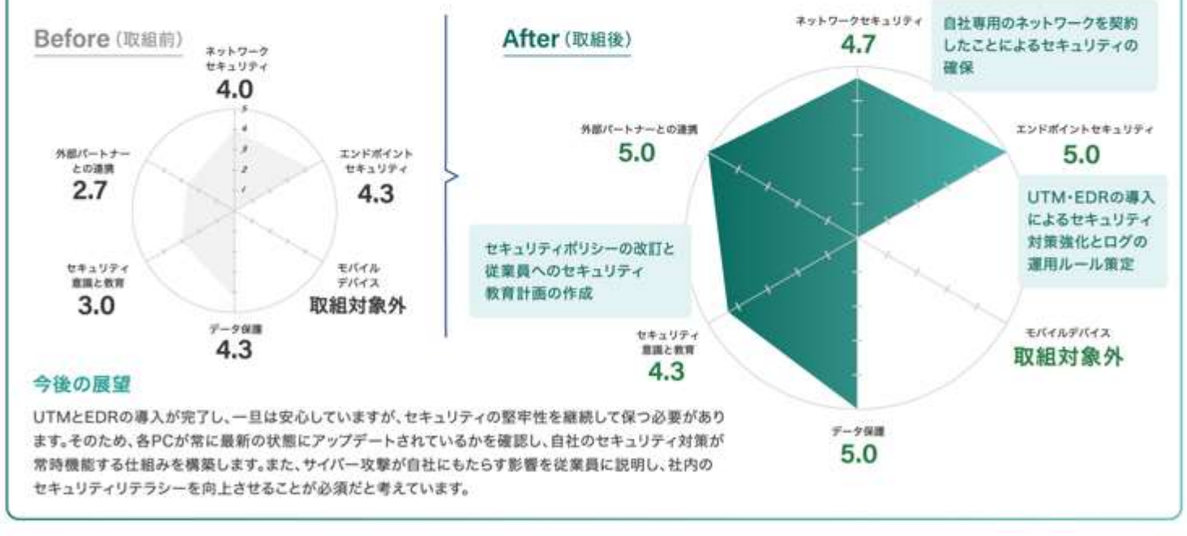
従業員のセキュリティリテラシー向上のため、教育に関する計画を作成しています。また、セキュリティポリシーを策定後、約4年もの間、見直しを行っていなかったため、本事業の専門家から提供される資料などを参考にしながら改訂を進めています。

※1　Unified Threat Management 統合脅威管理（複数のセキュリティ機能を統合した管理システム）
※2　Endpoint Detection and Response（端末のセキュリティ脅威を検知・分析・対応するセキュリティ技術）

結果と今後

1. 自社専用のネットワークの導入により、情報漏えいなどのセキュリティ上のリスクが軽減されました。またUTMのログは導入ベンダーから提供してもらえるため、セキュリティ担当者の負担を減らしつつ、問題が発生した場合にも迅速に対応可能となりました。　→　解決
2. EDRの導入によりエンドポイントセキュリティの強化は実現したものの、EDRをオフにしてしまう従業員がいるため、セキュリティ対策の重要性が浸透しきれていないと実感しています。自社のセキュリティ対策には、引き続き改善が必須であると考えています。　→　解決
3. セキュリティリテラシーの向上は急務のため、令和6年末から一般的なコンテンツベースで教育を開始しています。令和6年度内にセキュリティポリシーの改訂を完了させ、早々に改訂後のセキュリティポリシーを盛り込んで教育内容の見直しを行っていきます。　→　継続

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連携



今後の展望

UTMとEDRの導入が完了し、一旦は安心していますが、セキュリティの堅牢性を継続して保つ必要があります。そのため、各PCが常に最新の状態にアップデートされているかを確認し、自社のセキュリティ対策が常時機能する仕組みを構築します。また、サイバー攻撃が自社にもたらす影響を従業員に説明し、社内のセキュリティリテラシーを向上させることが必須だと考えています。

経営層の声

本事業に参加後、ネットワークの契約やUTMの導入など、自社のセキュリティ対策の改善が実感できたため、安心できました。自社にとってセキュリティ対策は優先度の高い取組であるため、継続して予算を組み込み、アップデートを図ってまいります。今後とも同様の事業があれば参加していきたいです。

参加者の声

本事業の専門家によるアドバイスやセミナー・ワークショップは、とても参考になりました。また、参加されている他社の方々とコミュニケーションが取れるため、セキュリティに関する悩みを相談したり、対策として導入した機器を紹介してもらえる機会が得られたので大変ありがたかったです。

サービス・その他

ITコンサルティング業　E社

属人化を脱却しリスク払拭へ、情報セキュリティ委員会の定期開催により体制強化を加速

企業プロフィール
- 業　　種：情報通信業
- 従業員数：～20名

セキュリティ体制　1名体制/兼務

事業内容　携帯電話向けアプリケーションや周辺機器の動作検証に関するコンサルティングおよび検証用端末のレンタルを行っています。また、創業当初から培った検証に関するノウハウに基づいた機種選定やプラン提案など、顧客のニーズに対応したソリューションを提供しています。

背景と課題

対策が属人的で組織として統一が図れていませんでした。また、情報資産管理台帳が未整備であり、システム対策も自社での把握が難しい状況でした。

取組内容

情報資産管理台帳を作成し運用に向け準備、セキュリティポリシーを自社Webページへ掲載、ベンダーに依頼している対策の現状把握と整備を行いました。

結果と今後

将来的にはISMS認証取得を視野に入れ、情報セキュリティ委員会でBCP(※1)やCSIRT(※2)構築について議論を重ねていく予定です。さらに、セキュリティポリシーの見直しや対策へのリソース確保についても継続的に協議し、自社のセキュリティ運用ルールを厳密に定めていきます。

背景と課題

背景

属人的だったセキュリティ対策を新しい担当者へ引き継ぐにあたり、知識強化が急務

1名体制によるセキュリティ対策では、すべてに手が回らない上、不測の事態によるセキュリティ担当者不在のリスクを抱えていたため、新たな担当者の育成が必要でした。
また、保有する情報資産を正確に把握できておらず、自社のセキュリティ状況を掴みきれていないことを改善するため、本事業に参加しました。

課題

1. 自社の情報資産の把握ができておらず、情報資産管理台帳が存在しない
2. 策定済みのセキュリティポリシーは社内で共有できておらず、対外的にも示せていない
3. 担当者の知識が不足しており、セキュリティ機器の運用状況を自社で把握できていない

取組内容

取組1　情報資産管理台帳のフォーマットを策定し、現在使用していないファイルをネットワークから隔離

IPA(※3)の「リスク分析シート」を参考にし、ファイル名など自社での運用に必要な項目を追加しながら、独自の情報資産管理台帳の策定に着手しました。また、情報資産の保管期間と保管方法を明確にし、古いものはネットワークから隔離するルールを設けました。

取組2　セキュリティポリシーを自社Webページに公開。情報セキュリティ委員会を定期開催へ変更

更新したセキュリティポリシーを自社Webページに掲載し、対外的にセキュリティ方針を示しました。また、社内に向けてセキュリティポリシーを浸透させるために、本事業への参加前から不定期に実施していた情報セキュリティ委員会を月に1回、定期開催することに決定しました。

取組3　ベンダーと連携してセキュリティ対策状況を点検し、その過程で発見した脆弱性への対策を実施

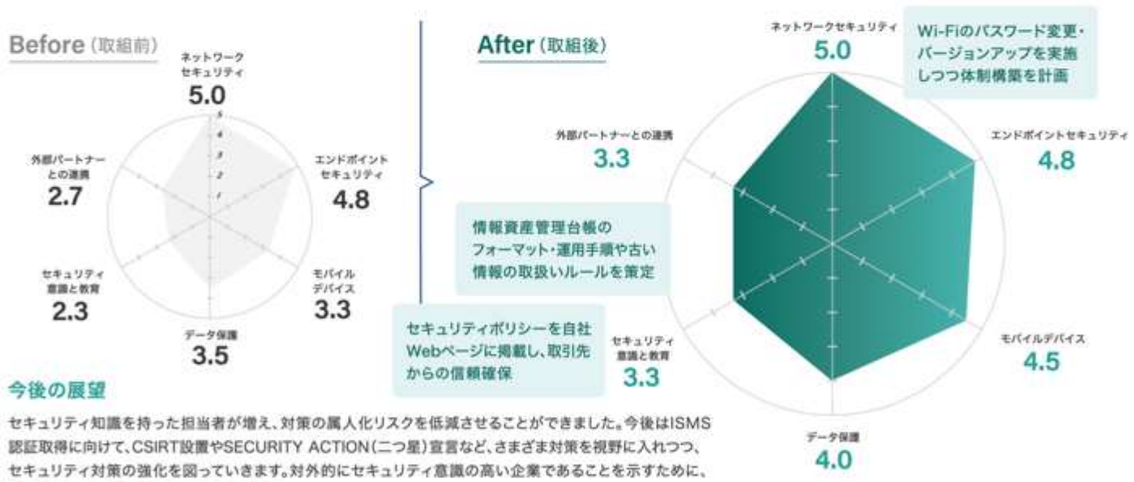
ベンダーに依頼して実施しているセキュリティ対策について、現状の運用・保守状況を問い合わせました。VPN(※4)、Wi-Fi、ルータ、NAS(※5)などがベンダーの保守対象ではないことが判明したため、一部は自社で、保守・更新を計画しました。

※1　Business Continuity Plan(事業継続計画)　※2　Computer Security Incident Response Team(セキュリティインシデント対応の専門チーム)
※3　独立行政法人情報処理推進機構　※4　Virtual Private Network(仮想専用通信網)　※5　Network Attached Storage(ネットワークに接続された記憶装置)

結果と今後

1. 情報資産管理台帳は令和7年度の運用開始に向けて、自社が保有する情報資産に対するリスクやそれぞれのリスクに見合う対応策の検討を進めています。台帳の作成を通して、自社が保有する資産の管理方法やリスクについて社内で共通認識を取ることを目指します。　→ 継続
2. セキュリティポリシーを自社Webページへ掲載したことにより、取引先から信頼を得る一歩を踏み出しました。
今後は、情報セキュリティ委員会でセキュリティポリシーの定期的な見直しを行い、より社員に浸透しやすい、実情に即した対策基準を定めます。　→ 継続
3. Wi-FiのパスワードをWi-Fiとより強固なものに変更しました。また、Wi-FiとNASのバージョンアップを実施しました。
今後は業務に支障をきたさないよう、保守計画や担当者を明確化し、定期的にバージョンアップを実施する運用ルールの策定を目指します。　→ 継続

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連携



今後の展望

セキュリティ知識を持った担当者が増え、対策の属人化リスクを低減させることができました。今後はISMS認証取得に向けて、CSIRT設置やSECURITY ACTION(二つ星)宣言など、さまざま対策を視野に入れつつ、セキュリティ対策の強化を図っていきます。対外的にセキュリティ意識の高い企業であることを示すために、取組の継続は必須であると考えています。

経営層の声

セキュリティ担当者の知識強化により、自社の体制整備に向け基盤が整いました。本事業に参加することにより、対策の過不足を整理でき、必要な対策が明らかになりました。また、情報セキュリティ委員会にて、担当者が自社に必要な対策を能動的に発信する姿を見て、成長を実感しました。

参加者の声

本事業への参加により、サイバー攻撃の脅威をはじめとする重要なセキュリティ情報を学びました。また、ワークショップやセミナーにて他社の取組を聞き、セキュリティ対策は「スモールスタート」「できることから」「継続的に」という基本を再確認できたことも収穫でした。

サービス・その他

臨床試験支援サービス業　F社

高度なセキュリティ対策を可能にする組織へ転換、医療機関や製薬会社の重要な情報を守る

企業プロフィール
- 業　　種：医療・福祉
- 従業員数：～20名

セキュリティ体制　1名体制/兼務/経営者

事業内容　臨床研究の支援業務、コンサルティング、医療機器の臨床試験業務、データ管理および統計処理業務などを行っています。臨床研究の実施体制を支援し、製薬会社や大学病院などの医療機関向けにビジネスを展開しています。

背景と課題

従来より経営者がセキュリティ対策を一人で検討・実施しており、自社のセキュリティ体制のレベルに不安と限界を感じていました。

取組内容

自社のセキュリティ対策レベルを可視化し、セキュリティ機器などの導入計画を策定しました。また、セキュリティ管理体制の目指す姿を明確にしました。

結果と今後

取扱う情報を重要度別に分類・体系化し、保有するオンラインストレージの運用を見直すことで、セキュリティ強化を図ることができました。また、今回の取組を通じて、経営層を含む複数人にてセキュリティ対策を検討したため、今後も長期的かつ継続的な対策を進めていくことができます。

背景と課題

背景

臨床試験支援サービス事業者としてベンダーと協力し、セキュリティ対策を推進

製薬会社や大学病院などが保有する特許申請前の機密情報を取扱っているため、高いセキュリティ対策レベルが要求されます。しかし、現状では経営者一人で対策を進めており、セキュリティ対策や管理体制の実効性に課題があると認識しています。そのため、今後どのように対策を強化すべきか非常に悩んでいます。

課題

1. 必要なセキュリティ対策レベルを把握しきれておらず、具体的な対策強化が実行できない
2. セキュリティ運用ルールや実行していくためのセキュリティ管理体制が整備されていない
3. 取引先の機密情報や個人情報のセキュリティ対策や運用ルール策定が不十分

取組内容

取組1　本事業の専門家派遣により、取扱う情報の重要性に見合ったセキュリティ対策レベルを整理

ネットワーク構成図を使用して、本事業の専門家と共に自社のセキュリティ対策状況を確認しました。また、ベンダーからのセキュリティ機器導入の提案内容を共有することで、より技術的なアドバイスを受けました。それに基づいて、ベンダーに最適なセキュリティ機器の再提案を依頼しました。

取組2　セキュリティポリシー策定やインシデント対応フローを見直し、管理体制の明確化が必要であると認識

セキュリティポリシーの策定とともに、「情報セキュリティ責任者の設置と役割決め」、「インシデント発生には情報を集約させて再発防止を図るためのフローの作成」などのインシデント対応フローの見直しを行い、目指すべきセキュリティ管理体制を明確にする必要性を認識しました。

取組3　重要な個人情報を安全に取扱うため、情報の分類などの具体的な運用ルールの策定を検討

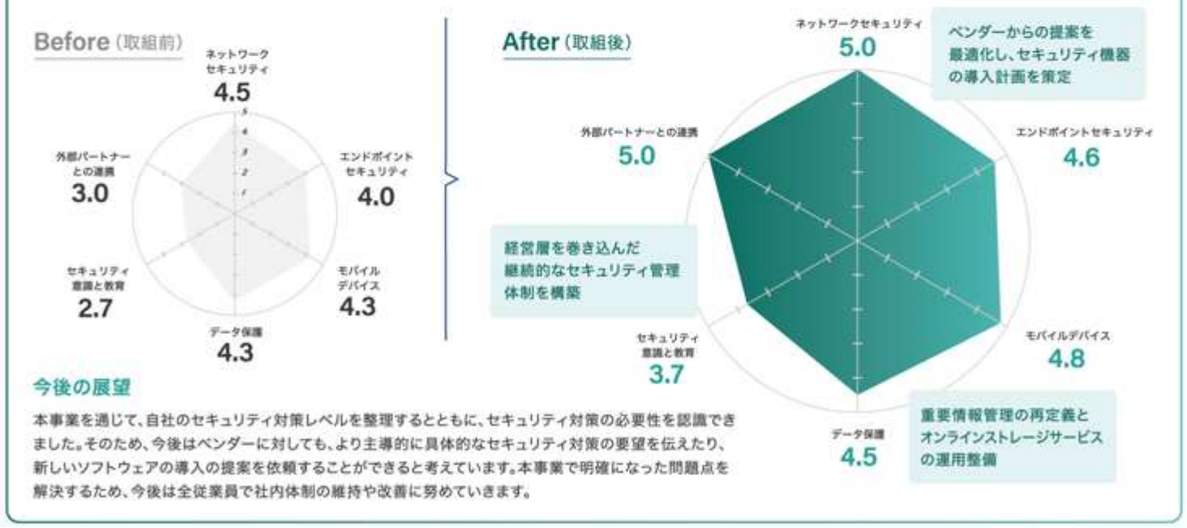
取引先の機密情報や個人情報を取扱うフォルダの運用ルール策定の必要性を認識しました。今後は、保有しているデータの内容や特性を整理し、情報の重要度を定義することにより運用ルールを明確にする予定です。利用しているオンラインストレージサービスの有効性の検証も進めています。

※1　Unified Threat Management 統合脅威管理（複数のセキュリティ機能を統合した管理システム）

結果と今後

1. ベンダーからの再提案を受け、自社として最適なセキュリティ機器やソフトウェアの導入選定を行っています。セキュリティ対策の有効性から導入の優先順位付けを行い、予算措置や補助金活用なども含めた今後のセキュリティ対策強化計画の方針を明確にしました。　→ 継続
2. セキュリティポリシー改善やインシデント対応フロー整備には、まだ時間が掛かりそうです。しかし、今回の取組を契機に、経営層を含む複数名が率先してセキュリティ確保のための議論を行い、長期的かつ多角的な視点でセキュリティ対策を推進できるようになりました。　→ 継続
3. オンラインストレージサービスに保有している重要情報の取扱いについて認識できました。また、既に導入していたディスクの暗号化ツールに加え、重要情報を保有するフォルダに対するアクセス制限によって、以前より強固な情報管理を進めたいと考えています。　→ 継続

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連携



今後の展望

本事業を通じて、自社のセキュリティ対策レベルを整理するとともに、セキュリティ対策の必要性を認識できました。そのため、今後はベンダーに対しても、より主導的に具体的なセキュリティ対策の要望を伝えたり、新しいソフトウェアの導入の提案を依頼することができると考えています。本事業で明確になった問題点を解決するため、今後は全従業員で社内体制の維持や改善に努めていきます。

経営層としての声

本事業の専門家派遣によって、不明瞭だった自社のセキュリティ対策レベルを明確にできました。また、ベンダーが提供しているネットワーク構成図やセキュリティ対策について改めて理解できたため、今後は限られたリソースでどのように対策を強化していくかについて長期的に検討していきます。

参加者としての声

自社のセキュリティに対して、適切なセキュリティポリシーを用意したり、インシデントフローの見直し・改善が必要だったりと具体的な方向性を把握できました。また、社内で決定権のある人を交えてセキュリティ管理体制を築く重要性も実感できました。今後も継続して、取組を実施していく予定です。

サービス・その他

不動産仲介業　G社

多国籍の従業員が多くセキュリティ意識向上が課題、「極意」の冊子を活用したユニークな研修実施

企業プロフィール
- 業　　種：不動産業・物品賃貸業
- 従業員数：～20名

セキュリティ体制　1名体制/兼務/経営者

事業内容　不動産売買や賃貸物件の仲介を中心に、投資用不動産の提案、不動産管理のサービスを提供しています。特に、多言語対応による海外顧客のサポートを強みとしており、日本人はもとより、国内外在住の外国人の日本における不動産探し、および不動産売却をお手伝いしています。

背景と課題

多くの個人情報を取扱うため、UTM(※1)導入や従業員へのセキュリティ啓発活動により一定の効果を上げてきましたが、技術面の課題が残っています。

取組内容

EDR(※2)導入などの管理体制強化を進めるとともに、過去のセキュリティ被害を教訓に注意喚起を行うなど、従業員の意識向上を図りました。

結果と今後

社内PCのOSの統一やEDR導入を計画することにより、セキュリティ管理体制が着実に改善されました。
また、定期的なセキュリティ教育を通じて、従業員のセキュリティ意識も向上しています。本事業の終了後も、継続的かつ計画的なセキュリティ対策強化を進めていくための基盤ができました。

背景と課題

背景

顧客の信頼を支えるための セキュリティ体制強化が急務

業務の性質上、多くの顧客情報を取扱うため、セキュリティ対策の強化が急務です。UTMの導入や従業員へのセキュリティ啓発活動により一定の効果を上げてきましたが、PCのOS統一やEDRの導入など技術面での課題が残っています。経営層主導で体制強化を進め、業界標準に準じたセキュリティ対策を模索しています。

課題

1. ランニングコストの負担が大きいため、セキュリティ対策にかける予算の確保に難航
2. 社内PCのOSが統一されていないため、管理や監視が難しい状況にある
3. 従業員のセキュリティ意識が低く、実際にインシデントが発生している

取組内容

取組 1

経営層がセキュリティ対策の重要性を再確認し、計画的な予算化を推進

ランニングコストは課題ですが、令和5年度にUTMを仮導入したことでウイルス感染が発覚し、迅速に対処できました。この経験からUTM導入の効果を実感し、「インシデントが発生してからでは遅い」という意識が経営層に共有され、セキュリティへの積極的な投資が進むことになりました。

取組 2

異なるOSで運用されてきたPCのOSを統一し、統合的なセキュリティ管理基盤を構築

EDR導入の障壁となっていたPCについて、社内PCのOS統一を進める取組を開始しました。従業員の利用状況を精査し、Windows OSのアップグレードなど、適切なインフラ環境を整備することで、統合的なセキュリティ管理基盤の構築に取り組みました。

取組 3

外国籍の従業員が多いため、セキュリティ意識向上に向けた継続的な取組が急務

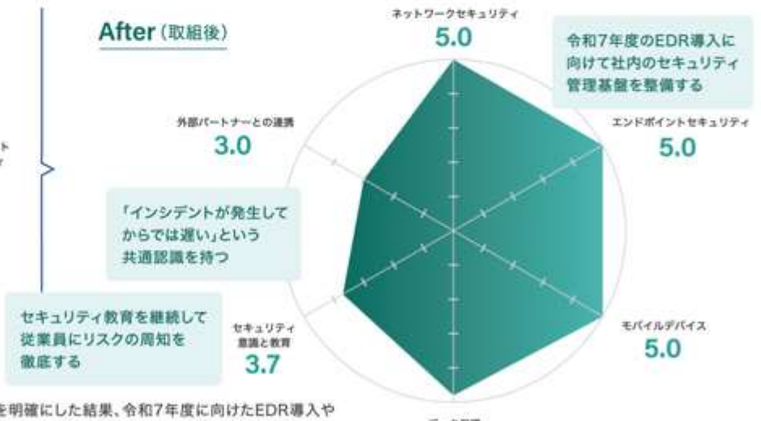
過去のセキュリティ被害を教訓に、実際のUTMレポートを用いて危険なWebサイト訪問のリスクを説明し、注意喚起を行いました。また、東京都提供の「中小企業向けサイバーセキュリティ対策の極意」の冊子を使って定例会議で情報周知を行い、セキュリティ意識向上に取り組んでいます。

※1 Unified Threat Management 統合脅威管理（複数のセキュリティ機能を統合した管理システム）
※2 Endpoint Detection and Response（端末のセキュリティ脅威を検知・分析・対応するセキュリティ技術）

結果と今後

1. 令和7年度に向けて、EDR導入を具体的に計画しています。経営層の理解と後押しを受け、今後も長期的な視点でセキュリティ投資を行い、新たな脅威にも対応できる強固なセキュリティ管理体制を構築していきます。 → 継続
2. UTMに加えてEDRの運用を含めた統合的なセキュリティ管理基盤を整備することで、外出先からの情報アクセスに対するセキュリティ対策が強化され、従業員が安心して業務に専念できる環境が実現します。今後もセキュリティ対策の強化を継続していきます。 → 継続
3. UTMのサポートベンダーから定期的にレポートが送られてくるので、危険なWebサイトへのアクセスなどの危険行動が検知された際には、対象のWebサイトやアクセスしたPCの特定による指導ができるようになり、従業員のセキュリティ意識が徐々に向上しています。 → 継続

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連携



今後の展望

本事業の専門家派遣を通じて、自社のセキュリティ課題を明確にした結果、令和7年度に向けたEDR導入やPCのOSの統一など、具体的な取組への道筋が見えてきました。また、セミナーやワークショップを通じて得られた知識を活用し、今後はセキュリティ規程の策定と共有を進めるとともに、定期的な社内教育を実施して、全社的なリスク対応力をさらに高めていく予定です。

経営層としての声

本事業の専門家派遣やセミナーで得た知見をもとに自社の課題を整理し、セキュリティ対策の強化を進めることができました。ランニングコストが課題ではありますが、「インシデントが発生してからでは遅い」という意識を持ち、顧客の信頼を得られるセキュリティ管理体制を整えていきたいです。

参加者としての声

本事業に参加して、「PC管理や社内教育が不十分である」という自社の課題を再確認できました。セミナーでは、有識者でなくても理解できるように、段階的にセキュリティ知識を学べた点がとても有意義でした。今後はこの経験を活かして、セキュリティ対策を計画的に強化していきたいと考えています。

サービス・その他

ITインフラサービス業　H社

仕組み(ルール、IT環境、教育文書)を見直し、情報セキュリティ意識の浸透と定着を徹底

企業プロフィール
- 業　　種:情報通信業
- 従業員数:～20名

セキュリティ体制　複数名体制/兼務/経営者

事業内容　パソコンのライフサイクル「企画・設計」「調達・導入」「運用・保守」「撤去・回収」の各フェーズにおいて、お客様の環境に応じて、運用の定着を見据えた企画・提案を行います。
運用開始後もPDCAサイクルを回しながら、継続的に支援をしています。

背景と課題
ISMS認証の取得、EDR(※1)の導入などの基本的な対策は実施しています。従業員へのセキュリティ意識の浸透に課題があると感じていました。

取組内容
教育資料と方法の見直し、モバイル端末の運用改善、BYOD(※2)端末の使用禁止、インシデント対応フローの整備を行いました。

結果と今後
令和7年度の教育実施計画をISMSの管理文書に反映し、確実に実行していきます。
また、モバイルデバイスの管理ツールを使用して、利用状況を管理します。あわせて、現場でのヒヤリハットの情報を収集し、ディスカッションの場を設けるなど、セキュリティ意識の浸透を徹底していきます。

背景と課題

背景

ISMS認証取得やEDR導入は行っているが、セキュリティ意識の浸透が不十分

ISMS認証を取得し、セキュリティ方針や規程を策定、EDR導入やアクセスログ取得など基本的な対策を実施してきました。しかし、お客様に安心・安全なサービスを提供する企業として、従業員全体への情報セキュリティ意識の浸透とセキュリティレベル向上の余地があると感じていました。

課題

1. ITインフラの設計や構築に従事しているが、従業員のセキュリティ意識向上が課題
2. BYOD端末を使用して社内情報の閲覧・取得において運用ルールが未整備
3. インシデント発生時の具体的な対応フローが未整備

取組内容

取組1

ISMS管理文書を改訂、教育資料へ反映し意識浸透を強化

情報セキュリティ意識を従業員に定着させるため、教育コンテンツの拡充を図り、外部サービスを利用していた理解度テストに自社セキュリティルールを組み込み、内容を最適化しました。また、課題に取り組むためにISMS各種管理文書の改版を行っています。

取組2

社給スマートフォンを配布し、BYOD端末の利用を禁止することで、セキュリティ対策の強化を推進

BYOD端末から業務データへのアクセスを防ぐため、重要データの保管禁止を明確化し、MDM(※3)で制限を実施しました。
令和6年度中の社給スマートフォンの配布を決定し、現在は情報システム担当がテスト使用で運用・セキュリティ評価を行っています。

取組3

EDRの脅威検知アラートに応じたインシデント対応フローを明確にし、現場向け手順書を作成する

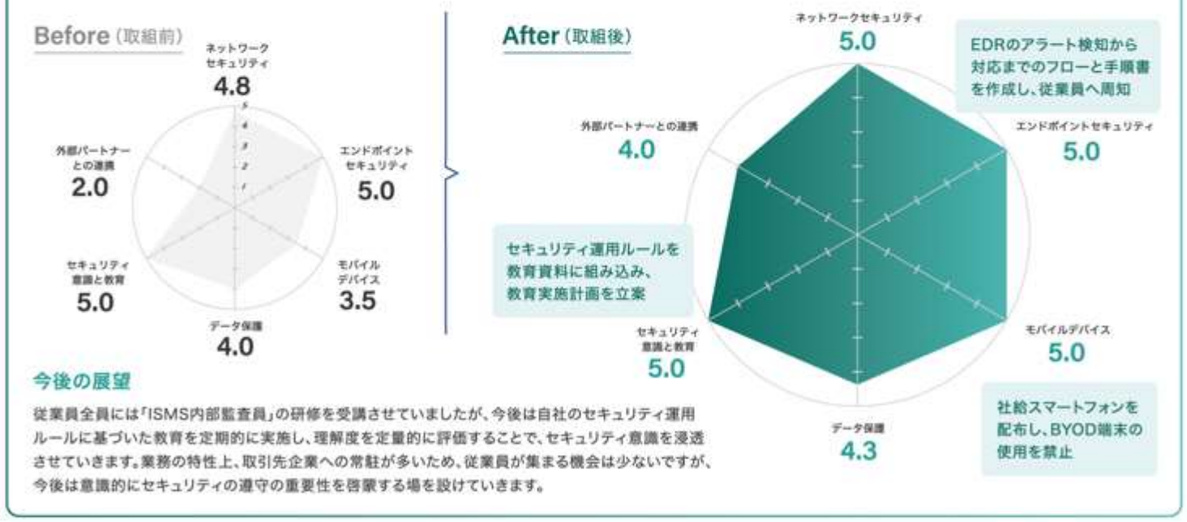
EDRが脅威を検知した場合の対応フローを整理しました。このフローには、セキュリティ担当者が行う確認内容や切り分け方法が含まれます。
検知されたアラートの緊急度に応じて、PCのフルスキャンや再キッティングを行う流れも明確化し、現場向けの手順書も作成しました。

※1:Endpoint Detection and Response(端末のセキュリティ脅威を検知・分析・対応するセキュリティ技術)　※2:Bring Your Own Device(個人所有のデバイスの業務利用)
※3:Mobile Device Management(モバイル端末を一元的に管理する仕組み)

結果と今後

1. セキュリティ教育は、これまで採用時のみ実施していましたが、今後は定期的に実施する方針で計画しています。令和7年度の教育実施計画をISMSの管理文書に反映させ、確実に実行することで、全従業員にセキュリティ意識を浸透させていきます。 → 継続
2. 社給スマートフォンの導入後には、BYOD端末の使用を禁止しました。また、モバイルデバイスの管理ツールを使用して、利用状況の管理を行っています。現場での運用ルールも整備し、従業員に周知することで、安全なセキュリティ運用を実現します。 → 継続
3. インシデント発生時の対応フローについては、今後、サイバー攻撃事例の追加など、さまざまなケースを想定して内容を充実させます。また、ヒヤリハットの情報を収集し、ディスカッションの場を設けて共有するとともに、必要に応じて対応フローに反映します。 → 継続

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連携



今後の展望
従業員全員には「ISMS内部監査員」の研修を受講させていましたが、今後は自社のセキュリティ運用ルールに基づいた教育を定期的に実施し、理解度を定量的に評価することで、セキュリティ意識を浸透させていきます。業務の特性上、取引先企業への常駐が多いため、従業員が集まる機会は少ないですが、今後は意識的にセキュリティの遵守の重要性を啓蒙する場を設けていきます。

経営層としての声
企業としてセキュリティ対策の重要性は理解していましたが、本事業を通じて、それが最優先事項であるべきと再認識しました。セキュリティ事故が発生した場合の自社の立場や取引先への影響を深く実感しました。本事業は非常に有益であり、参加できたことに大きな意義を感じています。

参加者としての声
セキュリティ対策は全従業員で取り組むものだと理解できました。
ワークショップで他社の取組を知ることができたため、それらを自社に取り入れたいと考えています。今後は、最新のインシデント情報やサイバー攻撃事例などを定期的にメールで発信するなど、全社的な情報共有に努めていきます。

サービス・その他

経営コンサルティングサービス業　I社

洗い出された課題の対応と従業員への情報発信という「地道な活動」により、社内の意識改革を推進

企業プロフィール
- 業　　種：学術研究・専門・技術サービス業
- 従業員数：～50名

セキュリティ体制　1名体制/兼務

事業内容　当社は経営コンサルティング事業を行っており、人材育成やリスキリングに関する官公庁の補助金・助成金に特化したBPO事業、支援事業、労務サポート事業を展開しています。官公庁や民間パートナーとの連携を通じて、企業の成長を促進し、中小企業の活性化に貢献します。

背景と課題

セキュリティ担当者に着任したばかりで、知識不足と現状把握ができず不安を感じていました。ISMS認証も取得済ですが、社内に浸透していません。

取組内容

現在取り組んでいるセキュリティ対策を整理し、課題洗い出しから始めます。また、担当者の知識習得や社内の意識向上のために情報共有を行います。

結果と今後

今後実施すべきタスクが整理され、セキュリティ対策強化の目処が立ちました。セキュリティ担当者は知識を習得することができ、今後の対策に活かせると考えています。また、従業員に対して、地道にセキュリティに関する注意喚起を続けてきた結果、些細なことでも相談を受ける機会が増えました。

背景と課題

背景

会社の規模拡大に伴い、全社的なセキュリティ体制の充実と意識向上が求められる

専門外の分野からセキュリティ担当者になり、前任者からの引継ぎも不十分でした。そのため、自社のセキュリティ状況や最新のセキュリティ動向については、その都度調べながら対応しています。ISMS認証は取得し、組織としては取り組んでいますが、セキュリティ意識が十分には浸透していないと感じています。

課題

1. ISMS認証取得時に作成した情報資産管理台帳の更新ができていない
2. 経営層からセキュリティ整備を導入するための必要な判断が得られない
3. UTM(※1)の管理やファイアウォールの設定が不明で、有効な対策ができていない

取組内容

取組1　情報資産管理台帳の作成と現状のセキュリティ対策の課題洗い出し、実施するべきタスクの整理を実施

本事業の専門家とともに、IPA(※2)が提供しているリスク分析シートを活用し、情報資産管理台帳を作成しました。また、現在のセキュリティ対策状況の課題を洗い出し、今後実施するべき具体的なタスクへの落とし込みと優先順位づけを行いました。

取組2　サイバー攻撃などによるセキュリティ被害状況などの情報提供を受け、社内に情報を発信

経営層はセキュリティの重要性を認識しているものの、取組を進めるための判断をできずにいました。サイバー攻撃による被害状況や被害額に関する資料を本事業の専門家から提供されたため、具体的なリスクを経営層に向けて説明し、継続的にセキュリティ意識の変革を促しました。

取組3　ネットワーク機器の設定状況が不明のため、まずはベンダーへの問い合わせにより現状把握を実施

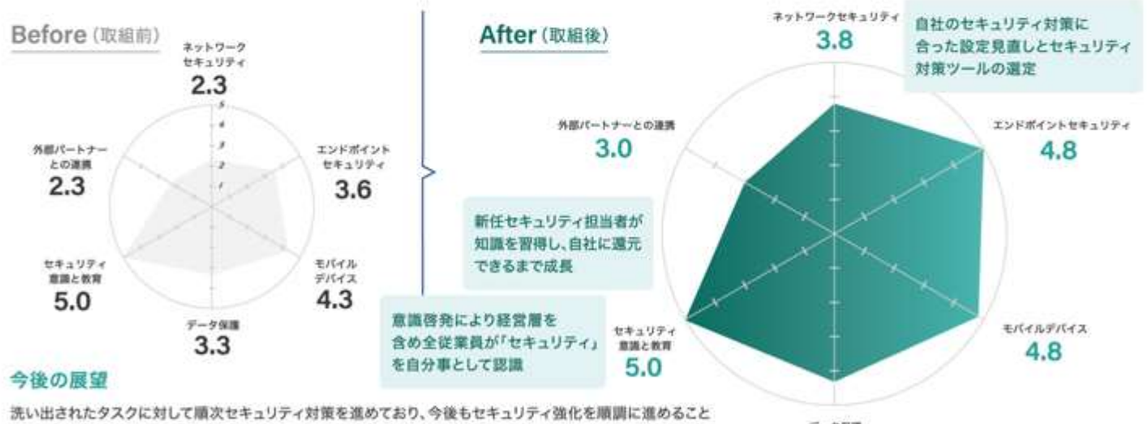
UTMは稼働中ですが、ネットワーク負荷が高いため、ベンダーとともに運用状況を確認し、他製品の検討を行っています。ファイアウォールについては導入経緯や設定状況が不明なため、まずは設定内容などの現状把握から始めました。

※1：Unified Threat Management 統合脅威管理（複数のセキュリティ機能を統合した管理システム）　※2：独立行政法人情報処理推進機構
※3：Mobile Device Management（モバイル端末を一元的に管理する仕組み）　※4：Virtual Private Network（仮想専用通信網）

結果と今後

1. セキュリティ担当者が情報資産管理台帳の使い方を理解したため、セキュリティリスクの評価と対策方法の検討を進めています。本事業のセミナーやワークショップへの参加や専門家の派遣を通じて、担当者のセキュリティ知識も蓄えられてきています。　→ 解決
2. 社内会議などで情報共有を行い、経営層や従業員の意識啓発に努めました。経営層がセキュリティ対策の実施を前向きに捉えていることに加え、従業員からセキュリティ対策に関する相談を受ける機会が増えるなど、全社的な意識の変化を実感しています。　→ 解決
3. UTMについては、入替に向けた製品選定を行っています。ファイアウォールはルータのアンチウイルス対策機能の設定追加で対応することにしました。今後は、ログ管理方法の検討やネットワーク診断などを行い、セキュリティ対策の強化を進めていきます。　→ 解決

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連携



今後の展望

洗い出されたタスクに対して順次セキュリティ対策を進めており、今後もセキュリティ強化を順調に進めることができます。また本事業を通じてMDM(※3)やVPN(※4)、多要素認証などの技術的対策により、さらなるセキュリティ強化ができることがわかりました。そのため、これらのセキュリティ対策ツールの導入に向けた検討を始めています。令和7年度も引き続き取り組んでいく予定です。

経営層の声

本事業への参加を通じて、非常に有意義な知見を得ることができました。現代のビジネス環境では、サイバーセキュリティ対策の強化は単なるリスク管理に留まらず、取引先からの信頼を得る基準となり、企業の競争力を左右する重要な要素であることを再認識しました。

参加者の声

本事業に参加したことで、セキュリティ対策の基本を学ぶことができました。また、セキュリティ意識は周囲に積極的に働きかけて醸成することが重要だと感じました。セキュリティ担当者として、事業規模が拡大する前に経営者を巻き込んで対策を進めることの重要性を実感しています。

サービス・その他

証券金融業　J社

金融庁のガイドラインに対応したセキュリティ確保に向け、対策推進のスタートを切る

企業プロフィール
- 業　　種：金融業・保険業
- 従業員数：～50名

セキュリティ体制　1名体制/兼務

事業内容　外国為替取引、証券取引、商品デリバティブ取引の3つの金融商品を取扱っています。対面取引に加え、一部オンラインの取引にも対応しています。個人のライフスタイルなどに合わせつつ、流動的な金融トレンドを把握し、総合的な取引ができることを目指しています。

背景と課題

近年、業界内でセキュリティ対策水準が高まる一方で、社内リソースが限られており、優先課題を選定できず、セキュリティ対策が後手に回っていました。

取組内容

セキュリティ課題の洗い出しと優先順位付けから着手し、情報資産管理の強化に向けた台帳や規程の更新、セキュリティ教育の計画などに取り組みました。

結果と今後

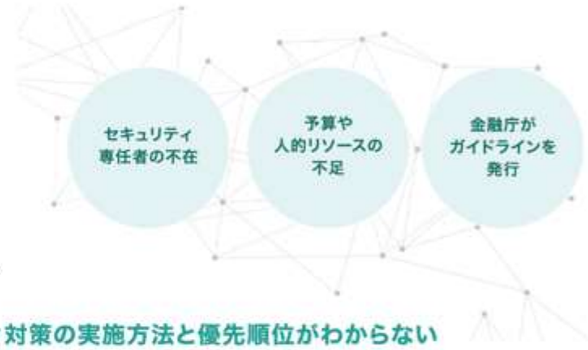
停滞していたセキュリティ課題への対応を、規程の整備などにより確実に進めることができました。
本事業を通して得た知識をもとに予算を確保し、EDR(※1)やパスワード管理ツールなど、新たなセキュリティ対策ツールの導入にも取り組んでいきます。

背景と課題

背景

人的リソース不足による整備の停滞と、証券金融業におけるセキュリティ要求の高まり

以前からセキュリティに関する課題が多くありましたが、近年はセキュリティ担当部署の人的リソース不足や専任者の不在が続き、セキュリティ対策が停滞していました。令和6年10月には金融庁の「金融分野におけるサイバーセキュリティに関するガイドライン」の発行が予定され、社内規程の見直しが必要でした。



課題

1. 証券金融業界で求められるセキュリティ対策の実施方法と優先順位がわからない
2. 従業員がインシデント発生による影響の重大さを十分に理解しておらず、知識と意識が不足
3. 情報資産として管理する対象が不明確で、アクセス権限の設定も明文化できていない

取組内容

取組1　自社のセキュリティ対策における課題の洗い出しと優先順位付け、セキュリティ規程を再検討

「金融分野におけるサイバーセキュリティに関するガイドライン」の遵守を目指し、本事業の専門家とともに、現在のセキュリティ対策における課題の洗い出しと優先順位付けを行いました。また、特にシステム障害発生時の対応手順に関するセキュリティ規程を再検討しました。

取組2　従業員へのセキュリティ教育を計画するとともに、月1回の全社会議にて注意喚起の機会を設ける

パスワードを記載した付箋をPCに貼ることを禁止するなど、デスク周りの整理を徹底しました。また、月に1回の全社会議では、インシデント事例を紹介しながら従業員への注意喚起を行っています。さらに、従業員向けの研修については、年に1回の実施を計画しています。

取組3　情報資産管理台帳における保護対象データなどの資産の明確化と、アクセス管理に関する規程の整備

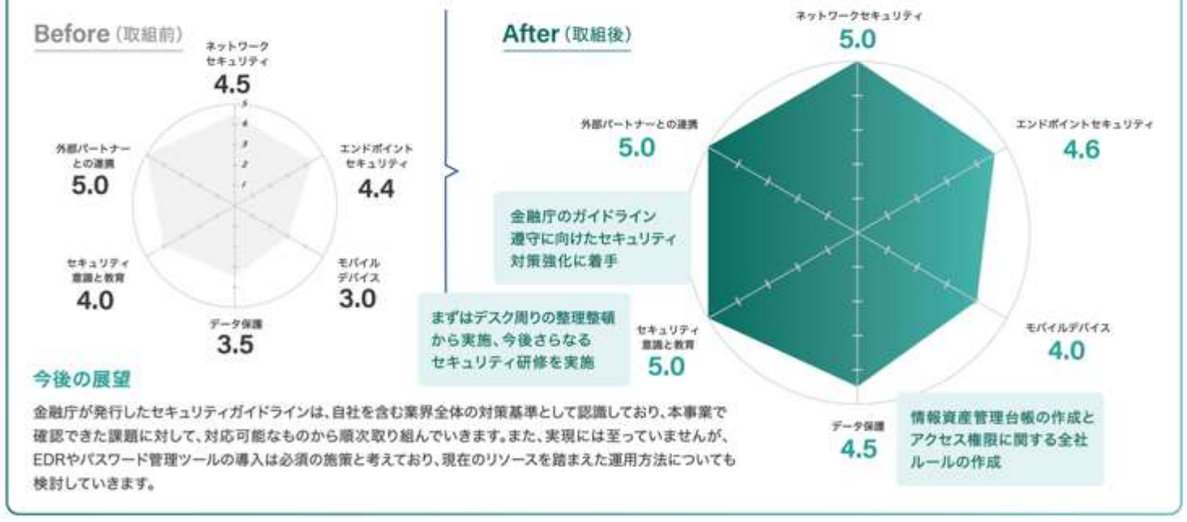
IPA(※2)が提供するリスク分析シートをもとに、情報資産管理台帳の作成に取り組みました。また、台帳作成と並行して、VPN(※3)接続時や重要データへのアクセス権限の付与について、情報の重要性とリスクを検討し、明文化することを目指しました。

※1　Endpoint Detection and Response(端末のセキュリティ脅威を検知・分析・対応するセキュリティ技術)　※2　独立行政法人情報処理推進機構
※3　Virtual Private Network(仮想専用通信網)

結果と今後

1. 再検討したセキュリティ規程は、無事に取締役会で決議され、運用を開始しました。また、金融庁のガイドラインに対し、自社のリソースや現在の対応状況を考慮した結果、現時点ではすべての項目に対応することが難しいため、実現可能な項目から進めていきます。　→　解決
2. 従業員向けの研修については、外部講師の招致も検討しつつ、全社会議での注意喚起を行います。また、ベンダーと協力して定期的にインシデント対応訓練を実施し、セキュリティ意識の向上に努めます。令和7年度には標的型攻撃メール訓練の実施も検討しています。　→　継続
3. 令和7年度には、情報資産管理台帳をたたき台として社内に共有できる状態を目指しています。これにより、保有する情報資産の整理と、重要なデータへのアクセス権限の管理を統一します。たたき台を作成後も定期的に見直し、最終的な完成を目指します。　→　継続

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連携



今後の展望

金融庁が発行したセキュリティガイドラインは、自社を含む業界全体の対策基準として認識しており、本事業で確認できた課題に対して、対応可能なものから順次取り組んでいきます。また、実現には至っていませんが、EDRやパスワード管理ツールの導入は必須の施策と考えており、現在のリソースを踏まえた運用方法についても検討していきます。

経営層の声

本事業を通じて、自社の課題を把握でき、セキュリティ強化に非常に役立ちました。担当者のセキュリティ知識が向上したことで、予算検討時に具体的な必要性を根拠として示してくれるため、経営層としても判断しやすくなりました。今回を契機に、セキュリティ対策をさらに推進していきます。

参加者の声

本事業に参加したことで、セキュリティ対策について多面的な視点を持てるようになり、経営層との対話の質が高まりました。稟議を提出する際に、対策の必要性や選定基準をコストを交えて明確に説明できるようになり、以前よりも説得力が増したと感じています。

サービス・その他

人事総務アウトソーシング業　K社

セキュリティ認証の取得に満足することなく、盤石なセキュリティ管理体制で顧客の安心感を担保

企業プロフィール
- 業　　種：サービス業
- 従業員数：～50名

セキュリティ体制　複数名体制/兼務

事業内容　海外駐在員やその家族に向けた生活支援サービスを提供しています。日本食や日用品などのECサイトを運営するほか、企業の人事・総務部門向けに福利厚生の提案も行います。また、海外赴任・帰任時の家財移動サポートや、有料人材紹介・派遣サービスも展開しています。

背景と課題

Pマーク(※1)の取得時に、セキュリティ対策は一通り整備しましたが、対策として十分なのか不安に感じていました。

取組内容

ベンダーに問い合わせて、セキュリティ対策状況や契約内容を確認しました。また、座談会形式で従業員とセキュリティについての勉強会を行いました。

結果と今後

本事業の取組により、自社が目指すべきセキュリティ対策が実行できていることを確認しました。
また、セキュリティ対策に関する意見を出しやすい環境を整えることができました。今後は、セキュリティ対策に能動的に取り組むため、ベンダーとの協議を進め、セキュリティ体制の強化に努めます。

背景と課題

背景

Pマークは取得済みだが、セキュリティ対策レベルや実効性に不安を感じる

Pマークの取得に合わせて、セキュリティ規程などの体制を整備しました。しかし、実際のサイバーセキュリティの脅威に対して、現状の対策で十分かどうか不安を感じていました。また、従業員のセキュリティ意識には個人差があり、より実態に即したセキュリティ対策の強化が必要だと考えています。

課題

1. セキュリティ運用をベンダーに任せており、自社のセキュリティ対策が把握できていない
2. 従業員がセキュリティに興味がなく、セキュリティ意識の醸成が必要
3. 自社のECサイトのセキュリティ対策レベルを検証できていない

取組内容

取組1　自社で取り組んでいるすべてのセキュリティ対策を把握し、自立したセキュリティ管理体制を目指す

ベンダーに問い合わせて、ファイアウォールの有無、デバイスのディスク暗号化、クラウドサービスのセキュリティ対策や監視状況、サーバの重要データの暗号化、サポート契約状況などを確認しました。確認結果については、本事業の専門家に評価を受けました。

取組2　メール訓練とセキュリティ対策に関する座談会を実施し、セキュリティリテラシーの向上を目指す

業務でメールを頻繁に使用しているため、従業員に対して標的型メールの訓練を実施しました。また、本事業のセミナーやワークショップで学んだ内容を、社内で座談会形式で共有しました。全従業員がセキュリティリテラシーを向上できるよう取り組みました。

取組3　自社のECサイトがサイバー攻撃に耐えられるか診断し、セキュリティ状況を正確に把握

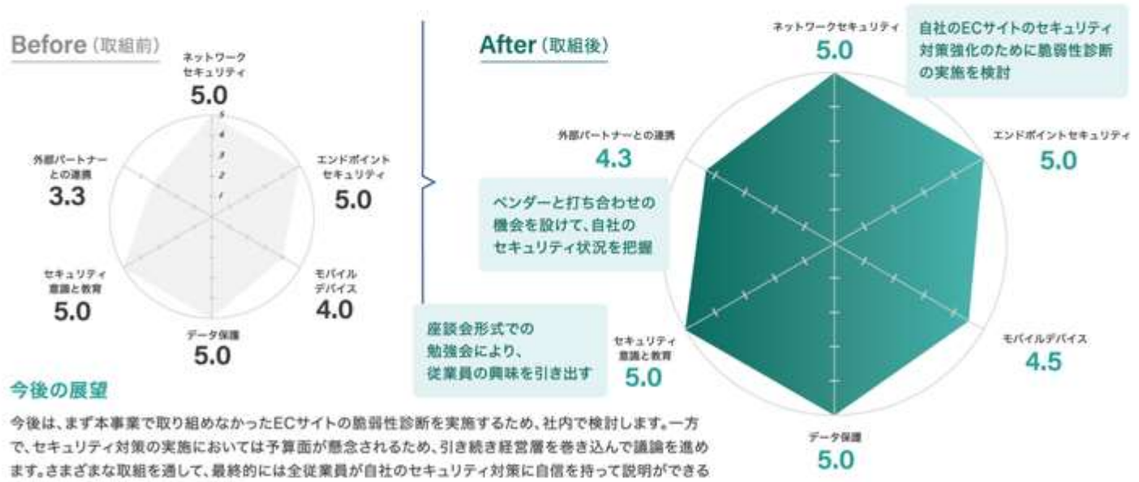
自社のECサイトのセキュリティ対策状況を把握するため、開発ベンダーと契約内容を確認し、脆弱性診断の実施を相談しています。
また、ECサイトからの個人情報やクレジットカード情報の漏えい防止のため、改ざん検知ソリューションの導入を検討しています。

※1　プライバシーマーク（個人情報を適切に取扱う体制を整備していると認定された事業者に付与）

結果と今後

1. 現在のセキュリティ対策は、自社が目指すべきレベルに達していることを確認しました。また、令和6年度中に、ベンダーとセキュリティ対策に関する打合せを行います。今後は、自社が能動的にセキュリティ対策に関与できるよう、ベンダーとの連携を強化していきます。　→　継続
2. これまで社内ではセキュリティ対策について議論が行われることはありませんでした。しかし、本事業の取組を通して、従業員から自社のセキュリティ対策について質問が増えました。従業員のセキュリティ意識が向上したことを実感しています。　→　解決
3. スケジュールの都合で現時点では脆弱性診断を実施できていませんが、令和7年度の実施に向けて、診断サービスの選定を進めています。経営層も脆弱性診断の実施には協力的で、診断結果から浮かび上がる課題への対策にも、積極的に取り組んでいきます。　→　継続

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連携



今後の展望

今後は、まず本事業で取り組めなかったECサイトの脆弱性診断を実施するため、社内で検討します。一方で、セキュリティ対策の実施においては予算面が懸念されるため、引き続き経営層を巻き込んで議論を進めます。さまざまな取組を通して、最終的には全従業員が自社のセキュリティ対策に自信を持って説明ができる状態となることを目指していきます。

経営層の声

サイバーセキュリティの危険性が年々高まる中、自社のセキュリティ体制が目指すべきレベルに達しているのかという不安を抱えていました。ただ、本事業を通して自社のセキュリティ体制を客観的に把握することができ、不安は払しょくされました。今後とも、社会から信頼を得られる企業を目指します。

参加者の声

本事業の専門家のアドバイスにより、自社のセキュリティ対策を再確認できました。社内で実施した座談会では、「セキュリティ体制の現状をもっと知りたい」という意見が出るようになり、コミュニケーションが活性化しています。今後とも、セキュリティ対策の運用ルールの改善に努めていきます。

サービス・その他

産業廃棄物処理業　L社

自社の業務や事業規模に見合った最適なセキュリティ対策を短期間かつ低コストで実現

企業プロフィール
- 業　　種：サービス業
- 従業員数：～50名

セキュリティ体制　複数名体制/兼務/経営者

事業内容　医療廃棄物の回収と運搬を行う企業です。医療機関に出向き、注射器、紙オムツ、廃酸、廃アルカリなどを回収して処分場まで運搬する事業を展開しています。循環型社会を構築する地球に優しい企業を目指しています。

背景と課題

ISMSの認証取得していますが、知識のあるセキュリティ担当者がいないため、必要なセキュリティ対策が完全ではないと感じていました。

取組内容

現状のネットワークやITインフラの活用状況を整理し、自社に必要なセキュリティ対策を洗い出し、優先順位をつけながら対応を進めました。

結果と今後

令和6年度中にEDR(※1)やUTM(※2)の本格運用を開始することにより、セキュリティ対策の対応を完了させる予定です。あわせて、ネットワーク構成図やPC配置図などのドキュメント更新を行い、トラブル発生時の迅速な対処に向けて継続的に整備します。

背景と課題

背景

専任のセキュリティ担当者がITに詳しくなく、必要なセキュリティ対策の検討や実行に苦労

小規模な事業者なりにセキュリティ対策を進め、ISMS認証を取得していました。しかし、自社のセキュリティ対策をより一層強化するために、本事業の専門家による第三者評価と、具体的で実行可能な支援が必要だと考えました。

課題

1. セキュリティ対策が有効か、ネットワーク装備やウイルス対策に先進性があるか不明
2. 事業規模にあわせて投資可能な範囲でのセキュリティ対策を行いたい
3. 既存システムやネットワーク機器の設置状況を完全には把握していない

取組内容

取組1　現状のIT・ネットワーク活用状況、取扱う情報などを共有し、必要なセキュリティ対策を検討

本事業で派遣された専門家に事業内容の詳細やIT・ネットワークの活用状況を共有し、自社に適したセキュリティ対策を検討しました。自社の事業規模や業務特性に応じたセキュリティ対策の課題を整理し、それぞれの課題に対する対応策とその優先順位の一覧を作成しました。

取組2　自社に最適なセキュリティ対策を検討し、EDRの全PC展開とUTMの新規導入を優先的に推進

昨年度、1台のPCに試験導入したEDRを全PCに展開しました。また、令和6年度には「中小企業サイバーセキュリティ基本対策事業」を活用してUTMを試験導入しました。本事業の専門家から機能面やログの見方についてアドバイスを受け、本格導入に向けた評価を進めています。

取組3　ネットワーク構成図やPCの配置図などのドキュメントを最新の内容に更新

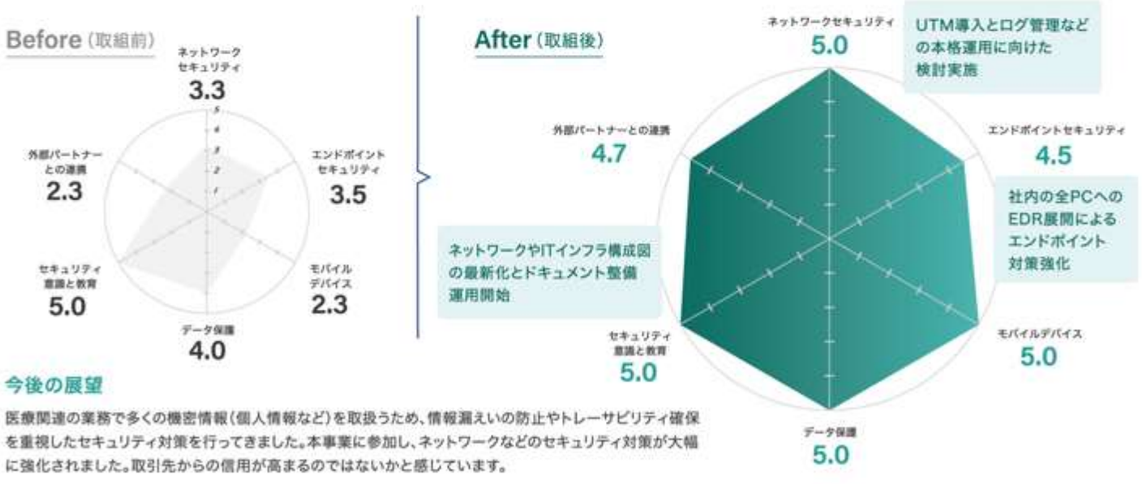
最新のネットワーク構成図などの資料が不足しているため、トラブル発生時に原因の特定や対処に時間がかかることが予想されました。そこで、ドキュメントの更新を行いました。本事業の専門家にネットワーク構成図の記載例を示してもらい、記載の粒度などを相談しながら作成しました。

※1　Endpoint Detection and Response（端末のセキュリティ脅威を検知・分析・対応するセキュリティ技術）
※2　Unified Threat Management 統合脅威管理（複数のセキュリティ機能を統合した管理システム）

結果と今後

1. ISMS認証を取得して運用していますが、セキュリティ対策が自社に適しているのかを確認したいと考え、本事業の専門家と共にセキュリティ対策の課題を洗い出しました。具体的な対策強化を行うことで、安心して日々の業務に取り組めるようになりました。　→ 解決
2. EDRを全PCに導入することでエンドポイントのセキュリティを強化しました。現在、UTMの試験運用を行っており、その結果を見ながら自社に適した製品とサポートベンダーを選定し、本格導入と運用を開始する予定です。　→ 解決
3. 社内で利用しているネットワークやITインフラを可視化して管理する重要性を理解しました。今後は、新たなITサービスやデバイスがあれば、当社にとって必要だと感じた場合、導入を検討します。　→ 解決

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連携



今後の展望

医療関連の業務で多くの機密情報（個人情報など）を取扱うため、情報漏えいの防止やトレーサビリティ確保を重視したセキュリティ対策を行ってきました。本事業に参加し、ネットワークなどのセキュリティ対策が大幅に強化されました。取引先からの信用が高まるのではないかと感じています。

経営層としての声

書類での業務が多いため、従業員に対しては日頃よりセキュリティ意識を持たせています。今回システム面でのセキュリティ対策も強化されたことで、全社的なセキュリティ意識を維持していく基盤ができました。こうした事業には経営者自ら参加し、率先して対応していくことが重要と感じています。

参加者としての声

他社の話を伺い、業務内容や事業規模、従業員数、業態によって必要なセキュリティ対策は異なり、さまざまなサービスを有効活用して、業務の効率化を進めていることを感じました。業務多忙でしたが、セキュリティ対策を考える有意義な時間となり、セキュリティ対策強化という十分な成果が得られました。

サービス・その他

広告業　M社

プロモーション事業の重要性を鑑み、緊急時の復旧対策整備と従業員のセキュリティ意識改革を実行

企業プロフィール
- 業　　種：学術研究・専門・技術サービス業
- 従業員数：～100名

セキュリティ体制　複数名体制/兼務

事業内容　WebやSNSキャンペーンの企画・アカウント運用に加え、広告代理業務などのセールスプロモーションを行っています。また、SNS運用時の事務局運営など、プロモーションに関わるさまざまなサービスを展開し、出版事業も手掛けています。

背景と課題

災害やテロなどの緊急事態におけるセキュリティ体制や従業員に対するセキュリティポリシーの浸透、モバイルデバイスの運用に不安がありました。

取組内容

LANのセグメントやケーブル配線の見直し、セキュリティ教育資料の作成、スマートフォンの利用状況に関する現状調査と管理方法の検討を行いました。

結果と今後

LANを複数セグメントに増やし、乱雑であったLANケーブルを整理したことでメンテナンス性が担保され、BCP(※1)が強化できました。またセキュリティポリシーを教育に取り込んだ結果、従業員のセキュリティ意識も大きく前進し、モバイルデバイスの管理についても安心できました。

背景と課題

背景

Pマーク(※2)とISMS認証を取得したものの不安が残る

業務で個人情報を取扱うためセキュリティインシデントは大きな脅威です。このためPマークとISMS認証を取得したものの、従業員に対するセキュリティポリシーの浸透、自社のセキュリティ対策、モバイルデバイスの運用、緊急事態でのセキュリティ体制などに不安を感じていました。

課題

1. 乱雑に配置されたLANケーブルのメンテナンス性が悪く、災害時の復旧作業を懸念
2. 従業員へのセキュリティポリシーの浸透に不安があり、意識向上への取組ができていない
3. 従業員が使うモバイルデバイスのセキュリティ対策と運用ルールが定まっていない

取組内容

取組1　LANケーブルを整理することでメンテナンス性を向上させBCPを強化

本事業の専門家のアドバイスに基づき、1セグメントで運用していたLANを複数セグメントに分割しました。物理的にも乱雑だったLANケーブルを整理し、メンテナンス性を向上させました。また、サーバラックを鍵付きにするなどのセキュリティ対策も実施しました。

取組2　従業員へのセキュリティ教育にセキュリティポリシーを取り込み、教育及びテストを実施

セキュリティ教育に、これまでのコンプライアンス遵守と個人情報保護の2軸に加えて、標的型メールへの対応やテレワーク時の注意点などセキュリティポリシーの具体的な内容を盛り込み、確認テストまで実施することにより、従業員に定着しやすいと自信が持てる内容となりました。

取組3　従業員が使用するスマートフォンのセキュリティ状況と利用状況を確認

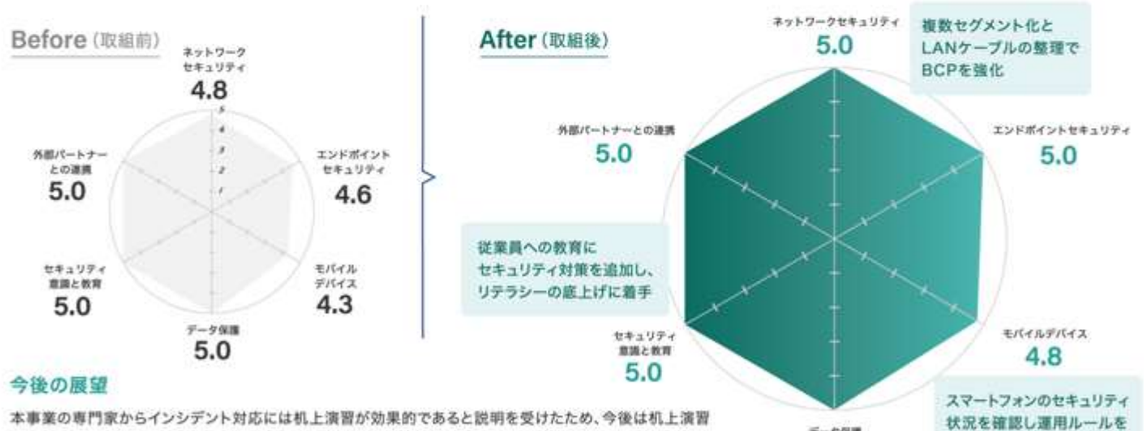
MDM(※3)の導入を念頭に現在の使用状況を確認したところ、従業員のスマートフォンは電話の利用が中心で業務での使用頻度が低いことあわせて、リモートロックやリモートワイプ機能の設定が可能であることなどが判明しました。

※1 Business Continuity Plan(事業継続計画)　※2 プライバシーマーク(個人情報を適切に取扱う体制を整備していると認定された事業者に付与)
※3 Mobile Device Management(モバイル端末を一元的に管理する仕組み)

結果と今後

1. LAN環境の整備により、トラブル発生時や災害などの緊急事態における調査や迅速な復旧対応が可能となりました。また、IPアドレスを容易に増やせるようになったので、今後の事業規模拡大や人員増強にも迅速に対応できるようになりました。　→ 解決
2. 教育後の確認テストでは再テストの基準を設けましたが、再テストが必要な従業員はいませんでした。全社としてセキュリティリテラシーの向上を実感しています。今後も継続して資料をアップデートし、計画的に教育を実施していきます。　→ 解決
3. 本事業の専門家との相談と調査の結果、クラウドサービスのアカウントの一時停止やスマートフォンの初期化が必要であることが判明し、MDMの導入は見送りました。一方で、これまで実施してきたスマートフォンの使用状況の確認は、引き続き実施します。　→ 解決

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連携



今後の展望

本事業の専門家からインシデント対応には机上演習が効果的であると説明を受けたため、今後は机上演習を実施し、インシデント発生時の対応や連絡経路などを随時見直していきます。また、従業員のセキュリティリテラシーには個人差があるため、こまめな情報共有や定期的な教育を継続していきたいと考えています。さらに、アカウント管理の強化を通じたセキュリティ向上のツール導入も検討しています。

経営層の声

セキュリティ対策は、事業の安定性につながる会社の中核と捉えています。本事業を通じて取り組んだ課題への対応や教育により、自社のセキュリティリテラシーはさらに向上したと感じています。これからも変化するセキュリティのトレンドを把握しながら、対策を強化していきます。

参加者の声

ぜひ多くの企業に参加してほしい事業です。本事業の専門家からの宿題で、セキュリティ対策と生産性の両立を妨げる原因を解決し、未解決の課題に取り組む良い機会となりました。学んだことを今後のセキュリティ対策に活かしたいと思います。

サービス・その他

人材支援サービス業　N社

企業プロフィール
- 業　　種：サービス業
- 従業員数：～300名

セキュリティ体制　1名体制/兼務

事業内容　若手人材の就職・転職支援、業界特化型採用支援、事業開発コンサルティングなどの幅広い事業を展開しています。各分野において、戦略立案から運用代行まで一貫してサポートを行い、企業の成長や業務効率化に貢献しています。

セキュリティルールの整備とインシデント対応力の向上、社内の情報資産の管理体制強化を実現

背景と課題
個人情報を扱うもののセキュリティルールの整備が不十分であり、インシデント発生時の対応やシャドーIT(※1)対策に不安を感じていました。

取組内容
セキュリティルールの整備とインシデント発生時の初動対応の迅速化に取り組みました。また、シャドーIT対策として資産管理ツールを導入しました。

結果と今後
本事業の専門家のアドバイスを受け、セキュリティルールの整備を進めました。また、資産管理ツールの導入により、社内のシャドーITの使用状況を把握できるようになりました。今後は運用ルールを随時更新するとともに、バックアップ方法も検討しながら、組織全体での運用体制強化を目指します。

背景と課題

背景
基本的なセキュリティ対策は行っているが、運用面の整備が不十分で安全性に懸念

Pマーク(※2)の取得やEDR(※3)の導入は行っていますが、1名体制でセキュリティを管理しているため、効率的な運用が難しく、現在の対応が適切かどうか判断できませんでした。
また、セキュリティルールは作成していますが、シャドーITの常態化など対策が不十分であり、安全性に懸念がありました。

課題
1. セキュリティルールが整備されておらず、従業員にセキュリティ対策が定着していない
2. 情報資産管理体制が不十分で、社内でシャドーITの存在が確認されている
3. 社内データへのアクセス権限の管理が不十分で、データ消失や情報漏えいのリスクがある

取組内容

取組1　セキュリティルールの整備に取り組み、従業員へのセキュリティ対策の定着を図る

IPA(※4)の提供する「情報セキュリティハンドブック」を参考に、セキュリティルールの整備に取り組みました。文書には、インシデント対応やAIの活用、クラウドサービスの利用ルールなどを盛り込みました。また、従業員が理解しやすいように、用語集も追加しました。

取組2　社内のシャドーITの使用状況を把握するために、資産管理ツールを導入

社内のシャドーITの使用状況を把握するため、新しくクラウドサービス型の資産管理ツールを導入しました。また、会社支給のスマートフォンにはMDM(※5)を導入し、許可されていないアプリケーションのダウンロードや特定のWebサイトへのアクセスを制限しました。

取組3　オンプレミスのサーバ構築やストレージサービス活用によるデータ保護とアクセス権限の見直し

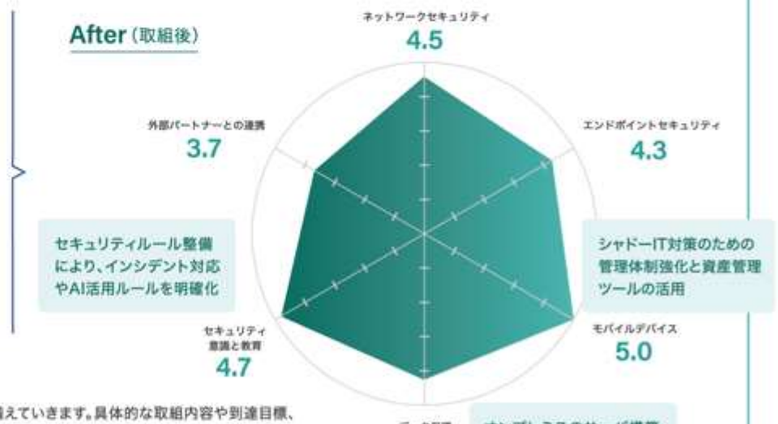
取扱うデータの増加に伴い、古いデータの管理にオンプレミスのサーバ構築やストレージサービスの導入を進め、万一インシデントが発生してもデータを保護できる環境を整備しています。また、アクセス権限の付与に関するルールやフォルダの管理方法の見直しも行いました。

※1　企業の管理部門が把握していないIT機器やソフトウェア、クラウドサービスのこと　　※2　プライバシーマーク（個人情報を適切に取り扱う体制を整備していると認定された事業者に付与）
※3　Endpoint Detection and Response（端末のセキュリティ脅威を検知・分析・対応するセキュリティ技術）　　※4　独立行政法人情報処理推進機構
※5　Mobile Device Management（モバイル端末を一元的に管理する仕組み）

結果と今後

1. 作成したセキュリティルールは、令和7年度中の本格運用を目指しています。このルールにより、従業員のセキュリティ意識が統一され、さらなる対策強化が可能となります。今後は定期的に見直すことで、より実態に即した内容に改善していきます。　→　継続
2. 資産管理ツールやMDMの導入により、従業員が使用しているソフトウェアやサービスが可視化されました。これをもとに、規制すべきソフトウェアやサービスの基準を検討していきます。今後も効率的な運用を進め、データ保護の体制を強化していきます。　→　解決
3. データ保存環境を整備するとともに、契約中のクラウドサービスをアップグレードし、ストレージ容量の拡張やアクセス管理を強化しています。これにより、特に退職者によるデータ流出や消失のリスクを低減し、より安全なデータ管理体制を実現します。　→　継続

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連携



今後の展望
自社のセキュリティレベルを高めることで、将来的な上場にも備えていきます。具体的な取組内容や到達目標、優先順位について議論を重ね、対策を推進していきます。また、過去に取得したPマークに加え、ISMS認証やISO/IEC27001認証などの取得も検討します。従業員のセキュリティ知識を強化するため、資格取得を全社的に推奨していく予定です。

経営層の声
本事業の取組を通じて、自社が目指すべきセキュリティ体制をロードマップとして明確に理解し、理想の体制に対する現状の立ち位置や今後、優先すべき課題を把握することができました。
また、セキュリティに関する知識を社内に蓄積できたことも大きな成果であると考えています。

参加者の声
セキュリティ文書や運用体制の整備において、本事業の専門家からアドバイスを受け、自社の課題を改めて認識するとともに、多くの気づきを得ることができました。今回得られた知見を活かし、必要に応じて外部リソースも活用しながら、実効性のあるセキュリティ体制の構築に取り組んでいきます。

サービス・その他

飲食サービス業　O社

上場に向けたセキュリティ管理強化のため、現場のインフラ整備やセキュリティ意識向上へ取り組む

企業プロフィール
- 業　　種：宿泊業・飲食サービス業
- 従業員数：～300名

セキュリティ体制　1名体制/兼務

事業内容　レストラン事業を中心に、多角的に事業を展開しています。全国で自社ブランドを直営展開することに加え、フードコート運営、惣菜事業、ケータリングサービスなど、さまざまな業態を通じて幅広く「食」のシーンに貢献しています。

背景と課題

多店舗展開を支えるITインフラ整備が課題です。
また、1,000名超の従業員に対し、1名体制でセキュリティ対策を進めることに不安がありました。

取組内容

店舗システムの集中管理によるセキュリティ環境構築、現場従業員のセキュリティ意識向上を目的とした教育プログラム改善などを開始しました。

結果と今後

リモートツールの導入によって集中管理が可能となり、担当者の負担を軽減しました。
また、人事研修にセキュリティ教育を組み込み、現場の意識向上を図ります。今後は情報資産の棚卸しやインシデント対応マニュアルの策定、経営層の理解促進を進め、全社的なセキュリティ体制の強化を目指していきます。

背景と課題

背景

1,000名を超える従業員に対し、1名体制でのセキュリティ対策が困難

飲食業界において、多店舗展開を支えるITインフラ整備は重要な課題です。同社では従業員1,000名以上を抱える中、情報システム部門の担当者が1名というリソースの制約があり、店舗ごとの端末管理や従業員のセキュリティ意識の向上といった課題が依然として残っていました。

課題

1. 自社のリソース不足により、十分にセキュリティ管理体制の構築ができていない
2. セキュリティ教育が不足しているため、従業員によるインシデント発生のリスクあり
3. パスワードが簡易的なものとなっており、データ保護の観点でリスクを抱えている

取組内容

取組1　直接現場に出向くことなく、店舗端末の集中管理ができるセキュリティ管理体制を構築

これまでは店舗のシステム環境が整備されておらず、セキュリティパッチの適用や必要なツールのインストールのために、担当者が店舗で作業する必要がありました。そこで、担当者の負担軽減のため、直接現場に向かわなくても集中管理ができる環境構築に取り組みました。

取組2　従業員の教育プログラムを見直し、希薄だったセキュリティ意識の底上げを計画

従業員のセキュリティ意識が低いという課題を痛感しており、セキュリティに関する教育プログラムの策定が必要と判断しました。既に人事部門で実施している研修にセキュリティ教育を盛り込む方向で調整を進め、従業員のセキュリティ意識を底上げしていきます。

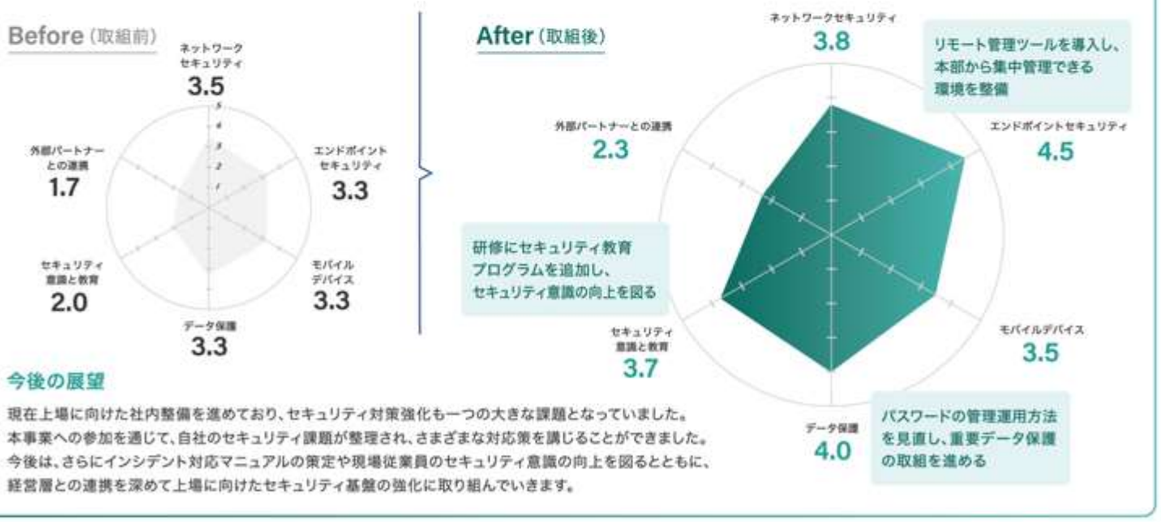
取組3　パスワード管理体制を構築し、重要データの情報漏えいリスクを低減

本事業の専門家から、サーバやネットワーク機器のパスワードが簡易的なものとなっているという指摘を受けました。そのため、管理対象の機器やツールを洗い出し、パスワード変更を行うとともに、パスワードのリセットなどの運用管理方法の見直しを行いました。

結果と今後

1. リモート管理ツールの導入により、店舗システムのメンテナンス作業を本部から効率的かつタイムリーに実施できるようになりました。店舗システム環境の監視や更新の作業漏れ防止などの対応ができたことで、店舗システムのセキュリティ環境が改善されました。　→ 継続
2. 既に実施している新入社員研修、中途採用者研修、店長研修に、不審メールの危険性など現場で起こり得る具体的な事例を盛り込みます。今後も高いセキュリティ意識を保てるよう、さまざまな事例を参考にして改善を重ねていきます。　→ 継続
3. 店舗では、令和7年1月から生体認証の実運用を開始しており、重要データ保護の取組が前進しました。今後は情報資産の棚卸しと適切なリスク評価を進め、優先順位を明確にした上で計画的にセキュリティ対策に取り組み、リスク最小化を目指します。　→ 継続

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連携



今後の展望

現在上場に向けた社内整備を進めており、セキュリティ対策強化も一つの大きな課題となっていました。
本事業への参加を通じて、自社のセキュリティ課題が整理され、さまざまな対応策を講じることができました。
今後は、さらにインシデント対応マニュアルの策定や現場従業員のセキュリティ意識の向上を図るとともに、経営層との連携を深めて上場に向けたセキュリティ基盤の強化に取り組んでいきます。

経営層の声

本事業を通じて、これまで漠然としか理解できていなかったセキュリティ対策の重要性を具体的に把握できました。
教育プログラムにセキュリティ要素を盛り込むなど取り組むべき具体的な施策も実行できたため、今後は従業員の意識改革と業務効率化の両立による更なる推進に期待しています。

参加者の声

セミナーやワークショップでは、他社との交流で新たな気づきを得ることができ、1人で抱えていた悩みを共有できた点が非常に有意義でした。また、本事業の専門家からアドバイスを受け、気づいていなかった課題が明確になり、計画に基づき期日までに取組ができたことは成果と捉えています。

サービス・その他

その他サービス業　P社

企業プロフィール
- 業　　種：サービス業
- 従業員数：～300名

セキュリティ体制　複数名体制/兼務

事業内容
産業廃棄物の収集運搬から中間処理まで一貫したサービスを通じて資源循環型社会の構築に取り組んでいます。迅速かつ安全な収集運搬や、中間処理工場での適正処理により、環境負荷の低減と高いリサイクル率の実現を目指しています。

外部の攻撃によるインシデントが発生し業務がストップ 過去の経験を活かし再発防止策を徹底

背景と課題
過去のインシデント経験から社内のセキュリティ対策を再検討していましたが、データ保護や従業員へのセキュリティ教育など課題が山積みでした。

取組内容
従業員へのセキュリティ教育を行うとともに、UTM(※1)やVPN(※2)などのセキュリティ機器の検討、PCのディスク暗号化に取り組みました。

結果と今後
本事業の取組を通して、従業員のセキュリティ意識の向上を実感しています。しかし、まだ従業員により個人差があるため、定期的に教育を行うことで組織全体の意識向上を図ります。また、セキュリティ機器を有効活用できていないことが判明したので、ベンダーと継続的に協議をしていきます。

背景と課題

背景

インシデント経験により セキュリティ対策の重要性を認識したが、 取るべき対策が山積み

過去に外部からの攻撃によるインシデントで、業務が1日停止した経験があります。セキュリティに関する専門知識が不足しており、セキュリティ製品の設定方法や対策の妥当性について判断できずにいました。そのため、外部からのネットワークアクセスや社内からの情報流出に対して対策が不十分でした。

課題

1. 従業員のセキュリティ意識が低く、インシデント発生のリスクが高まる
2. 社外からアクセス可能な社内ポータルサイトへのパスワード等のセキュリティ対策が未実施
3. PCの持ち出しが業務上発生するにもかかわらず、データが暗号化されていない

取組内容

取組1　フィッシングメール訓練や人為的な要因によるインシデント事例を共有し、セキュリティを自分事に

以前から一斉メールや社内ポータルサイトでのセキュリティに関する注意喚起は行っていましたが、従業員の意識向上にはつながりませんでした。そこで、人為的要因によるインシデント事例の共有やフィッシングメール訓練を通し、従業員が自分事に感じられる教育を行いました。

取組2　UTMの設定見直しとVPN導入により、外部からのアクセスの安全性を担保する

インシデント被害を受けた際は、社内のWebサーバにリモートデスクトップ接続ができる状態でした。そこで、本事業の専門家とともに導入済みのUTMの設定を見直しました。合わせて、VPNの導入も進め、ネットワークとリモートアクセスの安全性を担保します。

取組3　社外でのPC紛失に備え、ディスク暗号化による機密情報の保護体制を強化

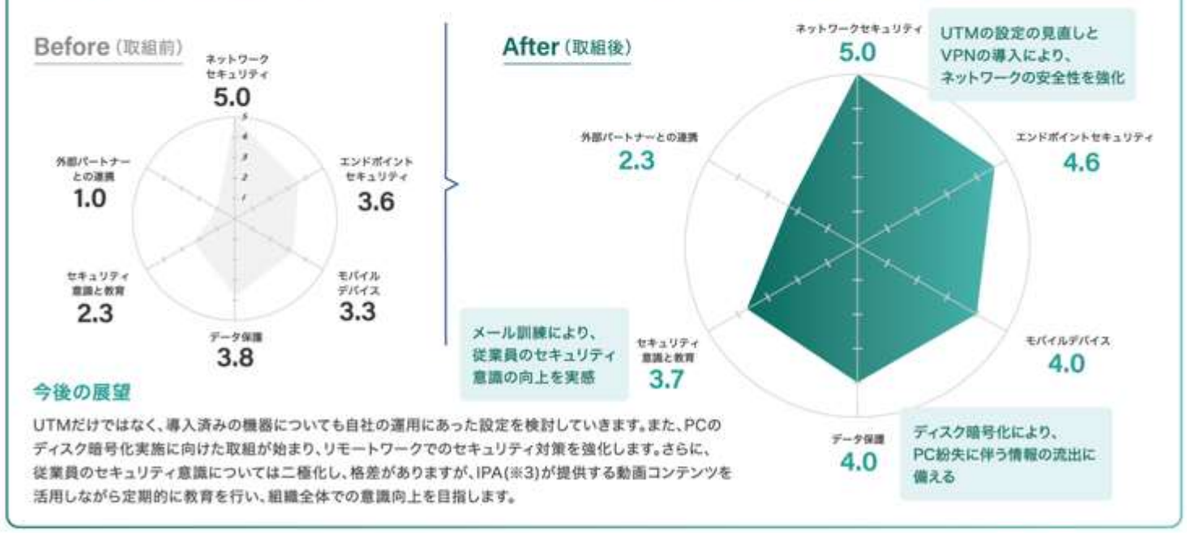
営業職の従業員がPCを社外へ持ち出すことがありますが、ディスクの暗号化がされていないことが判明しました。そこで、ディスクの暗号化ツールの導入を検討しました。併せて、データ復号時の鍵の管理方法について、アクセス管理ツールの活用も検討しました。

※1　Unified Threat Management 統合脅威管理（複数のセキュリティ機能を統合した管理システム）　※2　Virtual Private Network（仮想専用通信網）
※3　独立行政法人情報処理推進機構

結果と今後

1. 不審なメールを受け取った際に適切に報告する意識が醸成され、従業員のセキュリティ意識の向上を実感しました。一方でメール内のURLをクリックしてしまう傾向にあることが判明しました。フィッシングメールの開封率を全従業員の10%以下を目指します。　→ 解決
2. VPNについてはベンダーと対応範囲の協議をしており、令和6年度中には導入が完了し運用を開始します。また、取組の過程で、UTMのポート制限ができていないことが判明しました。そこで、ベンダーと制限すべき通信の確認を行い、適切な制限を設定します。　→ 継続
3. ディスク暗号化ツールについては、OSに標準搭載されているツールを使用する方向で計画をしています。OSのバージョンアップデートの兼ね合いもあり、現在は保留にしていますが、今後の導入によりPCを紛失した際のデータ保護を実現したいと考えています。　→ 継続

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連携



今後の展望
UTMだけではなく、導入済みの機器についても自社の運用にあった設定を検討していきます。また、PCのディスク暗号化実施に向けた取組が始まり、リモートワークでのセキュリティ対策を強化します。さらに、従業員のセキュリティ意識については二極化し、格差がありますが、IPA(※3)が提供する動画コンテンツを活用しながら定期的に教育を行い、組織全体での意識向上を目指します。

経営層の声

インシデント発生時には業務が止まり、多くの困難を経験したことから本事業へ参加しました。本事業の専門家派遣により、取り組むべき課題の優先順位と具体的な対策の道筋が明確になりました。経営層として今後もリソースを活用し、教育とシステム両面からセキュリティ対策の強化を図っていきます。

参加者の声

本事業のセミナーやワークショップを通じ、他社の実践例から新たな視点を得るとともに、自社のセキュリティ状況を見直すきっかけとなりました。特に、本事業の専門家のアドバイスにより、未整備だった領域の課題が明確になり、社内教育やシステム運用の方向性を社内で共有でき、とても有意義でした。

サービス・その他

総合コンサルティングサービス業　Q社

求められる高いセキュリティ水準に応じて、セキュリティポリシーとインシデント対応フローを全面刷新

企業プロフィール
- 業　　種：学術研究・専門・技術サービス業
- 従業員数：～300名

セキュリティ体制　複数名体制/兼務

事業内容　中小企業を中心に幅広いサポートを行っています。税務や会計、経営の支援をはじめ、企業の成長や課題解決を目的としたサービスを提供しています。また、法務や労務、資金調達といった分野でもサポートを展開し、企業活動を多角的に支える体制を整えています。

背景と課題

取引先が求めるセキュリティ水準は高まっている一方で、自社の対策は遅れており、従業員のセキュリティ意識にも個人差があると認識していました。

取組内容

パスワードポリシーやインシデント対応フローを見直し、セキュリティ水準を強化するとともに、従業員全体のセキュリティ意識の向上を図ります。

結果と今後

自社の体制にあったセキュリティ対策を実施した結果、取引先からの信頼獲得に向けて前進できました。
パスワードポリシーの更新やインシデント対応フローの策定などを進めたことで、取引先に対して自社の取組を説明できるようになりました。今後は、従業員の意識改革に向けた仕組みを構築します。

背景と課題

背景

各種文書の整備の遅れや従業員のセキュリティ意識の個人差により、対策が進んでいない

脆弱なパスワードが使われていたり、インシデント対応の文書が整備されていないなど、取引先が求めるセキュリティ水準に合っていない状況が発生していました。また、従業員からはセキュリティ対策の強化よりも、業務効率を求める意見が多く、従業員とのセキュリティ意識の共有にも課題がありました。

課題

1. パスワードポリシーが古く、取引先が求めるセキュリティ水準を満たせていない
2. インシデント対応フローが十分に整備されておらず、対応手順や責任者が不明確
3. 従業員のセキュリティ意識に個人差があり、テストを受講しない従業員も存在

取組内容

取組1　取引先が求めるセキュリティ水準を満たすため、新しいパスワードポリシーの策定などの文書化を実施

これまで6桁のパスワードが多く使われ、変更もされていませんでした。本事業のセミナーで単純なパスワード設定による脆弱性とそのリスクを学び、複雑かつ強固な設定を要求するパスワードポリシーを策定しました。また、重要データへのアクセス制限なども見直し、その文書化をしました。

取組2　自社のセキュリティ体制に基づいたインシデント対応フローを策定し、ドキュメントとして明文化

現在のインシデント対応フローは、箇条書きのメモのような文書しかなく、実際の運用に合っていませんでした。対応フロー図を作成することで視覚的にわかりやすくし、さらに、「誰がいつ、どういった動きをするのか」を明確にして、新しいインシデント対応フローを策定しました。

取組3　従業員へのセキュリティ教育を進めつつ、積極的にテストを受ける仕組みを構築

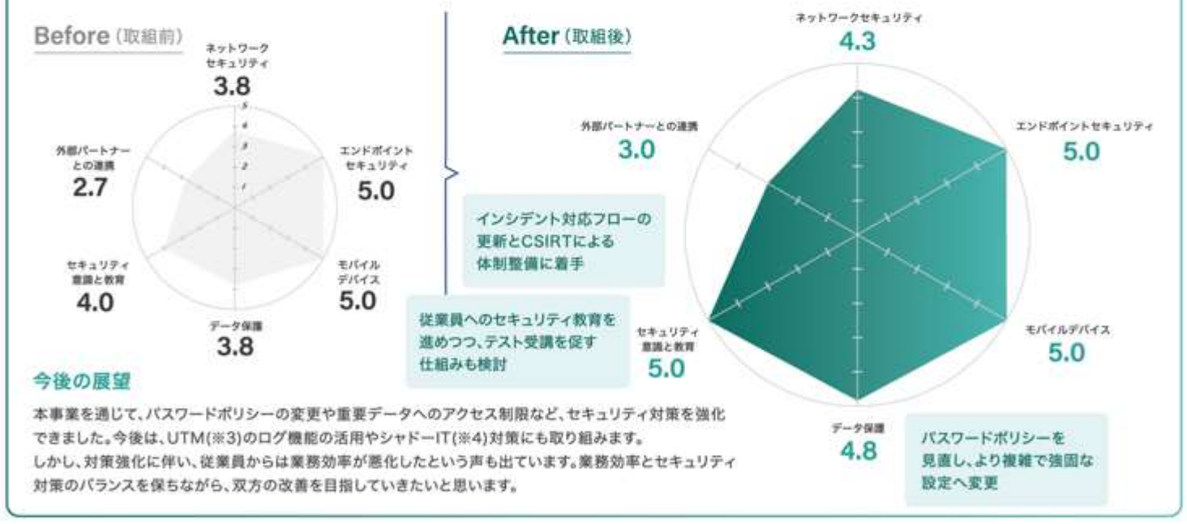
現在、eラーニングを活用したセキュリティに関するミニテストを週2回、各回3問程度実施しています。しかし、テストを受けない従業員も一定数いるため、テスト内容や頻度の見直し、またテストの結果を評価制度に反映させるなど、受講を促す仕組みを検討しました。

※1：独立行政法人情報処理推進機構　※2：Computer Security Incident Response Team（セキュリティインシデント対応の専門チーム）
※3：Unified Threat Management 統合脅威管理（複数のセキュリティ機能を統合した管理システム）　※4：企業の管理部門が把握していないIT機器やソフトウェア、クラウドサービスのこと

結果と今後

1. セキュリティポリシーの内容を抜粋して手順書と誓約書に記載することで、従業員が認識できるようにしました。今後新たに入社する従業員から新基準を適用し、既存の従業員は令和7年度から段階的にパスワード更新を行い、全社的に基準強化を進めます。　→ 解決
2. IPA(※1)の提供する「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」を参考に、CSIRT(※2)記述書の作成も進めています。フローの明文化により、社内で共通認識を醸成し、インシデント発生時の連携を迅速に行える体制を整備します。　→ 継続
3. テスト結果を評価制度に反映させることは引き続き検討していくことになりましたが、従業員のスキルアップを支援する社内制度を活用し、計画を進めています。また、未受講者の意見をもとにテスト内容を改善し、全従業員が取り組みやすい仕組みを作ります。　→ 継続

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連携



今後の展望

本事業を通じて、パスワードポリシーの変更や重要データへのアクセス制限など、セキュリティ対策を強化できました。今後は、UTM(※3)のログ機能の活用やシャドーIT(※4)対策にも取り組みます。
しかし、対策強化に伴い、従業員からは業務効率が悪化したという声も出ています。業務効率とセキュリティ対策のバランスを保ちながら、双方の改善を目指していきたいと思います。

経営層の声

本事業により、セキュリティ対策の方針や自社にあった対策を決定できたことは、非常に助かりました。特に、パスワードポリシーやインシデント対応の再構築に向けた動きは、取引先からの信頼を守るために重要だと考えています。今後は、さらに安全性を高めるための体制を構築していきます。

参加者の声

他社の取組を聞くことで、自社のセキュリティ状況を客観的に見直すことができました。特に、セキュリティ対策への予算が限られた企業と情報交換できたことは、非常に有意義だったと考えています。セキュリティ知識を体系的に学べたことも、本事業に参加して良かったと感じる点です。

サービス・その他

不動産売買業　R社

実務に則したマニュアル整備と従業員教育でセキュリティ対策強化

企業プロフィール
- 業　　種：不動産・物品賃貸業
- 従業員数：～300名

セキュリティ体制　複数名体制/兼務

事業内容
中古マンションの買取再販事業を通じて、リノベーションを施した理想の住まいを提供しています。独自ブランドを展開し、快適性・安全性を追求した価値ある住宅を届けます。また、10年間利用可能なアフターサービスを提供し、購入者に寄り添う総合的なサポートを行っています。

背景と課題

セキュリティマニュアルは作成していますが、実際の業務に適していません。また、インシデント対応や従業員のリテラシーの低さが課題となっています。

取組内容

シャドーIT(※1)の管理体制強化とマニュアルの見直しを進め、従業員のセキュリティ意識向上と迅速な初動対応が可能な運用体制の構築を目指しました。

結果と今後

本事業を通して、実務に即したセキュリティ対策の整備が進みました。また、従業員からセキュリティに関する前向きな声も聞こえるようになりました。今後も、全従業員がインシデント発生時に迅速な対応ができるよう、セキュリティ対策の浸透を目指していきます。

背景と課題

背景

最低限のセキュリティ対策は整備されているが、現場の業務運用とは合っていない

情報セキュリティに関するマニュアルは作成しているものの、実際の業務と合っていないため、あまり利用されていません。また、シャドーITの利用や社内のアカウント管理にも課題を抱えていました。また、従業員のセキュリティ意識の向上が進んでおらず、セキュリティ教育の見直しが急務となっていました。

課題

1. 社内で保有するアカウント管理の徹底やシャドーITへの対応が急務
2. 業務運用に合っていないマニュアルを見直し、現場業務とのギャップを解消
3. 従業員のセキュリティ意識の向上を目指し、セキュリティ研修の内容を見直したい

取組内容

取組1　シャドーIT対策とアカウント管理強化のため管理ツールを導入し、セキュリティ管理体制を整備

利用されていない社内のアカウントを把握し、シャドーITの利用実態とその影響を調査するため、いくつかの管理ツールを比較して導入を検討しました。また、アカウント管理表をもとに、従業員に付与されているアクセス権限の見直しを行い、アカウント管理体制を強化しました。

取組2　業務運用に適したマニュアルに修正することで、従業員の理解を促進し、実践可能な環境を整備

現在のセキュリティマニュアルが業務運用に適していない部分があると、本事業の専門家による評価を受けました。その結果、「社外の公衆Wi-Fiの利用について」、「パスワードの利用ルールに関する使い回しの禁止と強力な文字列への変更」についての内容を追加しました。

取組3　従業員へのセキュリティ研修や情報発信を通じ、全社的なセキュリティ意識の向上を促進

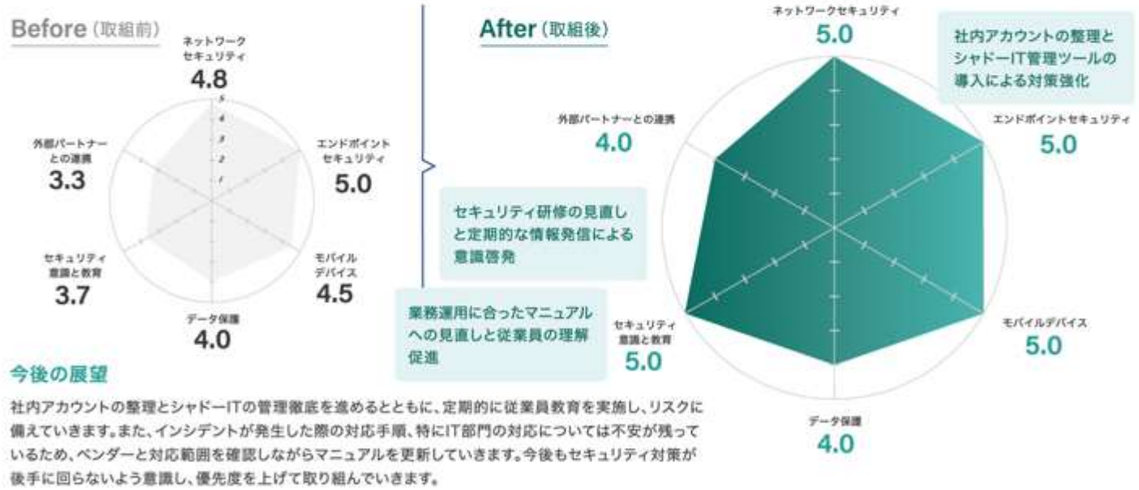
禁止している私用端末での業務利用が見受けられるため、インシデントの事例や損害状況を盛り込み、実務に近い内容を想定した研修内容に見直しました。セキュリティトレンドへの関心を高めるために、IPA(※2)のコンテンツの紹介などを定期的に社内に発信するようにしました。

※1　企業の管理部門が把握していないIT機器やソフトウェア、クラウドサービスのこと　　※2　独立行政法人情報処理推進機構

結果と今後

1. アカウント管理用のクラウドサービスの予算確保に向けて、本事業の専門家とともに発生可能性が高いセキュリティインシデントとそのリスクを整理し、経営陣に説明しました。これを受け経営陣も前向きに検討しており、令和7年度中に導入する予定です。　→　継続
2. 引き続きマニュアルを見直し、「インシデント発生時の初動対応と一次連絡先」、「生成AIの利用に関する注意事項」についてマニュアルに追記しました。インシデント対応については、ベンダーと対応範囲を確認し、自社としての対応手順を整理しています。　→　継続
3. 実務に即したセキュリティ情報を発信することで、従業員から前向きな声が聞かれるようになってきました。そのため、今後とも定期的な研修とトレンドに関しての情報発信を社内に続けていき、従業員全員のセキュリティ意識向上に努めます。　→　継続

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連携



今後の展望

社内アカウントの整理とシャドーITの管理徹底を進めるとともに、定期的に従業員教育を実施し、リスクに備えていきます。また、インシデントが発生した際の対応手順、特にIT部門の対応については不安が残っているため、ベンダーと対応範囲を確認しながらマニュアルを更新していきます。今後もセキュリティ対策が後手に回らないよう意識し、優先度を上げて取り組んでいきます。

経営層の声

本事業には、セキュリティ担当者の育成を目的として参加しました。担当者が着実に知識を習得し、成長していることを実感しています。情報セキュリティの重要性を再認識するとともに、セキュリティリスクの見える化とそれに対応する施策について費用対効果を鑑み実行していく必要があると感じています。

参加者の声

本事業のセミナー・ワークショップでは、基礎知識を体系的に学ぶことができ、大変有意義でした。また、実際にインシデントを経験した他社の方々とも話すことができ、サイバーセキュリティの脅威が決して他人事ではないと実感しました。今後も継続的に議論を重ね、自社に適した対策を実行していきます。

サービス・その他

システムインテグレーション業　S社

限られたコストや人的リソースを最大限活用し、全社でセキュリティ対策レベルを維持・強化

企業プロフィール
- 業　　種：情報通信業
- 従業員数：～300名

セキュリティ体制　複数名体制/兼務

事業内容　システム開発分野において独自の開発手法を提供しており、高価なミドルウェアを導入せずに、長寿命で拡張性の高いシステム構築を得意としています。さらに、企業内での開発・運用サポートも行うことにより、現代の情報化社会における真の効率化と利便性を追求しています。

背景と課題

ISMS認証の更新は経営方針として中止となりましたが、セキュリティ対策の維持・強化の方針には変更はなく、従来通り継続的な対策の検討が必要です。

取組内容

セキュリティ対策の課題として洗い出された、「BYOD(※1)端末のセキュリティ対策」や「業務データ保存の運用ルール策定」に取り組みました。

結果と今後

セキュリティに関わる検討は、新たに「ISMS事務局」から組織変更した「コンプライアンス委員会」で行っています。本事業での取組を全社にも反映させていくとともに、今回改訂した社内ルールの運用を徹底させ、必要に応じた見直しなどを行い、セキュリティ対策レベルの維持・向上に取り組んでいきます。

背景と課題

背景

ISMS認証の更新が中止となったものの、セキュリティ対策レベルの維持に変更なし

ISMS認証については、運用や更新にかかるコストの削減のため、経営方針として更新の中止を決定しましたが、従来通りのセキュリティ対策レベルの維持の方針に変更はありません。そこで、ISMS認証の更新などに予定していたコストや人的リソースを、セキュリティ対策の実施に振り向けることにしました。

課題

1. ISMS認証の更新が中止となり、セキュリティ対策の維持・強化方針の再検討が必要
2. BYOD端末のセキュリティ対策が不十分であることが判明
3. 業務で使用するファイルの保存運用が明確になっておらず属人化

取組内容

取組1　ISMS認証の審査に向けて作成した資料をベースに、分かりやすいドキュメントに再整備して展開

ISMS認証の審査に向けて作成していたセキュリティ関連のドキュメントを、実務に則した内容に分かりやすく改訂しています。インシデント発生時の対応フローについても、画像や図を使うことにより直感的に理解しやすい内容に見直して、全社に展開しています。

取組2　BYOD端末へのマルウェア対策ソフトウェア導入とデータ暗号化でエンドポイントセキュリティ強化

従業員には社給PCを貸与せず、BYOD端末を使用して業務を行っていますが、これらのセキュリティ対策が不十分だと判明しました。そのため、マルウェア対策ソフトウェアの導入とデータ暗号化の実施を決定し、全従業員に導入手順と必要性を周知し、導入後のエビデンスを取得しました。

取組3　業務データの保存先として、複数のファイル共有サービスを目的に応じて使い分けることに決定

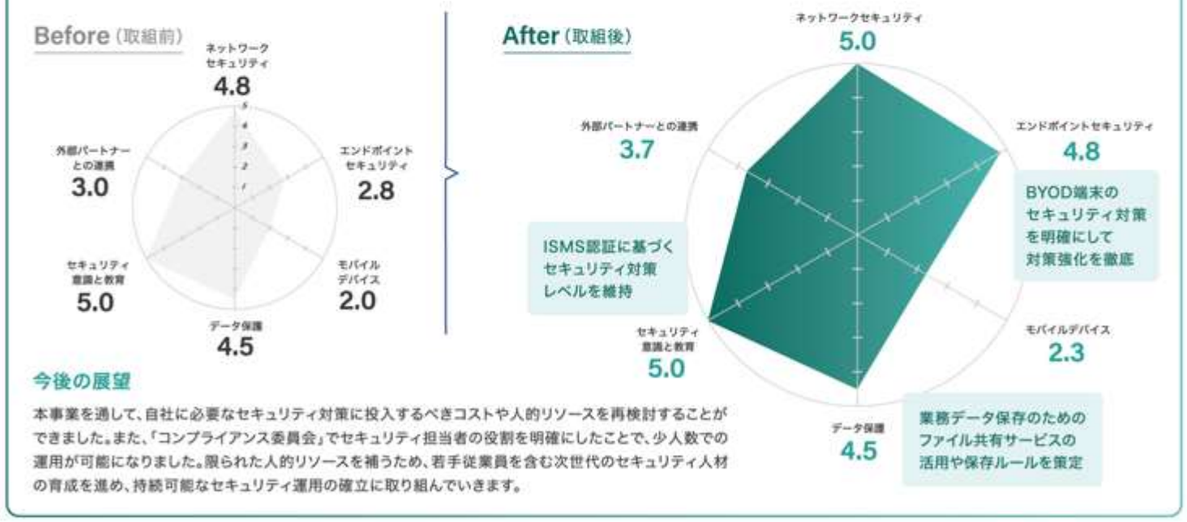
ファイルの保存先について、プロジェクトや業務の目的に応じてファイル共有サービスを使うことに決定しました。また、BYOD端末を利用する際に、不要なデータがローカルPC上に保存されないように、業務に必要な最低限のアクセス権限を各フォルダに設定し、ルールを再周知しました。

※1　Bring Your Own Device(個人所有のデバイスの業務利用)　※2　Mobile Application Management(モバイルアプリケーションを一元的に管理する仕組み)

結果と今後

1. 「ISMS事務局」から「コンプライアンス委員会」へ組織変更し、セキュリティ対策の検討を進めています。本事業で取り組んだ内容を全社で共有し、今回策定した社内ルールの運用を徹底することで、セキュリティ対策レベルの維持に努めます。　→　継続
2. BYOD端末のセキュリティ対策強化は、令和6年度中に完了する予定です。今後、端末運用の統合管理と効率化を進めるため、本事業の専門家のアドバイスを受けて、MAM(※2)の導入を検討しています。経営層も交えた議論を引き続き行っていきます。　→　継続
3. ファイル共有サービスの活用に関する運用ルールを策定しましたが、個々のプロジェクトや業務におけるファイルの参照や保存方法については、各業務担当者に判断を委ねています。退職者が使用していたデータの削除など、ファイルの一元管理も進めていきます。　→　継続

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連携



今後の展望

本事業を通して、自社に必要なセキュリティ対策に投入するべきコストや人的リソースを再検討することができました。また、「コンプライアンス委員会」でセキュリティ担当者の役割を明確にしたことで、少人数での運用が可能になりました。限られた人的リソースを補うため、若手従業員を含む次世代のセキュリティ人材の育成を進め、持続可能なセキュリティ運用の確立に取り組んでいきます。

経営層の声

本事業を通じて、自社の現状を把握し、効果的なセキュリティ対策を行うことの重要性を実感しました。属人化を解消しながら、効率的に運用できるセキュリティ管理体制の方向性が見えてきたと感じています。今後も経営層を含めた全社的な意識改革を進め、持続可能なセキュリティ運用の実現を目指します。

参加者の声

ワークショップを通して他社の課題や取組を共有する中で、自社の状況を客観的に把握することができました。また、中小企業でも工夫を凝らしてセキュリティ管理体制を維持していることに刺激を受け、自社の改善点を再認識する良い機会となりました。今後も社内の体制構築に貢献したいと考えています。

サービス・その他

金融商品取引業　T社

監査指摘を契機にセキュリティ対策の再検討を行い、金融庁のガイドラインへの準拠に目処を立てる

企業プロフィール
- 業　　種：金融業・保険業
- 従業員数：～300名

セキュリティ体制　複数名体制/兼務/経営者

事業内容　国内の商品先物取引、金融商品先物取引を行う企業です。国内商品市場の上場商品である金や原油、ゴム、農産物などを資産運用手段としてお客様に提案するとともに、国際情勢を踏まえた的確な情報を迅速に提供しています。

背景と課題

監査で指摘された事項の改善に向けて対応策が必要でした。また、自社のセキュリティ対策状況やセキュリティ担当者の知識を確認したいと考えました。

取組内容

自社のセキュリティ対策状況を数値化することで、現状が把握できました。また情報資産の整理やリスクの洗い出しを行い、セキュリティ管理規程を見直しました。

結果と今後

監査で指摘された「システムリスク評価」という課題をクリアすることができ、金融庁のガイドラインへの準拠についても見通しが立ちました。新たに従業員のセキュリティ意識と知識レベルをどのように向上させるかという課題が再認識されたため、継続的なセキュリティ教育の実施を検討しています。

背景と課題

背景

監査で指摘を受け、自社で独自に実施していたセキュリティ対策に不安あり

以前からUTM(※1)やVPN(※2)を導入し、セキュリティの確保に努めていましたが、セキュリティ対策について、監査で「システムリスク評価」が十分に行われていないという指摘を受け、現状の対策状況やセキュリティ担当者の知識レベルを第三者から評価して欲しいと考えていました。

課題

1. 金融庁のガイドラインへの準拠など、セキュリティ規程の整備やルール策定が遅れている
2. モバイルデバイスに対するセキュリティ対策が進んでいない
3. 従業員のセキュリティ意識を向上させる施策が不十分

取組内容

取組1　情報資産の整理とリスク分析を行い、セキュリティ管理規程の見直しを実施

監査では「システムリスク評価」が不十分との指摘を受けました。そのため、IPA(※3)が提供している「リスク分析シート」を活用しながら、自社の情報資産の整理、セキュリティリスクの分析・評価を行い、セキュリティ管理規程の見直しを進めております。

取組2　データ暗号化やOSのアップデート運用の徹底により、モバイルデバイスのセキュリティ対策を強化

本事業の専門家から、従業員が使うモバイルデバイスのセキュリティ対策についてアドバイスを受けました。そのアドバイスに従って、データを暗号化したり、OSを最新の状態に保ったり、パスコードを設定したりすることで、セキュリティ対策を一層強化しました。

取組3　従業員のセキュリティ意識の底上げなど、教育実施に向けた新たな課題を認識

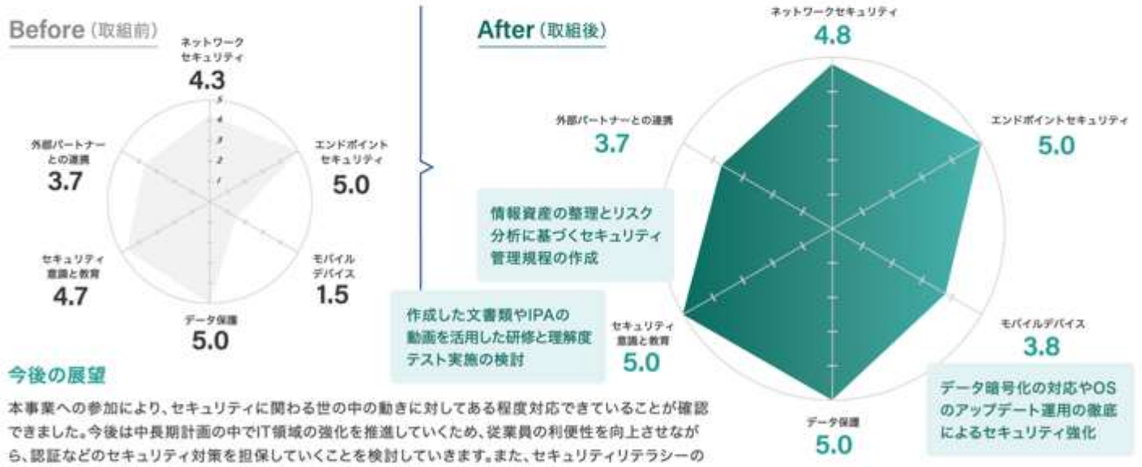
本事業の専門家との打合せやセミナー・ワークショップへの参加を通じて、セキュリティ担当者である自分の知識を体系的に整理することができました。新たに従業員のセキュリティ意識と知識レベルをどのように向上させるかという課題が生じました。

※1　Unified Threat Management 統合脅威管理（複数のセキュリティ機能を統合した管理システム）　※2　Virtual Private Network（仮想専用通信網）
※3　独立行政法人情報処理推進機構　※4　Mobile Device Management（モバイル端末を一元的に管理する仕組み）

結果と今後

1. セキュリティ管理規程などの見直しについては、令和6年度中に完了する予定です。監査での指摘事項についての改善も含め、令和6年10月に発表された「金融分野におけるサイバーセキュリティに関するガイドライン」への準拠についても目処が立ちました。　→ 解決
2. セキュリティ対策のさらなる強化策として、現在はモバイルデバイスへの生体認証の導入に向けた検討を行っています。また、今後はモバイルデバイスに対するリモートでのデータ削除やデバイスロックのため、MDM(※4)の導入などを継続検討していきます。　→ 継続
3. 今回作成したセキュリティ管理規程を使った研修やIPAの提供しているセキュリティ対策関連動画の視聴、セキュリティ対策演習などにより、従業員のセキュリティ教育を実施します。研修の実施後には理解度テストも行い、セキュリティ意識の定着を図ります。　→ 継続

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連携



今後の展望

本事業への参加により、セキュリティに関わる世の中の動きに対してある程度対応できていることが確認できました。今後は中長期計画の中でIT領域の強化を推進していくため、従業員の利便性を向上させながら、認証などのセキュリティ対策を担保していくことを検討していきます。また、セキュリティリテラシーの低い従業員の底上げも含めて、全社でセキュリティ意識の向上に取り組んでいきます。

経営層としての声

自社に不足していたセキュリティ対策を一つずつ補完していきたいと考えています。セキュリティ担当者に限らず従業員全体、そして経営層全体でセキュリティ意識を高めなければ、新たな脅威に対応できないことがわかりましたので、今後とも啓蒙活動を継続していきます。

参加者としての声

本事業のセミナー・ワークショップで学んだ内容はとても濃く、セキュリティ担当者である自分自身の知識を改めて整理することができました。一方で、自社全体を考えると知識面や対策面をはじめ自社に足りない部分も多く見つかったため、これらをどのように対応していくかが今後の課題です。