東京都産業労働局

中小企業サイバーセキュリティ
実践力強化プログラム

事例集

令和7年度版

40社の
対策事例を掲載

東京都産業労働局

令和7年度
中小企業サイバーセキュリティ実践力強化プログラム　事例集

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

発行年月日
令和8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・ソフトウェアの導入支援、情報セキュリティポリシーの策定支援などに取り組んでまいりました。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うえで、人材面やノウハウ面でのリソース不足が大きな課題であると認識し、東京都では令和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支援を実施しております。

近年では、クラウドサービスやテレワークの定着に加え、生成AIをはじめとするデジタル技術の急速な普及により、企業活動の利便性や生産性が飛躍的に向上する一方、情報漏えいや不正アクセス、ランサムウェア被害などのサイバーリスクも一層高度化・巧妙化しています。特に生成AIの業務活用が進む中で、意図しない情報流出やAIを悪用した攻撃への対策、適切なルール整備やガバナンスの確立が新たな課題として顕在化しています。

本事業では、企業のセキュリティ担当者等を対象に、自社の状況や事業特性に応じて必要なセキュリティ対策を選択・検討し、実践につなげることを目的として、サイバーセキュリティを取り巻く社会的背景や企業経営におけるセキュリティ対策の重要性、生成AI利活用における新たなリスクと対応の考え方などを含め、セキュリティ対策の全体像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したワークショップでは、参加企業によるディスカッションやグループワークを通じて、セミナーで得た知識やノウハウをアウトプットし、各社の取組事例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。さらに、セミナー・ワークショップを通じて明らかになっ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、個社の実情に応じた伴走型の支援を実施しました。

本事例集では、令和7年度に本事業へ参加した企業40社における具体的な支援内容や取組事例を紹介しています。業種や従業員規模、事業内容など、企業を取り巻く環境によって直面するセキュリティ課題や有効な対策は多種多様であり、サイバー攻撃の手法や脅威動向も日々変化しています。加えて、生成AIの活用拡大により、これまで想定されていなかった新たなリスクへの対応も求められています。こうした中で、自社に適したセキュリティ対策を検討し、実行し続けることは、企業経営に欠かせない重要な取組であり、その中核を担うサイバーセキュリティ人材の重要性を、本事例集を通じて感じていただければと思います。

社会におけるDXは急速に進展していますが、本来DXと車輪の両輪であるべきセキュリティ対策は、後回しにされがちな側面もあります。本事例集を手に取っていただき、さまざまな企業の取組からヒントを見つけていただくことで、自社における実践的なセキュリティ対策の推進にお役立ていただけましたら幸いです。

最後に、本事例集の作成にあたり、取材および原稿作成に多大なご協力を賜りました企業の皆様に、心より厚く御礼申し上げます。

令和7年度
中小企業サイバーセキュリティ実践力強化プログラム

事例集

目次

企業別事例

卸・小売

製造・建設

サービス・その他

事業概要

中小企業サイバーセキュリティ
実践力強化プログラムについて

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認識し、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、本事業で使用したテキストや事例集などは社会へ公開し、中小企業の皆様が自社でセキュリティ対策を行う際、活用できるツールとして利用していただくことで、中小企業全体のセキュリティ対策向上を目指します。

支援の全体像

専門家派遣

セミナー・ワークショップで得た気づき、課題を確認し、支援内容を検討します。またセキュリティに関する様々な観点からの相談や課題について幅広い角度から支援を実施します。

課題への取組実践

専門家と決めた取組内容やセミナー／ワークショップで得た知見を参考に取組を実施します。

課題の解決

課題の洗い出し

課題の共有

ワークショップ

自社のサイバーセキュリティ課題を特定し、実践的な解決策を検討・導入できる体制のヒントを得ます。セミナーで学んだ内容のアウトプットを通して、自社の課題感を明確にします。

セミナー

「次に何をするべきか」に対するヒントを提供し、持続的なセキュリティ対策につながる下地になるノウハウを提供します。

事業での取組

■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」、「セキュリティ関連の知識強化」、「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
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（情報セキュリティマネジメントシステム）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
自社の現在地を見える化：IT・セキュリティ棚卸し＆“攻め”の戦略づくり	想定インシデント対応検討：事例に基づく脆弱点の抽出と対策方針	CSF2.0（NIST Cybersecurity Framework 2.0）の適用演習：コア／ティア／プロファイルによる目標設定	ISMS（27001:2022）参照による対策基準設計：自社レベルに合わせた基準策定	管理策の採否判断とクラウド利用確認：評価表に基づく適用範囲の明確化

第6回	第7回	第8回	第9回	第10回
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組織として実践するためのスキル・知識と人材育成	サイバーレジリエンス能力の育成	生成AIおよびAIマネジメントシステム 全体総括
ゼロトラスト導入の要否判断と運用妥当性検証：標準ガイドラインの活用	サービス提供を想定したセキュア設計検討：要件定義～運用の留意点整理	人材・スキル要件の可視化：育成・確保に向けた実施計画の検討	継続的な育成設計：教育プログラム調査・業界ガイドライン参照による実行案	対応力の総合演習：インシデント机上演習と継続改善の振り返り整理

■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課題解決に向けて、多様な得意分野を持つ専門家が、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す。

1　企業のサイバーセキュリティの現状分析と基礎構築
- □ 現在のサイバーセキュリティ状況をヒアリング
- □ 新技術によるリスクの議論
- □ 全4回のステップの計画

2　管理策を活用しながら対策の実施
- □ 対策の基盤強化（組織的管理策・人的管理策の適用）
- □ 対策の実践準備（技術的管理策の選定）
- □ 物理的環境を確認（物理的管理策の確認）

■ワークショップ　全10回

セミナーと同日開催で全10回、4～5名のグループ形式で実施しました。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　セミナー／ワークショップ内容の実践
- □ セミナー／ワークショップで学んだ内容を活用しながら取組を深化

4　セキュリティ対策の継続ノウハウを実践
- □ 持続可能な手法の習得
- □ 内部体制構築の手法を習得
- □ 外部専門家との連携

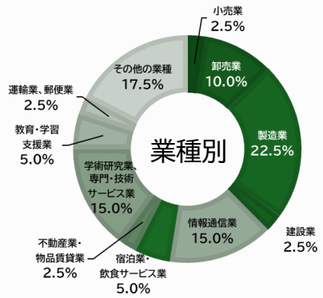
参加企業のセキュリティ体制と支援テーマ

業種	参加企業	従業員数	セキュリティ体制					取組テーマ					
			1名	複数	専任	兼務	経営層	ガバナンス管理	取引先管理	リスクの特定	攻撃等の防御	攻撃時の検知	インシデント対応・復旧
卸・小売	電子機器・電気部品販売業　A社	～5名	●			●	●			●			●
	化学品商社業　B社	～20名		●		●				●	●		
	機械商社業　C社	～50名		●		●		●			●		●
	オフィス関連商社業　D社	～300名		●		●	●					●	●
	寝具製造販売業　E社	301名～	●			●			●		●		
製造・建設	設備装置の設計・製作　A社	～20名	●			●		●	●	●	●		
	印刷・制作業　B社	～50名	●			●		●	●	●	●	●	●
	金属加工業　C社	～100名	●			●		●		●			
	樹脂加工製造業　D社	～300名		●		●				●			
	アパレル製造販売業　E社	～300名		●		●		●		●			
	医療関連製造業　F社	～300名	●		●			●		●			●
	広告・販促支援業　G社	～300名		●	●					●			
	設備工事業　H社	～300名		●	●			●		●			
	プラスチック製造業　I社	301名～		●		●		●		●	●	●	
	化粧品・医薬品製造業　J社	301名～		●	●			●		●	●		
サービス・その他	コンサルティング業　A社	～5名	●			●	●	●		●			●
	医療系コンサル業　B社	～5名	●			●	●	●		●	●	●	●
	社会保険労務士業　C社	～5名	●			●	●	●					
	環境・企画支援業　D社	～5名	●			●	●	●			●		●
	水産資材開発業　E社	～5名		●		●	●	●	●	●	●	●	●
	不動産業　F社	～20名		●		●				●			●
	情報通信業　G社	～20名		●		●			●	●			
	教育サービス業　H社	～20名		●		●	●	●			●		
	調査研究・コンサルティング業　I社	～20名	●			●			●	●			
	社会保険労務士業　J社	～20名		●		●				●	●		
	国際物流業　K社	～20名	●			●				●	●		●
	BPO・翻訳支援業　L社	～20名		●		●	●	●		●	●		
	出版業　M社	～20名	●			●		●		●			●
	情報通信業　N社	～50名		●		●		●			●		
	システム開発業　O社	～50名		●		●	●			●	●		
	情報通信業　P社	～50名		●		●				●			
	人材育成支援業　Q社	～50名	●			●		●	●	●	●	●	●
	監査業 R社	～50名		●		●	●	●		●			●
	調査・環境支援業　S社	～100名	●			●				●			
	システム開発業　T社	～300名		●		●					●	●	●
	採用支援業　U社	～300名	●			●		●			●		●
	人材支援業　V社	～300名	●			●		●		●	●	●	●
	飲食業　W社	301名～	●		●					●	●		●
	国際物流業　X社	301名～		●		●		●		●			
	情報サービス業　Y社	301名～		●		●				●			

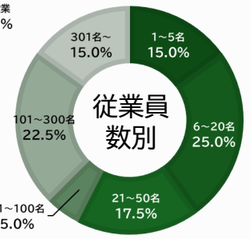
事業に参加した企業のうち、セキュリティ体制は1名体制／複数かはおおよそ半々で、兼務されている割合が8割程度だった。また、本事業に参加した約25%が経営層であった。取組テーマで最も多い領域は「リスクの特定」で約8割となっている。この領域では、主に情報資産の管理やリスクアセスメントに関する課題への取組を実施した。次いで、「ガバナンス管理」が約5割程度であり、この領域では、特に役割・責任・権限やセキュリティポリシー等の整備や見直しに関する課題へ取組んだ。

参加企業・参加者の属性

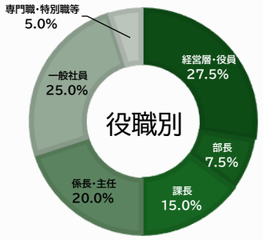
支援対象企業の属性



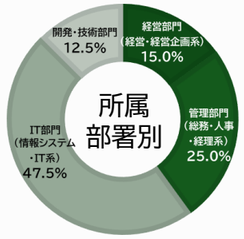
様々な業種や規模の都内中小企業40社にご参加いただきました。



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名にご参加いただきました。



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は、8割の参加者が満足と回答した。また、事業の支援内容に関しては、全体的に有効であると感じた参加者が多かった、特にテキスト等セミナー資料の公開や専門家派遣が有効であると感じた参加者が多かった。

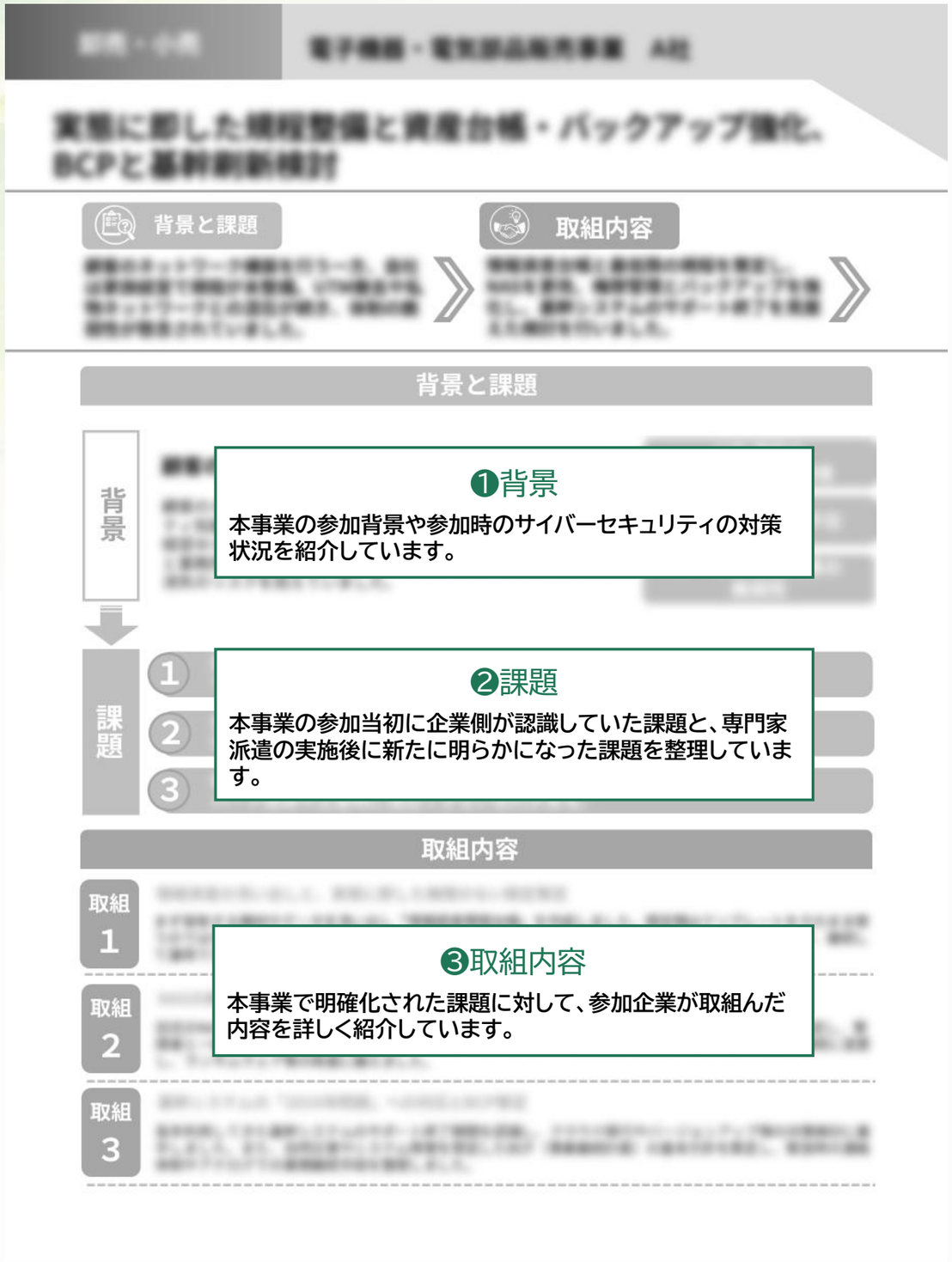
本事業を通じて、事業参加前と比べて貴社の情報セキュリティレベルに変化はありましたか？

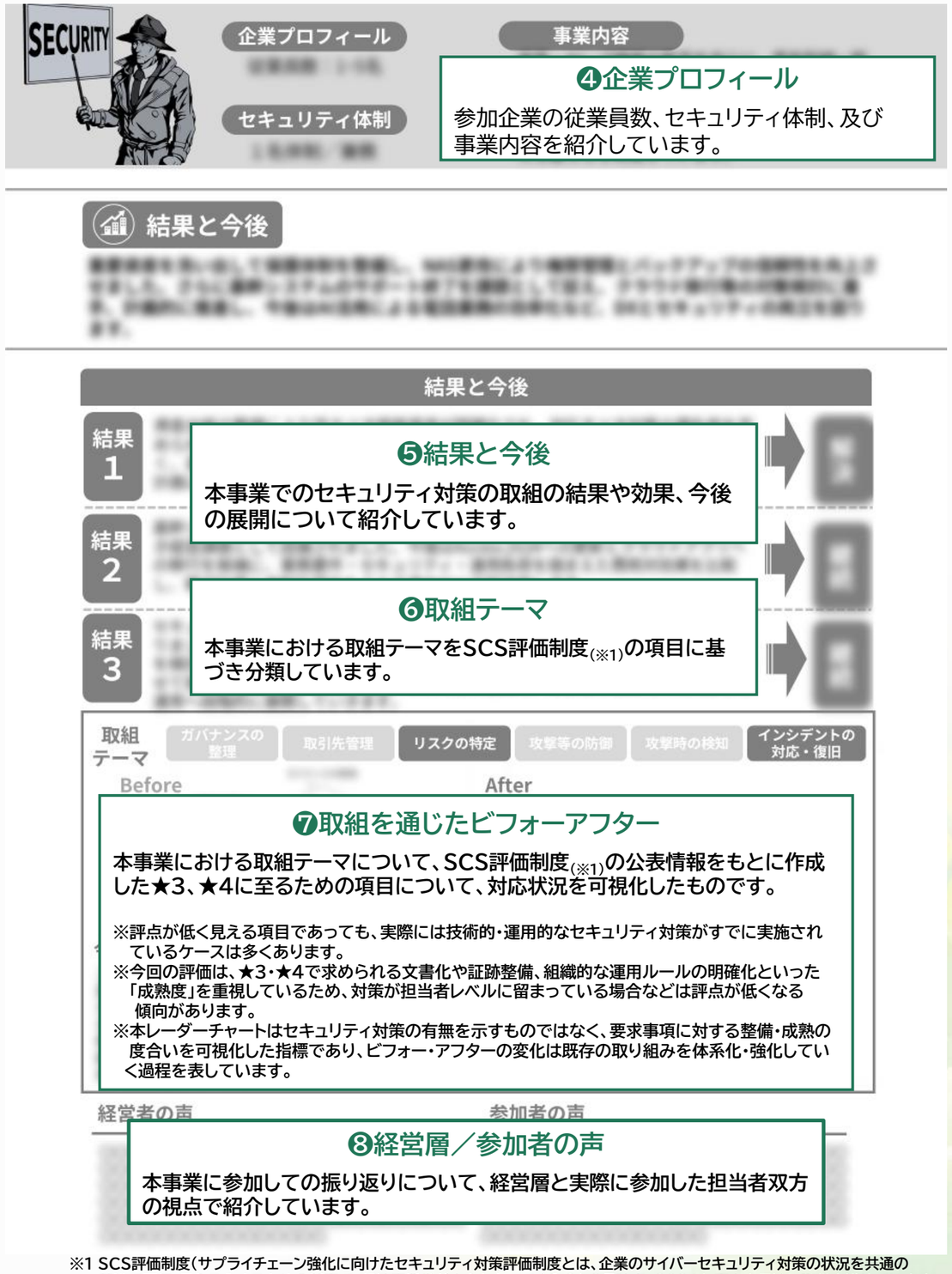
向上したと思う理由

自社に必要な対策の向上をはかれたから	86.5%
セキュリティ体制を強化できたから	59.5%
従業員に対して教育を実施したから	40.5%
規程類が整備できたから	54.1%
その他	2.7%

事業に参加した企業の9割弱が、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を強化できたからと回答した企業が多かった。

事例の見方





※1 SCS評価制度（サプライチェーン強化に向けたセキュリティ対策評価制度とは、企業のサイバーセキュリティ対策の状況を共通の基準で評価・見える化するための制度で、経済産業省が中心となって令和8年3月時点、2026年度末を目途に整備を進めています。

卸・小売

電子機器・電気部品販売事業　A社

実態に即した規程整備と資産台帳・バックアップ強化、BCP(※1)と基幹刷新検討

企業プロフィール
従業員数：1～5名

セキュリティ体制
1名体制／兼務

事業内容
AV機器や家電の販売、修理、電気工事などを手がける地域密着型の企業です。長年の実績を生かし、家庭や地域の暮らしを支えるきめ細かな対応を強みとしています。

背景と課題

顧客のネットワーク構築を行う一方、自社は家族経営で規程が未整備。UTM(※2)撤去や私物ネットワークとの混在が続き、体制の脆弱性が懸念されていました。

取組内容

情報資産台帳と最低限の規程を策定し、NAS(※3)を更改。権限管理とバックアップを強化し、基幹システムのサポート終了を見据えた検討を行いました。

結果と今後

重要資産を洗い出して保護体制を整備し、NAS(※3)更改により権限管理とバックアップの信頼性を向上させました。さらに基幹システムのサポート終了を課題として捉え、クラウド移行等の対策検討に着手。計画的に推進し、今後はAI活用による電話業務の効率化など、DXとセキュリティの両立を図ります。

背景と課題

背景

顧客の信頼を守るため足元の体制の再点検が必要

顧客のネットワーク構築を請け負う立場として、自社のセキュリティ知識と体制の再構築が必要と感じていました。しかし、家族経営ゆえにルールは曖昧で、UTM(※2)も撤去した状態でした。家庭用と業務用のネットワークも混在しており、サイバー攻撃やデータ消失のリスクを抱えていました。

- 公私混同のネットワーク環境
- ルール・台帳の不在
- データの保護対策の脆弱性

課題

1. 業務用・家族用・来客用ネットワークが未分離で、ウイルス感染や不正アクセスのリスク
2. 情報資産が把握できておらず、取扱いのルールもないため、管理が属人化
3. 基幹データのバックアップが不十分で、ハード故障や災害時に復旧できない恐れ

取組内容

取組1　情報資産の洗い出しと、実態に即した無理のない規程策定

まず保有する機材やデータを洗い出し「情報資産管理台帳」を作成しました。規程類はテンプレートをそのまま使うのではなく、家族経営の規模に合わせて必要最小限の内容に取捨選択して策定しました。形骸化を防ぎ、継続して運用できるルール作りを重視しました。

取組2　NAS(※3)の刷新による権限管理の適正化とバックアップ強化

旧式のNAS(※3)をRAID1(※4)対応の新規種へリプレースし、耐障害性を向上させました。併せてアクセス権限を設定し、管理者と一般利用を分離しました。重要データはクラウドとオフライン媒体への多重バックアップを行う運用に変更し、ランサムウェア等の脅威に備えました。

取組3　基幹システムの「2026年問題」への対応とBCP(※1)策定

長年利用してきた基幹システムのサポート終了期限を認識し、クラウド移行やバージョンアップ等の対策検討に着手しました。また、自然災害やシステム障害を想定したBCP(※1)（事業継続計画）の基本方針を策定し、緊急時の連絡体制やアナログでの業務継続手段を整理しました。

※1　Business Continuity Plan（事業継続計画：災害・事故・障害発生時でも重要業務を継続または早期復旧するための計画）
※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　Network Attached Storage（ネットワーク接続型ストレージ：ネットワーク経由で複数端末からデータを共有・保存できる装置）
※4　RAID1（同じデータを複数の記憶装置に同時に保存し、障害時のデータ保護を高める方式）

結果と今後

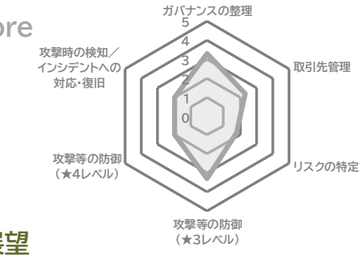
結果1　資産台帳の整備により守るべき情報資産が明確化され、対応すべき対策の優先度を定められる状態となりました。併せて規程も整備しましたが、作成して終わりではなく、運用を通じて継続的に更新することが重要です。今後は定期的な棚卸しと見直しを計画に組み込み、実効性を維持し改善を進めていきます。　→　解決

結果2　基幹システムのサポート終了までの残期間が短いことが明確となり、早急に対応すべき経営課題として認識されました。今後は基幹システムの更新とクラウドアプリへの移行を候補に、業務要件・セキュリティ・運用負荷を踏まえた費用対効果を比較し、移行計画と体制を固めたうえで速やかに方針決定します。　→　継続

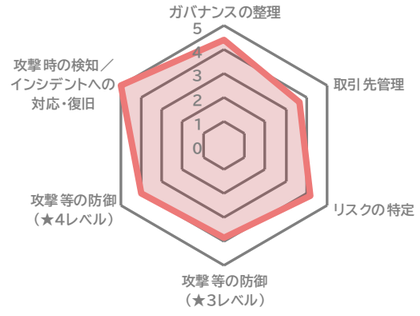
結果3　セキュリティの基盤整備が進んだことで、守りだけでなく攻めのIT活用へ視野が広がりました。今後は電話対応業務を中心に、AIによる録音・テキスト化・要約の仕組みを検討し、顧客管理システムと連携させて情報共有と対応品質の向上を図ります。併せて個人情報の取扱い、権限管理、ログ保全を整備し、安全性と業務効率を両立した運用へ段階的に展開していきます。　→　継続

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ **リスクの特定** ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

これまでは「何となく怖い」という漠然とした不安でしたが、情報資産の可視化により守るべき対象と必要な対策が明確になりました。基幹システム刷新は待ったなしですが、これを好機と捉え、AI活用等の業務効率化と併せて推進します。あわせて規程・教育・点検を継続し、投資判断も含めて改善を回しながら、セキュリティを経営の足腰として次世代へつなぐ体制を築いていきます。取引先の信頼も着実に高めます。

経営者の声

セキュリティは内部環境や外部環境に合わせて適宜柔軟に見直す必要がある。日々の業務に追われ後回しにしてしまうと、業務上の重大な危機に陥る可能性がある。本事業を通じて、自社の状況をしっかりと認識し、時代のトレンドとのギャップを埋められる具体的なアクションに繋げていきたい。

参加者の声

集合研修に参加してみて、他社の方と交流をしていく中で、皆様 多様な課題を抱えていることが具体的に分かった。また過去に起こったインシデントにおいて、どのようなことが起こり、どういった対策を取ったのか。本来はどうすべきだったのかという生の声が聞けて、とても勉強になった。

卸・小売

化学品商社業　B社

子会社事故を契機に、規程整備と二つ星取得で統制・教育を立ち上げ、外部評価にも備える

企業プロフィール

従業員数：6～20名

セキュリティ体制

複数名体制／兼務

事業内容

有機・無機化学品、特殊化学品、化粧品原料などを扱う化学品商社です。国内事業、貿易事業、受託事業を柱に、多様な産業分野へ安定供給と提案を行う体制を築いています。

背景と課題

子会社でのファイル消失・情報改ざん事故を機に危機感が高まった一方、知見者が不在で現状把握ができず、ルール・教育・運用が整っていませんでした。

取組内容

情報資産を棚卸しして優先課題を可視化。IPA(※1)のひな形を活用し規程案を作成しました。社内周知と教育計画を立て、二つ星申請への対応準備を進めました。

結果と今後

台帳整備により管理対象と優先順位が明確化され、規程・ハンドブックの整備および社内周知が進展しました。また、本支援を契機に二つ星の申請を実施しました。今後はロードマップに基づき、会議体およびKPI(※2)を設定し、教育・運用の定着とクラウド上のデータ整理（権限管理・共有ルールの見直し）を推進していきます。

背景と課題

背景

「何から始めるか」を可視化できておらず、規程・教育・運用を少人数で回す初動整備に不安

子会社でのファイル消失・請求情報の書き換え事故を受け、取引先への説明責任も意識するようになりました。しかし社内に知見者が不在で、最新のネットワーク図や端末/ソフト一覧もなく、UTM※3状況も不明でした。USBや個人クラウド利用も統制できていなかったため、資産の棚卸しとルール整備を検討していました。

- 子会社で事故発生（消失/改ざん）
- 知見者不在で外部委託依存が常態化中
- 体制・規程・教育が未整備で運用不安

課題

1. 管理対象・対策状況が不透明で、現場判断に依存し、優先順位・予算・責任分担が未確定
2. セキュリティ規程が未整備で、対外的に必要な統制・証跡を示せず、評価取得が困難
3. 周知・教育が不足し、データ管理や権限運用が部門・個人でバラつき、リスクの顕在化

取組内容

取組1　情報資産管理台帳を整備し、現状・リスク・優先度を短期間で可視化し、優先投資と担当を決める基盤構築

端末・クラウド・重要データを棚卸しし、物理/デジタル両面のリスクを整理しました。ベンダーから最新のネットワーク情報などを収集し、ウイルスソフト運用、USB利用、個人クラウド、推測されやすいパスワード設定などの論点を洗い出し、対応の優先度を合意しました。

取組2　IPA(※1)ひな形で情報セキュリティ規程・手順を整備し、証跡を揃えて二つ星申請に確実に接続

IPA※1の規程のひな形を用い、情報セキュリティ関連規程の必要事項を自社向けに編集し作成しました。情報セキュリティ関連規程の完成後には社内周知、情報セキュリティハンドブックを展開、専門家による最終確認を計画しており、二つ星申請までを実施しました。

取組3　周知・教育を定例化し、クラウド運用（整理／権限／共有）を全社ロードマップで定着

全社会議での周知資料を作成し、年2回の継続周知を実施しました。また、クラウドの整理・アクセス権設定ができない原因を共有し、分類ルール作成と棚卸しを実施しました。また、標的型メール訓練、会議体・KPI※2案の設計を含むロードマップ案作成を行いました。

※1　独立行政法人情報処理推進機構
※2　Key Performance Indicator（重要業績評価指標：組織や業務の目標達成度を定量的に測定するための指標）
※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　Mobile Device Management（モバイルデバイス管理：端末を一元的に管理し、設定・アプリ・セキュリティを遠隔で制御する仕組み）

結果と今後

結果1

情報資産台帳の整備により、未把握だった管理対象と優先課題が可視化されました。外部委託任せで社内に図面・一覧がない状態から、端末/クラウド/重要データの所在とリスクを整理しました。USB利用、個人クラウド、推測されやすいパスワード運用など論点を特定し、優先度の高い対策から着手できる状態にしました。今後は更新手順も定めます。

→ 解決

結果2

情報セキュリティ関連規程は最終的な整備と周知まで完了し、二つ星取得の申請も実施しました。これにより対外的にも規程の整備を案内できるレベルに到達しました。今後、直近では情報セキュリティハンドブックの社員展開を予定しています。関連規程やハンドブックの改訂・更新手順も整え、年次点検と経営層への報告も実施し、継続運用を行っていきます。

→ 継続

結果3

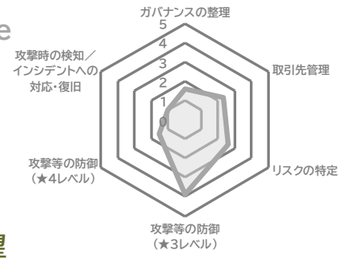
全社会議でのセキュリティ教育を実施したことで、社長含め社員の中でもセキュリティに対する意識が徐々に高まってきました。今後は標的型メール訓練などの施策を活用することで更なる周知徹底を図っていきます。また、クラウドの整理・アクセス権管理、パスワード方針など日常ルールを定着させていき、継続的に点検し改善サイクルを回していきます。

→ 継続

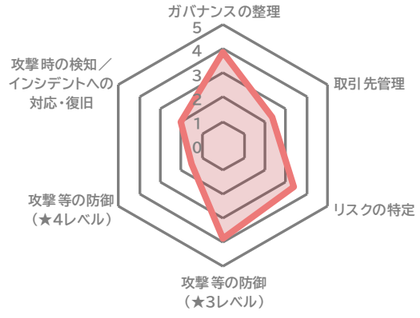
取組テーマ

ガバナンスの整理 ／ 取引先管理 ／ **リスクの特定** ／ **攻撃等の防御** ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

規程・教育を「作って終わり」にせず、会議体とKPI※2で継続運用します。クラウドの整理とアクセス権管理を進め、データ保護とバックアップを実効化。サプライチェーン評価への回答品質も高めます。あわせてUTM※3/MDM※4等の技術対策、ID管理・パスワード方針、インシデント対応手順と訓練、外部委託先との責任分界、経営層への定期報告を段階的に整備し、インシデントの再発防止を図ります。

経営者の声

数年前、子会社がサイバー攻撃を受け情報資産を失いました。情報セキュリティ対策は必要との認識はあったものの、何から始めるべきか明確に見えない中、当研修を通じて道筋を描き、情報資産台帳や規程を整備しました。社内研修の定期開催も仕組み化し、着実な一歩を踏み出しました。

参加者の声

情報資産台帳や情報セキュリティ関連規程が整備されていなかったり、また社員のセキュリティに対する意識が不足していました。自らもやはりそれらの意識が不足していた中、当研修にて様々な知見を習得し、社内に還元することで、会社のセキュリティレベルの向上に貢献できました。

卸・小売

機械商社業　C社

クラウド化促進および規程集の追加整備で、BCP(※1)を含めた情報資産保護・セキュリティ強化の実践

企業プロフィール

従業員数：21～50名

セキュリティ体制

複数名体制／兼務

事業内容

水圧機器・油圧機器などの制御装置を扱う機械専門商社です。海外メーカー製品も含めた幅広い商材を取り扱い、産業分野の設備調達や技術提案を通じてものづくりを支えています。

背景と課題

セキュリティ推進部署にて組織的に運営していますが、特定ITベンダー依存リスクやクラウドリフトに向けたセキュリティ体制強化の実施を考えていました。

取組内容

専門家からアドバイスを受け、情報セキュリティ規程の見直しや、ファイルサーバーのクラウドリフト、BCP(※1)観点でのリスク評価・対策の策定などに取り組みました。

結果と今後

情報資産可視化や、データ移行・保護に関する個別ワークショップにより、情報セキュリティ規程の改善とクラウドリフトに向けた基盤が整ってきました。また、BCP(※1)視点の強化によりレジリエンスの重要性を実感しています。本事業で構築したセキュリティ運用基盤を活用し、引き続き課題解決に向け進めていきます。

背景と課題

背景

組織的な力量向上と、クラウド活用およびBCP(※1)を考慮したセキュリティ対策強化を検討

セキュリティ推進部署を組織的に運営してきてはいましたが、外部ベンダーや外部コンサルを活用し運用してきました。そういった中で、BCP※1を考慮し、オンプレミス環境のクラウド化計画も視野にありました。そのため、今後のクラウド化等にむけて、システムや情報セキュリティ対策を第三者の評価をもとに把握し、さらに強化したいと考えました。

- オンプレミス環境のクラウド化
- 災害時におけるシステム復元基盤の構築
- クラウドサービス選定基準の確立

課題

1. ファイルサーバーのBCP(※1)環境が整っておらず、移行計画含め未検討
2. システムのバックアップは取っているが、災害時に復旧できるか等把握不足
3. 今後クラウドサービスを活用するにあたり、基準・規程が未整備

取組内容

取組1　情報資産・重要度等について個別ワークショップを受講し、クラウドリフトに向けた管理ルールを策定

本事業の専門家から、情報資産および、重要度・保護対象基準に対するワークショップを実施頂きました。ワークショップで得た知識とアドバイスを元に、ファイルサーバーのクラウドリフトに向けセキュリティの視点を強化した移行、システム運用計画の策定を実施しています。

取組2　バックアップ環境の可視化および、BCP(※1)を考慮した情報セキュリティ規程の策定を実施

現行システムを構築しているITベンダーに対し、BCP※1の観点で確認しなければいけない事項をまとめ確認を行いました。また、一部復元先が未確定のシステムについては、追加でクラウドサーバーを契約し、復元テストをITベンダーに実施いただくことで対策が強化できました。

取組3　情報セキュリティ規程に対しクラウドに関する基準を追加、自社の運用に適したルールへの見直しを実施

自社のレベルに合わせたクラウドサービスの選定・運用に関わる基準を考慮した規程の作成を行いました。今後、クラウドサービスを活用するにあたり、自社に必要なセキュリティレベルを確保しつつ、クラウドサービスの活用を進めていきます。

※1　Business Continuity Plan（事業継続計画：災害・事故・障害発生時でも重要業務を継続または早期復旧するための計画）

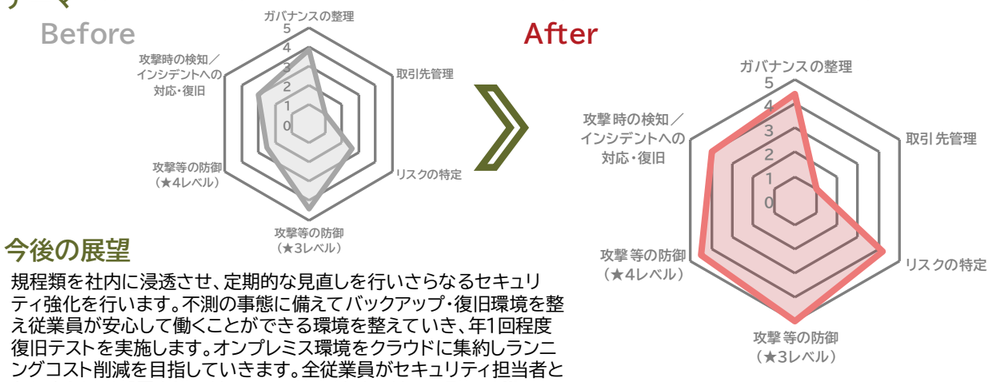
結果と今後

結果1　ファイルサーバークラウド化に向けたセキュリティ・運用ルール含めた基盤の強化を更に進めます。中期計画として、本格的にオンプレミス環境のクラウド化を実施する予定です。　→　継続

結果2　システム障害時の復旧時間、復元レベルを設定するとともに、復元に必要なクラウドサーバーの契約が完了しました。今後、年1回程度の復元検証等を含め、BCP※1を強化したリスクコントロールに向けた取り組みを継続していきます。またクラウドバックアップを導入しリストア確認済、復旧用基幹システム導入し、接続テストも行います。　→　解決

結果3　クラウドサービスの契約について申告・承認するルールはありましたが、今回制定したクラウドセキュリティ規程により、自社の組織に必要なセキュリティレベルを確保することができ、安心した運用が実現しました。今後、セキュリティ教育内でも定期的展開することにより、全社のセキュリティ意識向上に取り組んでいきます。　→　解決

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧



今後の展望

規程類を社内に浸透させ、定期的な見直しを行いさらなるセキュリティ強化を行います。不測の事態に備えてバックアップ・復旧環境を整え従業員が安心して働くことができる環境を整えていき、年1回程度復旧テストを実施します。オンプレミス環境をクラウドに集約しランニングコスト削減を目指していきます。全従業員がセキュリティ担当者となるように当部署主導でリテラシー教育（セキュリティ研修・攻撃メール訓練など）を実施していきます。

経営者の声

中小企業のセキュリティ対策について、専門家のアドバイスを受けながら基礎から学ばせる事が出来、現在の課題や今後の方向性が明確になりました。学んだ事を活かしてセキュリティ強化に取り組むとともに、本件に対する社員全員の意識レベルの向上に努めて参ります。

参加者の声

全10回のセミナーを受講することでセキュリティ知識を得ることができ、弊社でセキュリティ対策をしていた内容に問題がなかったことが自信につながりました。専門家の方に課題を洗い出していただいたことで今後やるべきことがクリアになりました。

卸・小売　オフィス関連商社業　D社

巧妙化する攻撃への対応力強化・ログ分析基盤の構築による侵入検知と被害最小化の検討

企業プロフィール
従業員数：101～300名

セキュリティ体制
複数名体制／兼務

事業内容
文具販売を軸に、オフィスレイアウトやデザイン、働く環境づくりまで支援する企業です。商材供給にとどまらず、オフィスの価値向上や業務効率化を総合的にサポートしています。

背景と課題

ISMS(※1)運用に加え、高度化するサイバー攻撃へ即応するため、社内体制の整備から一歩踏み込み、侵入検知や防御等の技術的対策について模索していました。

取組内容

機器リストに基づき、攻撃傾向に即した重要ログを選定し、ログの集約・可視化から分析運用までの計画を立案し、技術面からインシデント対応力の強化に取り組みました。

結果と今後

重要ログの可視化と初動対応の判断基準が明確化され、組織的な検知・防御体制強化のため土台が整いました。今後は、策定した運用手順の実践を通じて社内への定着を図るとともに、脅威動向に応じた継続的な改善により、更なる即応力の向上を目指します。

背景と課題

背景

巧妙化する攻撃への対応力強化が急務であり、ログ監視等の技術的対策の導入が必要

ISMS認証※2により管理体制は整っていました。一方で、現状のルール主体の運用では、巧妙な攻撃の兆候を捉える技術的手段にまで手が回らず、万が一の侵入を早期に検知しきれないことにリスクを感じていました。そのため、ログ監視等の技術対策を導入し、侵入を前提とした早期発見・即応体制を構築する必要性がありました。

- 実効的な技術的対策の確立が必要
- 攻撃の兆候を捉える早期検知能力の確保
- 事後対応の迅速化による被害拡大の防止

課題

1. 侵入や攻撃を検知するために取得しているログ情報に対して、十分に整理・分析する技術力強化が必要
2. 事象が発覚した場合、事前に収集していたログから原因を特定し対処・運用する技術力強化が必要
3. 最新の脅威情報を取得し、自社資産の脆弱性を即座に解消するための情報収集力の強化が必要

取組内容

取組1　不正アクセス検知を目的にUTM(※3)ログ分析・チェック体制やインシデント処理手順の作成

不正アクセスやマルウェア感染検知に目的を絞り、UTM※3ログを軸とした分析運用の仕組みづくりに着手しました。サイバーキルチェーンに基づき、UTM※3で検知可能なログ確認、外部への不正通信のチェック項目を検討しました。誰が、いつ、何をトリガーにチェックし、インシデント判断したかの処置手順を作成、運用フローを検討しました。

取組2　IPA(※4)等の情報収集体制を確立し、脆弱性情報に基づいた社内通知と対応指示を実施

ニュース報道やネット検索による脆弱性情報の取得方法に加え、IPA※4やJPCERT※5のメールマガジンの登録や公開情報の確認方法をハンズオン形式で実施しました。最新のセキュリティ情報をタイムリーに入手し、それに基づいた脆弱性情報や対応方法を社内に通知・対応指示する流れを構築しました。

取組3　環境整備とログ解析方法の共有などで調査能力の強化を促進

ドメインコントローラーのイベントログを活用した認証エラーの確認を検討項目に含め、運用ツールによるログオン解析方法を共有しました。新たなツールをサーバーにインストールしないことで、サーバーに影響を与えずに異常をチェックする調査能力の強化を図りました。

※1 情報セキュリティマネジメントシステム：組織の情報資産を守るために、リスク評価・管理策・運用・改善を体系的に管理する仕組み
※2 ISO/IEC 27001 に基づき、組織の情報セキュリティマネジメントシステムが適切に構築・運用されていると第三者が認証する制度
※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 独立行政法人情報処理推進機構
※5 JPCERT/CC（一般社団法人 JPCERTコーディネーションセンター）
※6 Business Continuity Plan（事業継続計画：災害・事故・障害発生時でも重要業務を継続または早期復旧するための計画）

結果と今後

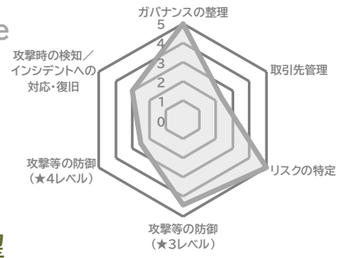
結果1
機器リストに基づき重要ログを特定し、分析の優先順位を整理したことで、どこから手を付けたらよいかを明確化することができました。今後は、優先順位をもとに分析手法の確立、運用手順を作成し、実務レベルでの解析スキルを定着させ、高度な攻撃に対しても迅速かつ正確に検知・分析できる体制の確立を目指します。
→ 継続

結果2
収集していたログ解析に関する技術的要件を整理しました。また、事象発覚時の初動から封じ込めまでの計画概要を作成しました。今後は、具体的な解析手法の確立や、対応手段の策定を行い、机上テストなどを通して、被害を最小限に抑えるための確実な対処能力の定着と向上を図ります。
→ 継続

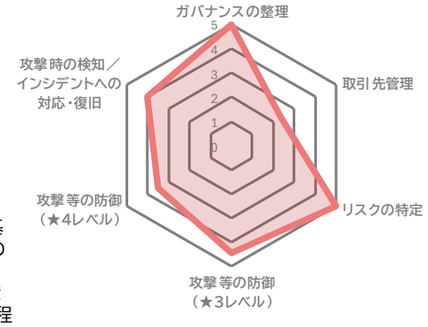
結果3
最新の脅威情報の取得ルートを整理し、自社資産への影響度を即座に判断するためのフローを定着することができました。
→ 解決

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ 攻撃等の防御 ／ **攻撃時の検知** ／ インシデントの対応・復旧

Before



After



今後の展望

今回作成したログ取得機器リストと優先度に基づき、ログ収集・解析基盤の構築を推進し、実効性の高い運用体制を確立します。特に、攻撃の早期検知から封じ込めまでの初動フローを標準化し、担当者が迅速に対処できる体制を目指します。あわせて、事業停止を防ぐBCP※6を策定し、代替手段の確保と復旧手順の確立を図ることで、有事の際も規程した日数以内に業務を再開できる強固なレジリエンスを実現します。

経営者の声

既にISMS認証※2を取得し規程やルールに基づくセキュリティ運用を継続しているが、多様化・巧妙化するサイバー攻撃に対しシステム担当者から検知や初動対応などの技術的対策力の強化という課題が挙げられていた。大規模な投資が難しい中、現場レベルで実践可能なセキュリティ技術の底上げを期待している。

参加者の声

講座を通してISMS※1以外の多様なフレームワークや手法を体系的に学び、ワークショップや座談会で他社のセキュリティ担当者の悩みや先進事例を共有でき、とても大きな刺激と学びになった。専門家派遣でサイバー攻撃対応としてのログ活用手法も整理でき、今後はレジリエンス向上を着実に目指す。

卸・小売　寝具製造販売業　E社

システム統合で複雑化した環境を刷新し、可視化と教育でセキュリティを強化

企業プロフィール
従業員数：301名以上

セキュリティ体制
1名体制／兼務

事業内容
寝具・寝装品を中心に、タオルやインテリア用品、健康関連機器まで幅広く扱う老舗企業です。長い歴史で培った品質と技術を生かし、快適な睡眠と暮らしの向上に貢献しています。

背景と課題

企業合併に伴いシステム環境が複雑化し、グループ全体でのセキュリティ統制と、潜在的な脆弱性の可視化が急務となっていました。

取組内容

支援事業で得た知見を元に、OS・サーバーの刷新とクラウド化、ログ監視の強化、および全社的な実践的訓練を実施しました。

結果と今後

全端末のセキュリティレベル統一と環境の最新化を実現しました。ログ監視による不正通信の可視化については、より高精度な検知に向けた対応を進めています。また訓練により不審メール開封率が低下するなど従業員の意識も向上しました。今後はグループ企業へのガバナンス強化を推進します。

背景と課題

背景

統合に伴う環境の複雑化と管理の課題

過去の企業統合により複数のドメインやサーバーが並立しており、一元管理が困難な状況でした。また、OSサポート終了への対応や、巧妙化するサイバー攻撃に対し、従来の対策だけでは検知・防御が難しくなりつつありました。

- グループ全体の統制不足
- 老朽化システムの残存
- サイバー攻撃の巧妙化

課題

1. 店舗等を含めた全端末へのセキュリティ対策の徹底
2. サーバーおよびPCのOS刷新とクラウド移行
3. 侵入を前提とした検知能力と社員教育の強化が必要

取組内容

取組1　ITインフラの刷新と防御機構の強化

OSサポート終了を見据え、PCおよびサーバーを最新OSへ刷新しました。同時にサーバーをクラウド環境へ移行し、閉域網を構築して安全性を確保しました。また、全端末へのディスク暗号化導入により盗難・紛失時の情報漏洩リスクを低減させました。

取組2　「可視化」による早期検知体制の確立

IT資産管理ツールの設定を見直し、許可されていないアプリの通信を可視化する取り組みを開始しました。また、サーバーでの特権ID監視やログ一元管理の強化にも着手し、不正の予兆を早期に発見できる体制づくりに努めています。

取組3　組織的な対応力向上とグループ展開

従業員に対し標的型攻撃メール訓練を複数回実施し、初動対応を定着させました。また、IPA※1のガイドラインに準拠したセキュリティチェックリストを作成し、グループ企業に対しても現状把握と対策の是正を働きかけ、組織全体の底上げを継続しています。

※1　独立行政法人情報処理推進機構
※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：インターネット上に暗号化された仮想専用線を作り、安全に社内へ接続する仕組み）
※4　Business Continuity Plan（事業継続計画：災害・事故・障害発生時でも重要業務を継続または早期復旧するための計画）

結果と今後

結果1　店舗等のPCやMacについても、OSの更新やセキュリティ対策ソフトの適用を徹底し、全社的なセキュリティレベルの統一を図りました。併せてネットワーク機器の刷新により通信状況が可視化され、トラブル時の迅速な切り分けと封じ込めが可能な環境を実現しました。　→　解決

結果2　複数回のメール訓練実施により、不審メールのリンククリック率が低下傾向を示すなど、従業員の「見抜く力」が向上しました。また、専用回線とUTM※2を用いたセキュリティルームの構築を進めており、機密性の高い業務を安全に遂行できる環境の実現を目指しています。　→　継続

結果3　IPA※1ガイドラインに則ったチェックリストを作成し、グループ企業のセキュリティ実態を定量的に把握しました。今後は、VPN※3環境の刷新によるデバイス認証の強化などを進め、場所を問わず安全に業務ができるゼロトラスト環境への移行を加速させていく予定です。　→　継続

取組テーマ　ガバナンスの整理 ／ **取引先管理** ／ リスクの特定 ／ **攻撃等の防御** ／ 攻撃時の検知 ／ インシデントの対応・復旧

今後の展望

今後はVPN※3環境の刷新によるデバイス認証の強化や、クラウド環境におけるデータ保護体制の強化を進めていきます。また、今回実施したグループ企業へのチェックリスト運用を定着させ、定期的な棚卸しと改善のサイクル（PDCA）を回すことで、グループ全体で高水準かつ均質なセキュリティガバナンスの維持を目指します。

経営者の声

中小企業を狙うサイバー攻撃が巧妙化する中、本プログラムへの参加は自社のリスク管理を見直す貴重な好機となりました。ツール導入に満足せず、有事の復旧（BCP※4）を見据えた体制強化と全従業員の意識底上げを並行して進める必要性を強く感じています。信頼される企業であり続けるよう対策を継続して参ります。

参加者の声

セミナーやワークショップを通じ、他社の事例や専門家の知見を直接吸収できたことは大きな収穫でした。自社のセキュリティ対策を見直す良い機会となり、具体的対策を進めることができました。この学びを活かし、今後も組織全体の防御力を高めていきます。

建設・製造

設備装置の設計・製作　A社

セキュリティ意識の世代間格差の低減、社内啓蒙に向けた継続的なセキュリティ確保の仕組み作り

企業プロフィール
従業員数：6～20名

セキュリティ体制
1名体制／兼務

事業内容
ものづくり分野において、生産設備・専用装置の設計製作を主たる事業とする企業です。現場での加工・組立技術を基盤としつつ、顧客要求に基づく装置構想、設計、製作、立上げまでを自社で一貫して対応できる体制を構築しています。

背景と課題

1点物の製品を開発することの多い事業で、熟練工も多く技術者の年齢層も幅が広いため、ITリテラシーやセキュリティに対する意識格差を埋めたいと思っていました。

取組内容

情報資産の洗い出しと、資産ごとのリスク対策を元にセキュリティを継続的に守る仕組みを学び、経営陣の理解拡大や従業員の啓蒙活動へ繋げる取り組みを行いました。

結果と今後

本活動を通じた知見や資料を元に会社の情報資産やそれらが持つリスクを経営陣に説明し、セキュリティ対策への理解を強化することができました。また、従業員への教育によりセキュリティへの意識の向上が見られ、IT関連で不安なことを相談してもらえる状況が増えました。

背景と課題

背景

取引先に信頼してもらえるセキュリティ環境作りを、経営陣を巻き込んで強化したい。

事業特性上、大手企業向けに一点物の製品などを製造することが多く、大手企業のセキュリティ要求に対応したセキュリティ環境を、経営陣の理解を得ながら構築する必要がありました。

- セキュリティ対策への不安
- 世代間で異なる社員のセキュリティ意識
- 明文化されていないセキュリティリスクと対策

課題

1. IT担当が独学でセキュリティ対策を行ってきたが、全体像も基準も分からない状態
2. 事業特性上、職人的な社員が多く年齢層も幅広いため、各個人のセキュリティ意識にばらつき
3. 情報セキュリティ確保のための施策に対して、経営陣の理解を得ることに苦心

取組内容

取組1　体系化されたセキュリティ確保の仕組みを学び、実践し、助言を受けることで基準の習得

本事業のセミナー・ワークショップにて、セキュリティフレームワークの全体像や中身の解説・実践があるとのことでしたので、学んだ内容を元に自社で実践し、その結果を派遣専門家にチェックしてもらうことで、体系化された知見を手に入れようとしました。

取組2　専門家の助言や当該プログラムに参加する他社事例を学ぶことでセキュリティ教育の改善の検討

専門家の助言や、本事業を通じて共有された他社IT担当者の事例を基に、セキュリティ教育の見直しを行いました。社内に専用チャネルを設置し、クイズ形式の社内向けセキュリティ診断の実施による啓蒙を進めることで、社員の理解度向上と意識の平準化につなげました。

取組3　当該プログラムを通じて見える化した情報資産やそれに対するリスクを示し経営陣の理解深化を図る

専門家の持つ事例から、本事業で実践する情報資産管理台帳や情報資産ごとのリスク対応計画など、具体的なリスクを元に説明をすると効果的と考え、情報資産管理台帳とリスク対応計画を作成した後に経営陣と情報を共有する機会を設けることにしました。

※1　ISO 9001（品質マネジメントシステム：製品・サービスの品質を安定させ、顧客満足を高めるための国際規格）
※2　SCS評価制度（サプライチェーン強化に向けたセキュリティ対策評価制度）

結果と今後

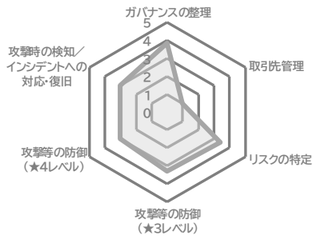
結果1　セミナー・ワークショップを通じて基礎知識を学び、実践した上で専門家に個別のアドバイスを頂けたことで、セキュリティフレームワークの概要の把握と、実務としての管理の勘所の両方が、完璧とまでは言えないものの理解できました。今後も定期的な管理を行おうと思います。　→ 解決

結果2　専門家や本事業参加の他社担当者の知見を通じて、社内向け情報セキュリティ教育の実施方法や効果確認の進め方を具体化できました。社内の専用チャネルでクイズ形式の診断を行うことで、社員の理解度を把握しやすくなり、意識の平準化にもつながりました。また、成果として、教育を一過性で終わらせず、定期的に実施・見直しする運用の流れも共有できました。今後も社内状況に応じた改善を継続していきます。　→ 継続

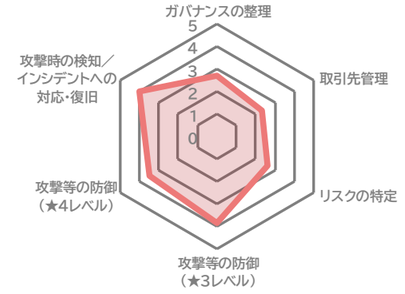
結果3　情報資産管理台帳や個別のリスク対応計画を経営陣に示す機会を頂いたことで、会社全体の情報資産やリスクの大きい情報資産について経営陣と認識を共有することができました。また、個別のリスク対応計画について定期的に経営陣と会話をするきっかけを得たことで、次年度に打つべきセキュリティ対策の共通認識が持ちやすくなりました。今後も経営陣とのコミュニケーションに役立てたいと思います。　→ 継続

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

当社は大手製造業にて使われる一点物の製品を開発する事の多い事業特性があり、技術に関する情報など、流出した際の損害が大きいと思われる情報資産を多く扱っていることから、継続して穴の無いセキュリティ環境構築を進めて行きたいと考えています。また、今回習得した再帰的なプロセスを例えばISO9001（品質マネジメントシステム）※1などの取得に向けた活動にも役立てていきたいと考えています。

経営者の声

本事業を通じ、サイバーセキュリティを経営課題として整理できた。自社の現状と優先順位が明確になり、今後は人材育成と継続的な対策を通じて、取引先から信頼される体制構築を進めたい。

参加者の声

実務と結び付けて体系的に学べたことに加え、ワークショップを通じて自社課題を自分事として捉えられた点が非常に有益だった。本事業を土台に学習を継続することが、資格取得につながるとともに、SCS評価制度※2への準備としても有効だった。

建設・製造　印刷・制作業　B社

ISMS認証(※1)取得で、取引先への信頼獲得とBCP(※2)含めた組織的セキュリティ強化を実践

企業プロフィール
従業員数：21～50名

セキュリティ体制
1名体制／兼務

事業内容
デザイン制作、DTP、デジタルコンテンツ制作、アッセンブリ、総合印刷を手がける制作会社です。印刷とデジタルを組み合わせ、企画から制作・納品まで一貫して対応しています。

背景と課題

重要取引先の要請をきっかけに、ISMS認証(※1)取得を決めました。あわせてセキュリティ知識や対策に対して、自社で自走できる力量をつけていきたいと考えていました。

取組内容

専門家からアドバイスを受け、第三者的なISMS認証(※1)に向けた規程整備の知識定着・境界防御・BCP(※2)観点でのリスク評価・対策の策定などに取り組みました。

結果と今後

ISMS認証(※1)取得にむけ、現時点では第二回審査が残っていますが、問題なく認証取得の目処が見えてきました。また、BCP(※2)視点の強化により、バックアップだけでなく、レジリエンスを含めた重要性を実感しています。次年度以降もISMS(※3)の運用とあわせて、BCP(※2)管理策の拡充にむけて引き続き課題解決を進めていきます。

背景と課題

背景

ISMS認証(※1)の取得と境界防御およびBCP(※2)を考慮したセキュリティ対策について強化を志向

昨今のサイバーセキュリティ事故等の影響もあり、特に海外の大手取引先よりセキュリティ対策について厳しくチェックが入るようになってきました。そういった中で、社内でもセキュリティ対策は進めていたものの、より信頼性を高めるためISMS認証※1取得とともに、端末セキュリティやBCP※2をより意識した対策を強化したいと考えました。

- ISMS認証(※1)の取得
- 端末セキュリティの強化
- 災害時におけるレジリエンス力強化

課題

1. 取引先から求められるセキュリティ対策評価について回答が未実施
2. 重要情報資産へのアクセスにおいて、セキュリティリスク対応が不徹底
3. 重要データのバックアップは実施しているが、ランサムウェア対策によるバックアップデータ保護が未実施

取組内容

取組1　第三者評価による、知識定着化とガイドライン・管理策策定の力量アップを踏まえたISMS認証(※1)の取得

本事業の専門家から、ISMS認証※1コンサルティング企業からの依頼に対し、特にBCP※2の観点で管理策の考え方、リスク評価ポイントのアドバイスを頂きました。そこで得た知識と力量を元に、具体的なガイドラインへの落とし込みを実施し、ISMS認証※1審査へ望んでおります。

取組2　情報資産洗い出しとリスク評価の実施および、ゼロトラスト(※4)を意識したアクセス管理の実現

まず、ISMS認証※1取得プロセスの一つである、情報資産の洗い出しとリスクアセスメント手順について、アドバイスを元に整備を進めました。あわせて、アイデンティティ管理の強化を進めるために、ソリューションにおけるライセンスの見直しと機能アップを図りました。

取組3　ランサムウェア対策を考慮したバックアップ環境の整備と、BCP(※2)ガイドラインの策定

各端末の重要データ等について、クラウドへのバックアップの他、さらにイミュータブルな環境への2次バックアップも視野に含める事により、ランサムウェアによるバックアップデータ損失のリスク低減を図る計画を立てています。

※1 ISO/IEC 27001 に基づき、組織の情報セキュリティマネジメントシステムが適切に構築・運用されていると第三者が認証する制度
※2 Business Continuity Plan（事業継続計画：災害・事故・障害発生時でも重要業務を継続または早期復旧するための計画）
※3 情報セキュリティマネジメントシステム（組織の情報資産を守るために、リスク評価・管理策・運用・改善を体系的に管理する仕組み）
※4 ゼロトラスト（Zero Trust：すべてのアクセスを「信用しない」ことを前提に、常に検証し続けるセキュリティモデル）
※5 PoC（Proof of Concept：概念実証。新しい技術・仕組み・サービスが“実現可能かどうか”を小規模に検証する取り組み）
※6 JIPDEC（一般財団法人 日本情報経済社会推進協会）が運営する ISMS 認証の公式制度体系

結果と今後

結果1　解決

無事にISMS認証※1取得ができる目処が立っています。次年度以降についても、ISMS※3で定めたセキュリティ運用の定着とさらなる強化とともに、組織全体の力量アップを継続して目指します。

結果2　継続

ソリューションプロダクトのレベルを1ランクアップして契約しました。これにより、ID 管理とデバイス管理を統合したアクセス制御基盤を活用したセキュリティ・アクセス強化ができる基盤が整いました。次年度以降、まずはPoC※5にて実施検証し、全社展開を目指します。

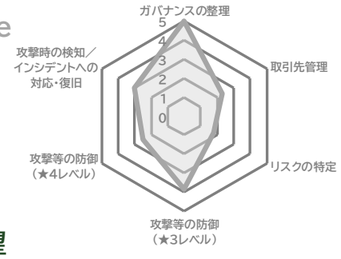
結果3　継続

ISMS※3の管理策とあわせて、BCP※2・バックアップについてガイドラインの策定を行いました。今後、具体的なソリューション導入に向け、製品選定・構築を計画していますが、ISMS※3で定めた管理策があるため、実現すべきセキュリティ強化ポイントが明確であり、進め方のイメージができています。

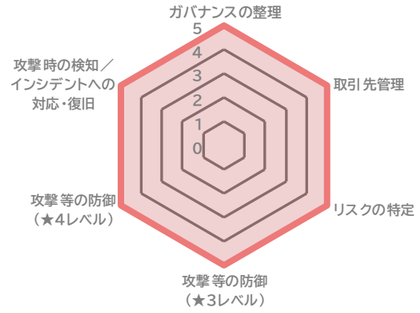
取組テーマ

ガバナンスの整理 / 取引先管理 / リスクの特定 / 攻撃等の防御 / 攻撃時の検知 / インシデントの対応・復旧

Before



After



今後の展望

今回の事業で、ISMS認証※1取得と共に組織としてサイバーセキュリティ対策力・知識と共に、従業員のセキュリティ意識の高まりも効果として実感ができています。継続してISMS※3の運用を回していきます。また、クラウドサービスの有効活用が今後の企業成長により重要となっていく市場環境ですので、クラウドセキュリティに対する強化にむけて、ISMS 認証スキーム（ISMS-CLS）※6等必要に応じて検討していきたいと考えています。

経営者の声

ISMS認証※1を取得する事で会社全体が会社を取巻くリスクについて関心を持ち、考えるようになった。物事に対する考え方が変わり、仕事以外にも目を向けるようになり良い方向に進めている。セミナーを通して色々な事業の参加者様との交流を頂き更に刺激を受け、新しい事への挑戦をし続けたいと思っている。

参加者の声

特定の商品に紐づいたセミナーや、ネットオフラインの集まりとは違い東京都主催しかも全10回というボリュームだからこそ、安心して幅広い多くの事を学べ、セミナー仲間の皆さんと仲良くなれました。貴重な機会を頂き、大変感謝しております。得られたものがとても多く参加して本当に良かったです。

建設・製造　金属加工業　C社

属人的な情シス体制の課題を克服し、業界ガイドライン対応を推進

企業プロフィール
従業員数：51～100名

セキュリティ体制
1名体制／兼務

事業内容
プレス、レーザー加工、溶接、治工具金型製作などを行う製造企業です。部品加工から組立まで対応し、産業用途に応じた精度と安定供給で顧客の製品づくりを支えています。

背景と課題

情報システム業務を単独で担当する体制により管理が属人化し、規程や資産台帳も未整備なため、取引先が求めるセキュリティ基準を満たせていませんでした。

取組内容

ネットワーク図と資産台帳による現状可視化、身の丈に合った規程策定、ITリスク対応BCP(※1)への拡張に取り組みました。

結果と今後

ネットワーク図や資産台帳の整備により、守るべき情報資産と対策の優先度が明確になり、属人的な対応から組織的な管理体制へ移行する道筋がつきました。今後は策定した規程の運用定着を図るとともに、BCP(※1)訓練や教育の継続的な実施を通じて、全社的な対応力の向上を進めていきます。

背景と課題

背景

属人化した管理体制とセキュリティ整備の遅れ

システム管理を一人で担当しており、日々の対応に追われ、組織的なルール作りや文書化が未着手でした。取引先からの要請で業界ガイドラインへの準拠が必要となりましたが、現状とのギャップが大きく、何から着手すべきか不明確でした。

- 属人的な管理体制
- ガイドライン準拠の要請
- 規程・ルールの欠如

課題

1. ネットワーク図や資産台帳がなく、保護すべき情報資産の全体像が不明確な状態
2. 共通IDの使い回しや、個人の記憶に頼ったパスワード管理など、認証管理の脆弱性
3. セキュリティ規程が存在せず、BCP(※1)も自然災害中心でITリスクが考慮外

取組内容

取組1　ネットワーク図と情報資産台帳の作成による守るべき情報の可視化

専門家の支援のもと、未整備だったネットワーク構成図を作成し、接続機器を棚卸ししました。また、ハードウェアだけでなく、契約、ライセンス、ドメイン等の無形資産や重要データを含めた資産台帳を整備し、管理対象を明確化しました。

取組2　実効性のあるセキュリティ規程の策定と認証管理の適正化

業界ガイドラインを参考にしつつ、自社の身の丈に合ったセキュリティ規程を策定しました。また、課題だった共通アカウント運用を見直し、重要システムへの多要素認証導入やパスワード管理ルールの見直し方針を決定しました。

取組3　ITリスクに対応したBCP(※1)への拡張と実効的な教育計画の立案

自然災害中心だったBCP※1を見直し、サイバー攻撃を想定した対応手順の検討を開始しました。また、形骸化していたクイズ形式の教育から、生成AIを活用した教材作成や理解度テストを伴うeラーニングへの転換を計画しました。

※1　Business Continuity Plan（事業継続計画：災害・事故・障害発生時でも重要業務を継続または早期復旧するための計画）

結果と今後

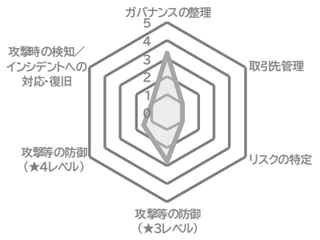
結果1　ネットワーク図と情報資産台帳を整備し、機器や重要データ、契約・ライセンスなどを含む管理対象を可視化しました。その結果、守るべき資産とリスクの所在が明確になり、限られた人員体制でも優先度を意識した効率的かつ計画的な情報セキュリティ管理が可能となりました。　→ 解決

結果2　業界ガイドラインを参考に、自社の実情に即したセキュリティ規程を策定しました。共通ID運用の見直しや認証管理方針の整理を進めたことで、個人の判断に依存した属人的な運用から、組織的なルールに基づく管理体制へ移行する明確な転換点となりました。　→ 継続

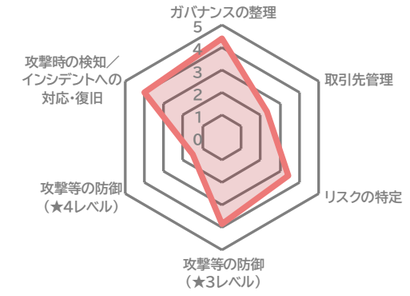
結果3　自然災害中心だったBCP※1を見直し、サイバー攻撃を想定した対応を検討するとともに、教育手法も刷新しました。次年度に向けて訓練やeラーニングを含む具体的な実行計画を策定し、継続的に改善を進めるための基盤が整いました。　→ 継続

取組テーマ　ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

情報セキュリティを単なる技術対策ではなく「経営管理の仕組み」として捉え直し、今回策定した規程の運用定着とメンテナンスを最優先に進めます。また、現場を巻き込んだBCP※1訓練の実施や、生成AIを活用した教育により、全社的な意識向上を図ります。

経営者の声

顧客企業よりサイバーセキュリティ強化の要求が厳しさを増す状況にあって、土台となる社内体制構築の機会を得たことに深い感慨を覚えます。リスクの明確化、規程の策定など、これまでわずか1名で進めた取組を全社的な情報リテラシーの変容へと繋げるべく、今春より教育計画を実践の場に移す予定です。

参加者の声

セミナー・ワークショップでは、他社様の取り組み状況や具体的な対策事例を共有いただき、自社の現状を客観的に見つめ直す良い機会となりました。また専門家派遣では社内課題の整理と優先順位付けが進み、今後の具体的な行動につながる実践的な学びとなりました。

建設・製造　樹脂加工製造業　D社

規模拡大に合わせたセキュリティの最適化、見える化と標準化でセキュリティ最新化と拠点間の格差を解消

企業プロフィール
従業員数：101～300名

セキュリティ体制
複数体制／兼務

事業内容
ガスケットやパッキン、フッ素樹脂、ゴム、カーボン材料の加工・販売を行う企業です。樹脂の切削や熱加工に強みを持ち、工業部品分野で機能性と精度を支える製品を提供しています。

背景と課題

社員数増と地方拠点設置からも時間経過し、セキュリティをより厳格化したいと考えていました。一方で、業務効率が落ちないための対策を検討していました。

取組内容

COO(※1)と各拠点（工場）のIT責任者とでセキュリティ担当者の会議体を作り、情報資産の管理と、資産ごとのリスク対策を行うなど体系的な仕組みなどを導入しました。

結果と今後

セミナー・ワークショップを通じて学習したセキュリティフレームワークと専門家派遣での助言を元に、各拠点のIT担当者で情報資産の洗い出しを行い見える化を推進するとともに、洗い出したリスクの分析や対策を検討し、自社での自主的かつ定期的なセキュリティ確保の仕組みのきっかけを作りました。

背景と課題

背景

事業規模の拡大・拠点の増加に伴い、セキュリティレベルの強化を検討

規模の拡大に伴い、工場や従業員数が増加した一方で、セキュリティの確保は古い知識に依存した教育や、特定の人に依存した管理になっていました。今後の規模拡大に備えて、継続したセキュリティ確保の仕組みと組織を導入したいと考えていました。

- 事業規模の拡大・拠点の増加
- セキュリティ基準・教育の古さ
- 明文化されていないセキュリティリスクと対策

課題

1. 現在の事業規模や拠点数にセキュリティ教育や仕組みが未成熟
2. セキュリティの継続的な確保に向けた専門的な知識が不足
3. 社員のITやセキュリティリテラシーに合わせた教育の実施不足

取組内容

取組1　セキュリティ確保の対象把握やセキュリティ確保を実施する仕組みの基礎を固め

業務に精通した社員の退職タイミングとも重なったため、全拠点のIT担当者にて拠点ごとの情報資産の洗い出す活動を行い見える化を実施しました。また、見える化した情報資産のうち、リスクが高いものに対してリスク対応計画を策定し、リスクに備える仕組みの導入も実施しました。

取組2　セキュリティ確保活動の継続的な実施の仕組みや体制の構築

当活動のセミナー・ワークショップを通じてセキュリティ確保のための主なフレームワークや管理すべき対象、内容などを学習しました。また派遣専門家の助言の下で情報資産管理台帳を起点とした自社の情報資産管理やリスク対策の定期的な見直しの仕組みを学ぶ取り組みを行いました。

取組3　社員へのITリテラシーや情報セキュリティ教育の底上げ

教育資料の入手や最適化、教育の手段や効果の確認方法など、専門家との対話を通じて対応が出来そうなことが分かりました。社内で取り組もうとしている課題を専門家に説明し、取り組み内容の客観的な評価やリスクを説明してもらい、自社で教育資料の整備から教育の実施、効果の確認までができる体制を作れる様に取り組みました。

※1　COO（Chief Operating Officer：最高執行責任者）

結果と今後

結果1　解決

各拠点ごとの情報資産の見える化の結果、思っていた以上に守るべき資産が多くあることが把握でき、また、リスク対応計画を実際に書いてみることで、想定されるリスク（不確実な要素）やリスクが顕在化した際に会社が受ける被害などが想像することができました。さらに、今まで特定の人に依存していた情報資産管理を仕組み化することができました。今後も年度単位などで継続して行きたいと思います。

結果2　継続

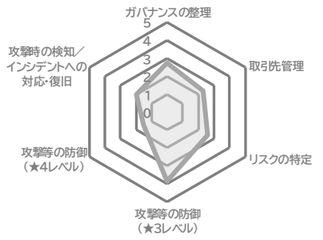
今回の活動に参加する前は、セキュリティ確保の全体像も知らず、どこから手を付けて良いのかも分からない状態のため、独自の基準で手当を行ってきましたが、情報資産管理台帳を起点として、定期的に何をどう見直せば良いのか理解できました。今後もこの活動を継続し、新しいリスクに備えられる様にしたいと思います。

結果3　継続

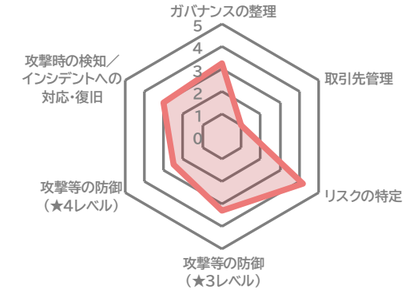
専門家との対話の中で、一般的にはどこから教育資料を入手し、どの様な手段で教育を行っているのか、またその効果はどの様に測定するのかを学びました。また独自の教育や啓蒙活動が必要になった際にAIを使った教育動画の作成などが便利なことやAIを使う際の注意点・リスクなどを学びました。今後も試行錯誤しながら教育の仕組みを整備して行きたいと思います。

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ **リスクの特定** ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

今回の活動を通じて、見えていない資産やリスクを把握できました。また、活動を各拠点のIT担当者に担当してもらったことで、属人化しないセキュリティ確保の仕組み化ができました。当社では素材加工を事業として行っていることから、大きなサプライチェーンに組み込まれることが多く、今話題のサプライチェーンにおける情報セキュリティ確保の要請増加が見込まれます。今後もこの仕組みを活かした情報セキュリティ確保を進めて行こうと思います。

経営者の声

社員 全員のデジタルリテラシーの向上を図りたいというのが目的でした。マイクロソフト365の導入を決断し、メール、チャット、クラウド、オンライン会議など、バラバラで管理がしにくかったリソースを統合し、アクセス管理を精度よく実施し、サイバーセキュリティのレベルアップをしていきます。

参加者の声

専門的な内容も多く難しさはありましたが、国が企業へセキュリティ強化を強く求めている現状を再認識しました。ワークショップで他社事例を聞けたことも有益で、特にサイバーレジリエンスの考え方が刺さりました。学びをチームに展開し成果につなげます。

建設・製造

アパレル製造販売業　E社

情報セキュリティ規程刷新とUSB制御・標的型攻撃メール訓練の実践

企業プロフィール

従業員数：101～300名

セキュリティ体制

複数名体制／兼務

事業内容

法人向けユニフォームやオリジナルアパレルを展開する企業です。業務用途に適した機能性とデザイン性を両立し、企業や現場のブランド価値向上を衣服面から支援しています。

背景と課題

当社にとって優先順位の高いセキュリティ対策は何なのか、当社の会社規模であれば、どのレベルまで対策すべきなのかが分からないため、勉強したいと考えました。

取組内容

セミナー・ワークショップで情報セキュリティの基礎を勉強しつつ、当社にとって必要な対策を専門家と相談して、優先順位の高いものから対策していきました。

結果と今後

関連規程作成や標的型攻撃メール訓練など、着実に推進することができました。社内導入済のセキュリティツールについても、活用の幅を広げるめどを立てることができました。来年度以降の対応計画案も作成することができましたので、セキュリティ委員会を活用してしっかりと実行していきたいと思います。

背景と課題

背景

セキュリティの知識不足で対策の優先度と必要範囲に悩み

専門的なセキュリティに関する知識が十分ではない中で、どういう順番でセキュリティを対策していったらいいのか、また当社の会社規模であれば、リソースの制約がある中でどの程度の対策が必要になってくるのか、悩んでいました。セキュリティ対策を客先からも求められる中で、セキュリティ知識習得が必要と感じていました。

- セキュリティ関連規程が不十分な内容
- 社内導入ツールの活用が不十分
- 標的型攻撃メールのリスク対応

課題

1. 情報セキュリティ関連規程における今日的要件への未対応
2. セキュリティツールを総務が主体となって導入したが、システム部門としては活用が不十分
3. 標的型攻撃メールのリスクに対応するため、社員の訓練が必要

取組内容

取組1　セキュリティ関連規程の抜本的見直しとセキュリティルールの明確化

過去に定めた情報セキュリティ基本方針と情報システム管理規程は今日的にみると十分な内容ではないので、抜本的に見直してIPA※1の情報セキュリティ関連規程（サンプル）をベースに作成することとしました。見直す中で曖昧だったセキュリティルールの明確化を図りました。

取組2　セキュリティツールを利用してのUSBの使用禁止

総務が主体となって導入したセキュリティツールを使えばUSBの使用禁止を実現できることが専門家との会話の中で判明しました。早速、USBの使用を禁止する方向で調整を開始しました。

取組3　標的型攻撃メールの訓練を実施して社員のセキュリティ意識を向上

標的型攻撃メール対策として訓練メールを用いた疑似攻撃を実施し、開封状況の分析や開封してしまった人への注意喚起、訓練結果の共有を通じて社員の意識向上と被害未然防止に取り組みました。

※1　独立行政法人情報処理推進機構
※2　SCS評価制度（サプライチェーン強化に向けたセキュリティ対策評価制度）

結果と今後

結果1

IPA※1の情報セキュリティ関連規程（サンプル）をベースに規程を作成しました。この規程の運用を開始する準備を進めています。来年度できるだけ早く、規程の教育を全社員に対して実施し、セキュリティ意識の向上を図っていきたいと考えています。

→ 継続

結果2

USBの使用を禁止する方向で調整を進めたところ、ネット銀行等どうしても利用しなければならないケースがあることが判明しました。使用許可申請が出された場合は使用を認めるという運用ができないか、READはOKだがWRITEは禁止とできないかなど、検討しています。

→ 継続

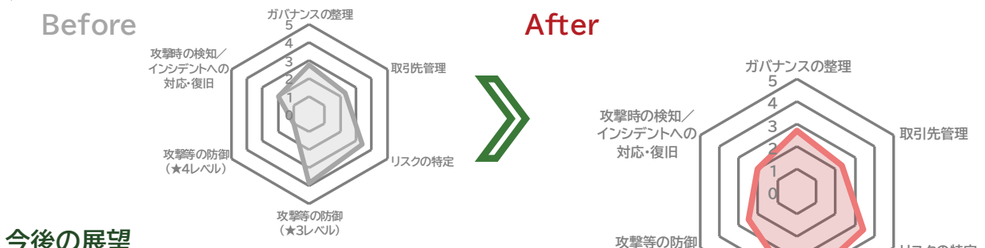
結果3

標的型攻撃メール対策として訓練メールを用いた疑似攻撃を実施したところ、多くの人が開封してしまいました。開封してしまった人への注意喚起を実施し意識向上を図りました。今後も定期的に訓練を実施し、開封者0を目指していきたいと思います。

→ 継続

取組テーマ

ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧



今後の展望

情報セキュリティの規程整備と体制構築が着実に進み、USB制御やバックアップ強化など技術面の向上も視野に入っています。今後は経営会議での承認を得つつ、情報資産管理台帳の完成、組織体制の確立、運用ルールの徹底を図ることで、実効性の高い情報セキュリティ基盤を強固にしていきたいと思います。また、来年度開始予定のSCS評価制度※2で成熟度★3を早期に達成できればと考えています。

経営者の声

当社は法人向けユニフォームを展開しており、顧客からの信頼が何より重要です。昨今、取引先からも厳格なセキュリティ対策が求められる中、今回の取り組みで規程整備と技術的対策の両面を強化できたことは、経営基盤の安定化に直結する成果だと感じています。今後もセキュリティ委員会を中心に、実効性の高い組織体制を確立してまいります。

参加者の声

専門知識が不足する中、自社の規模感に合った対策レベルをご教示いただけたことが大変助かりました。IPA※1のサンプルを活用した規程の見直しや、標的型攻撃メール訓練の実施など、着実に体制を整えることができました。訓練では開封者が多かったという課題も見えましたが、これを糧に開封者ゼロを目指し、継続的な意識向上に取り組んでいきます。

建設・製造

医療関連製造業　F社

セキュリティガイドライン策定とあわせ、セキュリティ強化を意識したネットワーク環境の再構築

企業プロフィール

従業員数：101～300名

セキュリティ体制

1名体制／専任

事業内容

医療・衛生関連製品の製造や包装・滅菌体制を備える企業です。複数拠点で生産・品質管理を行い、安全性と安定供給を重視したものづくりで医療分野を支えています。

背景と課題

社内ネットワークの老朽化が進み、通信不具合の他、構成の最適化を含めリプレースの検討とともに、セキュリティ強化の視点を加えて実施したいと考えていました。

取組内容

ITベンダーに依存している状況でしたので、自社内で状況を把握し対応できる力をつけたいと考え、情報資産の洗い出しとリスクアセスメント実施などに取り組みました。

結果と今後

情報資産の洗い出しとリスクアセスメントが完了し、強化すべき対象と、優先順位が可視化されました。次年度でのリプレース計画とあわせ、新拠点のネットワークも同様の進め方を実施することで、組織として一貫したセキュリティレベルを担保できるように進めていきます。

背景と課題

背景

セキュリティ強化とあわせ、リスク管理された社内ネットワークを構築を検討

ネットワーク老朽化に伴い、通信不具合なのか、セキュリティリスクなのか判断ができない状況が続いておりましたが、ITベンダーへの依存度が高く明確に改善できない状況でした。そこで、本事業を活用し自社の力量アップ含め最適な環境を目指した活動を実施したいと考えました。

- 情報資産リスクの可視化と管理能力強化
- 社内ネットワーク強化の実施
- 社内力量アップ環境の構築

課題

1. ネットワーク環境を再構築するにあたり、状況の把握が足りていない事により、方針含め策定が未整備
2. ネットワーク不具合含め、業務影響が出ている環境を改善が未徹底
3. セキュリティに関しての社内教育がなく情報収集が属人化

取組内容

取組1　情報資産洗い出しとリスクアセスメントの実施

本事業の専門家から、ISMS※1をベースとした情報資産におけるとりまとめとリスクアセスメント手順について、社内情報をもとに伴走形式で支援を頂きました。ここで得たナレッジをさらに活用し、適応範囲を順次広げています。

取組2　新ネットワークセキュリティ要件の策定と社内ネットワーク環境の再構築

実施したリスクアセスメント結果をもとに、社内ネットワーク環境のリプレース方針の策定を進めました。また、本来想定されていなかった環境においても視野を広げることで、全社的な要件標準化にも横展開していきます。

取組3　簡易脅威インテリジェンス環境の策定

まずは、全社的に脅威情報を集める仕組み化とその運用ルールの検討を実施し、ガイドラインの制定を進めています。その他、力量アップに関するテストや、Webベーストレーニング等についても情報収集を並行し、順次仕組み強化を計画しています。

※1　情報セキュリティマネジメントシステム（組織の情報資産を守るために、リスク評価・管理策・運用・改善を体系的に管理する仕組み）

結果と今後

結果1

IT ベンダーからの意見だけでなく、自社内においても、現状どのような機器で、どれだけ大きいリスク発生源が潜んでいるのかを客観的に把握することができるようになりました。また、IT投資における優先順位付けにも有効活用が見込まれています。

→ 解決

結果2

本社社内ネットワーク環境のリプレース方針が決まったことで、実際に次年度以降で実施目途を立てることができました。また、拠点ネットワークについても、合わせて同レベルの要件で実施計画を立てることができ、全社的なセキュリティ強化におけるガバナンス力も向上していくと感じています。

→ 解決

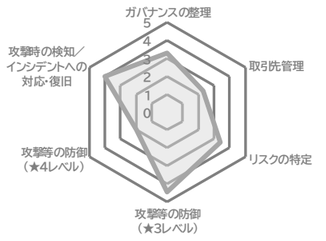
結果3

社内グループウェア等の既存情報共有基盤を活用し、運営できないか現在継続検討中です。また、全社的な運営方針となるため、関係部署等との協業調整も含め、次年度以降も継続して活動していきます。

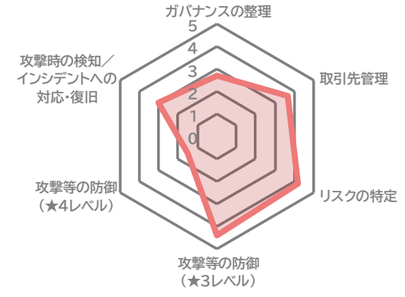
→ 継続

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ **リスクの特定** ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

今回計画した、ネットワーク強化・リプレースの実装をインターネット回線や電話回線の2重化も視野に入れて進めます。また、情報セキュリティ教育環境の整備とともに、ITベンダーとの役割・分担のバランスを考えた運用ができる体制構築を進めていきます。

経営者の声

ネットワーク環境が大きく変化を起こす近年の状況から、企業のサイバーセキュリティに対する意識と変化に対応できる知識を社内に植え付けられる人材の育成を期待した。社内システムへの脅威を最小限に留める技術形成可能な環境構築を進めていく。

参加者の声

近年、サイバー攻撃が身近なところで実際に起きている中でセキュリティの重要性や日常業務の中で気を付けるべき具体的な対策について本プログラムを通して学ぶことができた。今回学んだ内容を今後の業務や日常生活の中でも意識し、安全な情報管理に努めていきたいと考える。

建設・製造　広告・販促支援業　G社

インシデント対応力向上に向けた構成図整備と実践的教育の取組

企業プロフィール
従業員数：101～300名

セキュリティ体制
複数名体制／専任

事業内容
コミュニケーションプランニング、クリエイティブ、デジタル・フィジカルプロモーションを総合的に手がける企業です。顧客のブランド価値向上に向け、販促領域を一貫して支援しています。

背景と課題

Pマーク(※1)取得や規程整備、社員教育は進めてきたが、実際のインシデント対応力や社員のセキュリティ意識に不安があり、実践的対策を課題と考えていました。

取組内容

インシデント初動対応(特にランサムウェア)や効果的な社員教育など実践的準備に取り組みました。

結果と今後

ネットワーク構成図と対応フロー整備が進み、迅速なインシデント対応体制を構築しました。AP(※2)更新に向け図面も継続見直しを行いました。また、ヒヤリハット共有体制を強化し、管理部門主導で全社周知を推進しています。IPA(※3)教材を活用した定期的な教育で社員のセキュリティ意識向上を図る予定です。

背景と課題

背景

高度化するサイバー脅威と監査指摘を契機に自社の情報セキュリティ対策強化の必要性を痛感

Pマーク※1の更新や独自の取組を進めてきましたが、サイバー攻撃の高度化や社内監査での指摘、関連会社でのランサムウェア感染を受け、現在の対策が十分に機能しているのか懸念が生じました。初動対応手順の曖昧さや社員教育の不足、古い端末の残存など運用面の課題も見え始め、今のままでは不十分でした。

- 社内監査での指摘
- 初動対応手順の曖昧さ
- 社員教育に対する不安

課題

1. インシデントが実際に発生した際の具体的な対応の想定が困難
2. インシデントとして対応する範囲がアクシデントのみと限定的
3. 体制や規程は設けているものの従業員までセキュリティ意識が浸透しているのか不安

取組内容

取組1　ネットワーク構成図(論理・物理)の見直しとインシデント対応フローの整備

専門家と既存の論理・物理構成図を確認し、VLAN※4情報の追記や機器リスト整備を行い、インシデント時の影響範囲特定と属人化防止を目的とした構成図の精度向上に取り組みました。また、インシデント発生時の対応フローは、緊急連絡先や対応手順を明記し、ランサムウェアを含むインシデントごとに複数作成し、緊急事態に備えました。

取組2　ヒヤリハット事例のリスト化と社内共有体制の強化

社内で発生したヒヤリハット事例の整理と社内ポータルサイトでの注意喚起ページ作成を進めるとともに、IPA※3やJPCERT/CC※5の最新情報を社内ポータルサイトに表示し社員のセキュリティ意識向上を図りました。

取組3　教育コンテンツの活用と社内セキュリティレベル向上施策の推進

IPA※3の教育動画や資料を社内ポータルサイトへ掲載し、あわせて社内システムのログイン時に桁数の多いパスフレーズ方式を採用するなど、社員のセキュリティリテラシー向上に取り組みました。

※1　プライバシーマーク(個人情報を適切に管理・運用している事業者として認定されたものに付与される制度)
※2　Access Point(無線LANアクセスポイント。Wi-Fi の電波を発し、端末をネットワークに接続させるための機器)
※3　独立行政法人情報処理推進機構
※4　Virtual LAN(物理ネットワークを仮想的に分割し、異なるグループの通信を論理的に分離する仕組み)
※5　JPCERT/CC(一般社団法人　JPCERTコーディネーションセンター)
※6　SCS評価制度(サプライチェーン強化に向けたセキュリティ対策評価制度)

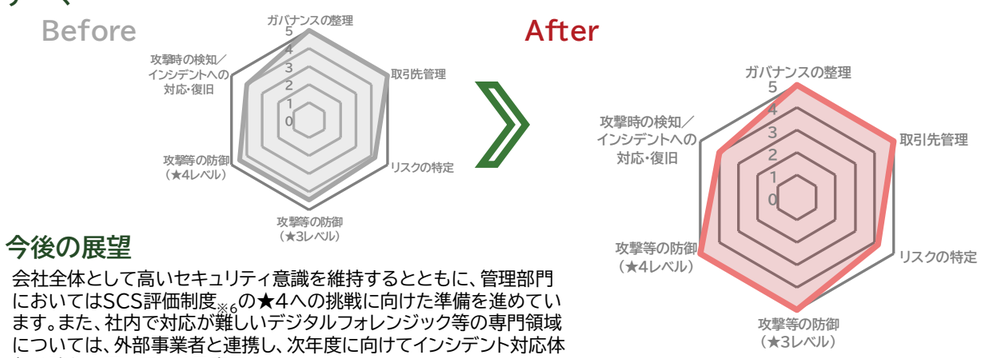
結果と今後

結果1　インシデント対応フロー資料の作成およびネットワーク構成図の整備が順調に進み、インシデント発生時にも迅速な対応が可能となる体制を整えました。また、2026年4～5月には無線AP※2の全台数リプレースを予定しているため、ネットワーク構成図については今後も随時見直しを行う予定です。　→　継続

結果2　社内ポータルサイトを活用し、各種セキュリティリスクに関する注意喚起を行う体制を整備しました。今後も管理部門が中心となり、セキュリティリスク情報を迅速に把握し、全社へ速やかに共有・周知する仕組みを確立していく予定です。　→　継続

結果3　IPA※3が提供する動画や資料を活用し、社内ポータルサイトや朝礼等の機会を通じて、社員向けセキュリティ教育を定期的に実施する計画を策定しました。管理部門が中心となって取り組むことで、社内におけるセキュリティリスクへの意識向上が図られています。　→　継続

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ **リスクの特定** ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧



今後の展望

会社全体として高いセキュリティ意識を維持するとともに、管理部門においてはSCS評価制度※6の★4への挑戦に向けた準備を進めています。また、社内で対応が難しいデジタルフォレンジック等の専門領域については、外部事業者と連携し、次年度に向けてインシデント対応体制の強化を図っていく予定です。

経営者の声

専門家派遣やセミナー等を通じて、自社のセキュリティ対策やインシデント対応を総点検する貴重な機会となりました。具体的な改善策への評価や最新動向の共有は非常に有益で、継続的な対策の重要性を再認識しました。今後も情報収集に努め、組織的なレベルアップに取り組んでまいります。

参加者の声

講義ではポイントをとらえた丁寧な説明のおかげで理解が深まりました。またワークショップを通して自社の体制の現状や必要な対策を振り返る機会となり、他社のセキュリティ担当者との意見交換は新たな気付きを得るきっかけになりました。今回学んだ事を活かし、セキュリティ強化に向けた取組を進めていきます。

建設・製造

設備工事業　H社

既存対策の不足を補い規程整備と体制強化でSCS評価制度(※1)★4を目指す実践

企業プロフィール

従業員数：101～300名

セキュリティ体制

複数名体制／専任

事業内容

電気・通信設備や内装設備の企画・設計・施工、ネットワーク構築、入退室管理や監視カメラまで手がける企業です。オフィスや施設の機能性と安全性を支える総合設備会社です。

背景と課題

セキュリティ関連の事業者として、来年度開始予定のSCS評価制度(※1)で成熟度★4を早期に取得するため、現状の不足点を的確に把握し改善を急ぐ必要がありました。

取組内容

成熟度★4達成に向け改めて、体制・規程・技術の観点で課題を洗い出し、改善方針を整理して具体策の優先順位付けまで検討しました。

結果と今後

現状整理と課題抽出により、体制整備・規程改訂・監視検知の強化など成熟度★4の早期達成に向け重点的に強化すべき領域が明確となり、対応の道筋が具体化しました。今後は、「サイバー攻撃による『深刻な被害』ゼロ」を目指して当社のDXをもっと安全に」をスローガンに、課題別に優先度と期限を定め、KPI(※2)で進捗を管理しながら施策を計画的に実装し、継続改善の仕組みを確実に定着させます。

背景と課題

背景

SCS評価制度(※1)★4を目指すために、実効性と継続性を重視したセキュリティ強化が急務

助成金申請を機に★2を宣言し、次の段階としてIPA(※3)・経産省が検討を進めるサプライチェーン強化に向けたSCS評価制度(※1)での★4達成を目標に掲げました。既存対策は一定整備されていましたが、リスク管理・体制・運用に課題が残り成熟度要件との差がありました。そこで不足するルールや責任分担を再整理し、実効性と継続性を重視したセキュリティ強化が必要でした。

- ★4達成を見据えた体制強化
- 規程と運用の乖離是正
- 高度化する脅威への対応

課題

1. セキュリティ体制や責任分担が十分に整理されておらず、継続的改善サイクルが未確立
2. 機密区分やバックアップ等の実運用が規程に合っておらず、実効性のある管理が不徹底
3. 侵入前提の検知・分析体制やログ確認が不十分で、脅威への早期対応が困難な状況

取組内容

取組1　セキュリティ委員会を中核とした統制体制を明確化し、継続的改善の実現

セキュリティ委員会を不定期開催から定期開催へ移行し、情報セキュリティと個人情報保護を横断的に統制する体制を検討しました。教育責任者を明確化し、教育計画・実施結果・課題を委員会で共有し評価することで、継続的改善サイクルが機能する管理体制の構築を進めました。

取組2　機密区分およびバックアップ運用を実務に即して再設計

機密区分が細分化され運用しづらい点と、バックアップが3-2-1ルール未達である点を課題として整理し改善方針を検討しました。区分は実務に即して簡素化し、手順周知と責任分担を明確化のうえ、異媒体・オフサイト保管を含む運用へ移行する体制整備を進めました。

取組3　侵入前提の考え方に基づき検知・分析・初動対応能力を段階的に強化

ログ取得に加え、定期的な確認・分析を運用へ組み込み、異常を早期に検知できる体制を整備しました。あわせて社内負荷を踏まえつつ、侵入後の被害拡大を抑止する対応力向上を目的に、外部監視も可能なXDR(※4)導入を検討しました。

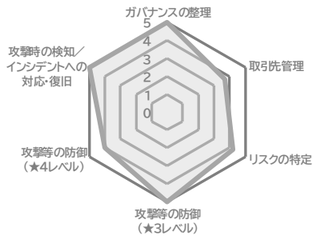
※1　SCS評価制度（サプライチェーン強化に向けたセキュリティ対策評価制度）
※2　Key Performance Indicator（重要業績評価指標：組織や業務の目標達成度を定量的に測定するための指標）
※3　独立行政法人情報処理推進機構
※4　Extended Detection and Response（EDR を拡張し、複数領域の脅威を横断的に検知・分析・対応する仕組み）
※5　プライバシーマーク（個人情報を適切に管理・運用している事業者として認定されたものに付与される制度）

結果と今後

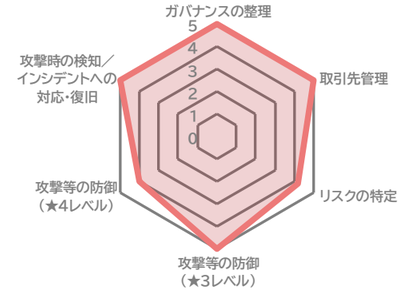
結果1	検討の結果、セキュリティ対策は個別に実施されている一方で、体制や意思決定、改善の流れが整理されておらず、全社統制が弱い点を確認しました。今後はセキュリティ委員会を定期開催し、Pマーク(※5)運用と連携した役割分担を明確化します。計画立案から実施、評価、改善までを継続的に回す管理体制を整備し、実効性の高い運用定着を図ります。	継続
結果2	機密区分とバックアップに関する実務が十分に運用できていないことが判明し、現場での統一運用に課題があると確認しました。今後は情報資産の重要度に応じて実行可能な機密区分を再定義し、判断基準と手順を明確化します。あわせて3-2-1ルールの考え方に基づき、媒体の分散とオフサイト保管を含むバックアップを段階的に整備します。	継続
結果3	基本的なセキュリティ機器は導入されている一方、侵入後の挙動検知やログ分析が十分でなく、兆候把握と初動判断に遅れが生じ得る点を課題として整理しました。今後はログの定期確認を手順化し、アラート対応の責任分担も明確化します。定期訓練も実施し、社内負荷を抑えつつ監視できるXDR(※4)を段階導入して、侵入前提の検知・初動対応力を強化します。	継続

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

本事業を通して、対策は個別に実施されている一方、体制・意思決定・改善の流れや機密区分、バックアップ運用、侵入後の検知とログ分析に課題が残りました。今後はセキュリティ委員会を開催しPマーク(※5)と連携した役割分担を明確化、計画・実施・評価・改善を課題管理で回します。併せて資産重要度に応じた区分再定義と3-2-1準拠のバックアップ整備、復旧訓練、ログ確認とXDR(※4)導入により統制と初動対応力を継続強化します。

経営者の声

サイバーセキュリティ対策は、当社の存続と成長を左右する重要な経営判断の一つです。今回の専門家派遣等を通じて、運用面の不足が明確になりました。今後は監視体制や規程の整備、社員教育を強化し、DX推進とセキュリティ確保を両立した強固な体制を全社一丸となって構築してまいります。

参加者の声

「深刻な被害ゼロ」のスローガンのもと、専門家の支援により当社の課題が明確になりました。現場と乖離していた機密区分やバックアップ運用を見直し、監視体制の強化を図ります。また、全社一丸となって強固な体制を構築するため、現場での継続的な改善サイクルと社員教育に取り組んでまいります。

建設・製造　プラスチック製造業　I社

ID・権限管理の統合および情報資産管理台帳の整備で、サイバー攻撃を想定したBCP(※1)・セキュリティ強化の実践

企業プロフィール
従業員数：301名以上

セキュリティ体制
複数名体制／兼務

事業内容
工業用精密プラスチック部品の設計・製造・販売と、金型の設計・製作を手がける企業です。量産体制と技術力を生かし、幅広い産業向けに高品質な部品供給を行っています。

背景と課題

取引先のガイドライン適合を目指すが、認証基盤や情報資産管理が未整備であり、サイバー攻撃を想定したインシデント対応体制も不明確だった。

取組内容

ID・権限管理基盤導入の検討、重要情報の定義と資産台帳の整備方針策定、およびサイバーリスクを想定したBCP(※1)の論点整理を行った。

結果と今後

メール対策や資産管理の論点が整理され、具体的な整備方針が定まった。次年度に向け、認証基盤構築、資産台帳の全社展開、手順書策定と訓練実施の計画を立案した。

背景と課題

背景

ガイドライン適合に向けた認証基盤と資産管理の整備が未着手

取引先要請で業界ガイドライン適合が必要だったが、オンプレミスとクラウドを統合した ID・権限管理基盤がなく個別管理で、共有PCでの本人特定が困難だった。また、ハードウェア以外の情報資産管理が未着手であり、BCP※1もサイバー攻撃を想定していなかった。

- 認証基盤が未導入で個別管理の状態
- データの重要度定義と管理が不十分
- サイバー攻撃想定のBCP(※1)が未整備

課題

1. 共有PCが多くID管理が煩雑なため、統合認証基盤による本人確認と管理の統一が必要
2. 資産管理がハードウェア偏重のため、重要データの定義とリスクに応じた管理台帳が必要
3. BCP(※1)が自然災害中心のため、サイバー攻撃を想定した復旧計画と対応体制の構築が必要

取組内容

取組1　統合認証基盤の導入検討と共有PC対策の整理

現状の個別認証のリスクを分析し、オンプレミスとクラウドを統合した ID・権限管理基盤を用いた統合管理の導入を検討しました。特に工場等の共有PCにおける本人特定（多要素認証の活用等）の運用ルールや、コストと運用のバランスを考慮した導入計画を策定しました。

取組2　情報資産管理台帳の整備と重要情報の定義付け

既存のIT資産管理ツールの機能不足を確認し、ハードウェアだけでなく業務データを含めた管理台帳の構成を検討しました。全部署の保有情報を洗い出し、機密性に応じた「重要情報」を定義して管理する方針を固めました。

取組3　サイバーインシデントを想定したBCP(※1)策定支援

従来の自然災害用BCP※1とは区別し、サイバー攻撃発生時の事業継続計画の要件を整理しました。被害を最小限に抑えるための初動対応（ログ保全やネットワーク遮断）の手順書作成に向けた論点整理と体制検討を行いました。

※1　Business Continuity Plan（事業継続計画：災害・事故・障害発生時でも重要業務を継続または早期復旧するための計画）

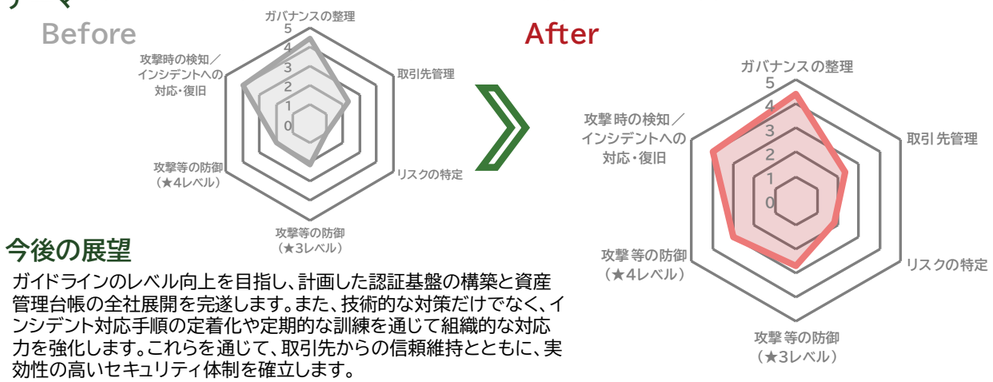
結果と今後

結果1
共有PCが多い現場特性やオンプレミスとクラウドが混在する環境を踏まえ、統合認証基盤の必要性と具体的な導入方式（クラウド連携・多要素認証活用）が明確になりました。次年度は設計・構築を進め、全社で一元的なアカウント管理と本人特定の確実性向上を図ります。
→ 継続

結果2
ハードウェア偏重だった管理を見直し、業務データを含めた情報資産の管理対象と粒度が整理されました。次年度は各部署へのヒアリングを通じて台帳を完成させ、重要度に応じた管理、定期的な棚卸しとリスク分析を行う運用を開始します。
→ 継続

結果3
サイバー攻撃を想定したBCP※1の観点から、インシデント対応の論点整理により対策範囲と初動対応の考え方が明確になりました。次年度は手順書の文書化を完了させ、標的型攻撃訓練やBCP※1訓練を通じて実効性を高めます。
→ 継続

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧



今後の展望

ガイドラインのレベル向上を目指し、計画した認証基盤の構築と資産管理台帳の全社展開を完遂します。また、技術的な対策だけでなく、インシデント対応手順の定着化や定期的な訓練を通じて組織的な対応力を強化します。これらを通じて、取引先からの信頼維持とともに、実効性の高いセキュリティ体制を確立します。

経営者の声

本事業を通じて、認証基盤と情報資産管理の整備が全社の安全性向上と業務の安定化につながることを期待しました。今後は運用の定着と訓練を継続し、サイバー攻撃にも揺るがない事業継続力を高めていきます。また、取引先からの信頼をより強固にする取り組みに力を入れていきます。

参加者の声

今までのセキュリティ対策は、取引先から要求されているガイドラインに適合させることに注力していましたが、当該事業に参加することで、より広い範囲でのセキュリティ対策を知ることができるいい機会となりました。今後も得られた知見を社内に浸透させていけるようにします。

建設・製造　化粧品・医薬品製造業　J社

研修と規程整備を軸に、段階的なリスク可視化と教育定着で組織全体の情報セキュリティ水準を向上

企業プロフィール
従業員数：301名以上

セキュリティ体制
複数名体制／専任

事業内容
オーラルケア、スキンケア、医薬部外品分野を中心にODM製品を展開する企業です。長年の技術力と開発力を基盤に、健康と美容に関わる製品づくりで多様なニーズに応えています。

背景と課題

昨今の被害増加を受けて、セキュリティ水準向上の必要性を認識する一方、対策の到達点や網羅性が不明確で、従業員への浸透不足が課題でした。

取組内容

研修で知識を習得しリスクを洗い出すとともに、規程の実効性を高め、ハンドブック運用を徹底し全社的な底上げを図りました。

結果と今後

研修で得た知見を踏まえ現状を再点検した結果、見落としていたリスクや改善点を把握し、具体的な対策につなげました。情報資産の棚卸しにより業務の無駄や管理不備も可視化され、業務改善にも波及しました。今後は改善策の定着と継続的な見直しを進め、より実効性ある体制強化を図ります。

背景と課題

背景

世情を踏まえ、情報セキュリティの水準向上の必要性を強く感じている

相次ぐセキュリティ被害の報道を受け、自社の対策強化の必要性を強く認識していました。必要と考えられるツールは導入しているものの、その水準が十分か判断できず、規程整備も最低限にとどまっていました。従業員へのルール浸透状況にも不安があり、全社的な見直しが課題となっていました。

- ゴールが不明瞭
- ツール以外の対策の必要性
- 従業員のセキュリティ意識

課題

1. セキュリティ対策の十分性・網羅性に対する不明確さ
2. 情報セキュリティ関連規程の見直しの必要性を認識
3. 情報セキュリティのルールの従業員への浸透状況が不明瞭なため不安

取組内容

取組1　情報セキュリティマネジメントの習得と自社への適用の実施

セミナーやワークショップに積極的に参加し、情報セキュリティに関する知識の深化を図りました。あわせて得られた理解を踏まえ自社のリスクを洗い出し、既存規程の妥当性を点検するとともに、見直すべきポイントの整理と改善策の検討を進めました。

取組2　情報セキュリティ管理規程類の実効性の向上

最近の情報セキュリティ事故の報道を踏まえ、情報セキュリティ関連の規程等を精査し、自社運用で同様の問題が生じ得る箇所を点検しました。さらに情報資産管理台帳を作成してリスクや弱点を可視化し、追加すべきルールや手順改善を整理して実効性向上を図りました。

取組3　教育体制の充実を行い、規程類が確実に実施・定着することを促進

信頼性の高い教材としてIPA※1が提供する資料を積極的に活用しました。従来はハンドブック改訂時の掲載に留まっていたため、教育内容と実務の乖離を点検し、逸脱の是正を進めることで教育効果の向上とルール定着の強化を図りました。

※1　独立行政法人情報処理推進機構

結果と今後

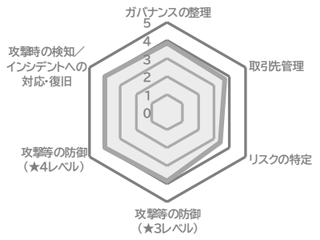
結果1
集合研修やワークショップで得た知見を踏まえ自社の現状を再点検した結果、見落としていた情報資産や業務プロセス上のリスクを把握することができました。規程の全面改訂には至りませんでしたが、検討過程でバックアップ体制など改善点を特定し是正を実施しました。今後の規程整備や運用高度化を進めるための基盤づくりとして有意義な一歩となりました。
→ 継続

結果2
情報資産管理台帳の作成にあたり、業務負担増への懸念があったため、全社展開に先立ち自部門および関連部門で試行しました。その結果、不要または陳腐化した情報資産を把握し、整理・更新を実施しました。これにより情報セキュリティ管理の効率化に加え、業務改善の効果も確認できました。今後の全社展開に向けた実践的な基盤が整ったと考えています。
→ 継続

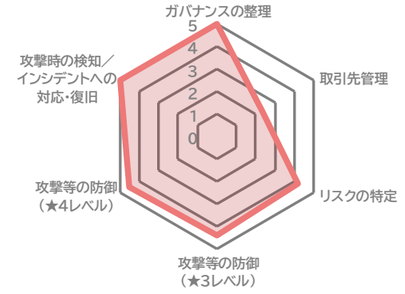
結果3
従来はセキュリティハンドブックを掲載するのみで周知が不十分でしたが、業務実態との乖離を点検し是正を図ったことで、現場の意識向上と行動変容が進み、ルール逸脱の抑止につながりました。今年度はIPA※1教材の確認にとどまりましたが、今後は積極的に活用し、教育内容の充実とハンドブックの品質向上を図ってまいります。
→ 継続

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

情報資産台帳の全社的な整備を着実に進めるとともに、関連規程の見直しと運用状況の点検を通じて実効性の向上に取り組みます。あわせて外部研修の積極的な活用やセキュリティハンドブックの定期的な改訂を実施し、従業員一人ひとりの理解と意識を高めます。これらの取組を継続することで、組織全体のセキュリティ基盤を段階的に強化し、安定した事業運営を支える体制の確立を目指します。

経営者の声

本事業にIT部門の中核社員を受講させた結果、セミナーやワークショップを通じて、情報セキュリティはIT部門だけの問題ではなく、事業継続や企業価値、対外的な信頼に直結する重要な経営テーマであることを改めて認識する機会となった。漠然としていたセキュリティ対策の進め方が整理され、役員会で受講者より報告も実施、経営層の視点からも着手すべきポイントが明確になった点は大きな成果である。今後も、情報セキュリティを経営の重要課題の一つとして位置づけ、継続的な点検と改善を重ねることで、安定した事業運営と信頼性の高い組織基盤の構築が期待される。

参加者の声

本事業に参加したことで、自社の情報セキュリティ対策を体系的に見直す機会となりました。受講前は自社の対策範囲や従業員へのルール浸透に課題がありましたが、セミナー後には着手すべきポイントが明確になり、体制づくりも進みました。研修を通じて管理や教育の重要性を再認識し、ツールだけでなく総合的な取り組みが必要だと感じました。受講後は規程の点検や情報資産台帳作成に取り組み、業務改善やバックアップ体制の見直しにつなげることができました。今後も継続的に対策を進め、セミナーで得た知見を基に全社の教育を展開し、組織のセキュリティ強化と安定した運営を目指します。

サービス・その他　コンサルティング業　A社

海外取引先に信頼されるためのクラウド環境に適したセキュリティ体制構築

企業プロフィール
従業員数：1～5名

セキュリティ体制
1名体制／兼務

事業内容
ジム運営サポートを中心に、課題整理や戦略見直し、実行支援を行う企業です。中長期視点で運営改善を支え、施設ごとの状況に応じた実務支援を通じて継続的な成長を後押ししています。

背景と課題

海外取引拡大のため信頼性向上が急務でしたが、専任者不在で資産管理やルールが未整備の状態でした。

取組内容

資産の洗い出しによる管理台帳の作成、実情に即した規程（ハンドブック）策定、従業員教育を行いました。

結果と今後

情報資産と運用ルールの可視化が進んだことで、セキュリティ対策が経営課題として明確に認識されるようになりました。属人的な管理から脱却し、組織としての対応方針が整理されたことを踏まえ、今後はバックアップやログ管理等の技術的対策を段階的に強化していく方針です。

背景と課題

背景

海外取引拡大に向けた信頼性確保と管理体制の構築が不透明

社員数名で運営し、バックオフィス業務はクラウドサービス中心です。今後、海外企業との取引拡大を計画しており、対外的な信頼性を担保するためセキュリティ体制の構築が急務でした。しかし、専任担当者が不在で何から着手すべきか不明確な状況でした。

- 海外取引拡大への対応
- クラウド中心の業務環境
- 専任不在と知見不足

課題

1. 保有情報資産が不明確で、守るべき対象が特定できていない状態
2. 明確な規程が存在せず、セキュリティ対策が個人のリテラシー任せ
3. 将来の組織拡大を見据えた、体系的な教育の仕組みが未整備

取組内容

取組1　情報資産の洗い出しと管理台帳の整備による「守るべきもの」の可視化

PC、スマホ、クラウドサービス等の資産を洗い出し、情報資産管理台帳を作成しました。情報の所在や重要度を整理することで管理対象を明確化し、退職時のアカウント削除や最小権限の原則適用など、具体的な運用ルール策定の基盤を築きました。

取組2　クラウド中心の業務環境に適したセキュリティ規程（ハンドブック）の策定

IPA※1のひな形を参考に、オンプレミス機器が少ない自社環境に合わせて内容を精査しました。形式的な規程ではなく、社員が理解しやすい「セキュリティハンドブック」として整備し、日々の業務に直結するルールの明文化を進めました。

取組3　全従業員への意識教育と外部研修の活用によるリテラシー向上

作成したハンドブックを用いた社内教育の枠組みを検討しました。また、最新の脅威動向を把握するために外部のセキュリティ講習への参加を決定し、経営層を含む全従業員が当事者意識を持ってセキュリティに取り組む文化の醸成を図りました。

※1　独立行政法人情報処理推進機構
※2　SECURITY ACTION（セキュリティアクション：中小企業が情報セキュリティ対策に取り組んでいることを自己宣言する制度）

結果と今後

結果1　解決

情報資産管理台帳の整備により、これまで把握が不十分であった情報資産の所在や重要度、想定されるリスクが可視化されました。個人の判断や経験に依存した管理から脱却し、組織として情報資産を管理・保護する意識が社内に定着しつつあります。これにより、セキュリティ対策を計画的に検討・実施するための基盤が整いました。

結果2　継続

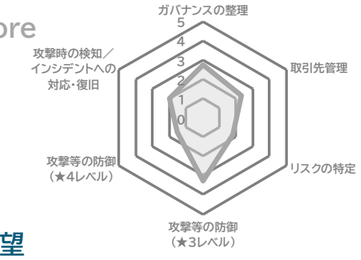
クラウド上のデータに対するバックアップやログ管理といった技術的対策については、その重要性が社内で共有され、実施方針の整理まで進みました。一方で、具体的なツール選定や導入方法、運用体制の構築については検討段階にとどまっており、実運用の開始に向けた対応が今後の課題として認識されています。

結果3　継続

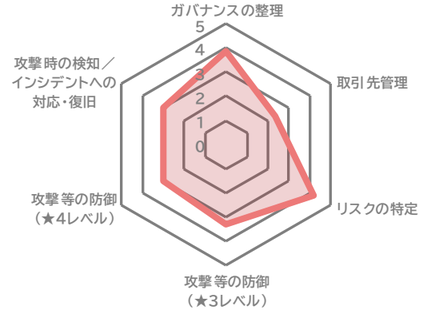
セキュリティハンドブックの作成に着手し、日常業務に即したルールの整理を進めました。内容の完成および全社的な周知徹底を継続して取り組みます。また、単発対応にとどまらないための定期的な教育サイクルの確立に取組んでいきます。引き続き次年度にかけて、これらの教育・周知・運用の定着を図る必要があります。

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

今後は、整備した情報資産管理台帳とハンドブックの運用を定着させます。また、クラウドデータのバックアップやログ監視体制の構築など技術的対策も強化します。将来的にはSECURITY ACTION※2の宣言等も視野に入れ、海外取引先からも信頼される体制を目指します。

経営者の声

この度は、貴重なアドバイスをいただきありがとうございました。セキュリティの現状と、これから何をすべきかが明確になり、大変勉強になりました。教わった対策を一つずつ実行し、体制を整えていきたいと思います。

参加者の声

セキュリティの現状把握と今後の対策について、具体的な道筋が見えてまいりました。まずは何から着手すべきか、優先順位を含めた対策案をチーム内で共有させていただきます。様々な方と一緒に議論することが出来て大変有意義な時間を過ごすことができました。ありがとうございました。

サービス・その他　医療系コンサル業　B社

取引先要求水準への対応に向けた情報セキュリティ基盤構築の取組

企業プロフィール
従業員数：1～5名

セキュリティ体制
1名体制／兼務

事業内容
人材育成コンサルティングや教育・研修、ウェルネス関連コミュニティを組み合わせた事業を行う多面的な生活支援をしています。

背景と課題

取引先との法人契約に求められる水準への対応を進める中、対策が十分に整っておらず、事務所移転に伴うインフラ構築についても方向性が明確ではない状況でした。

取組内容

IPA(※1)の指針に沿った規程整備を計画し、データのクラウド化や移転先環境、端末の物理的な紛失対策など、ソフトとハード両面の安全対策を進めました。

結果と今後

取引先対応にIPA※1準拠の規程を進め、翌年度までに必要な資料を作成予定である。クラウド型のファイル共有・ストレージサービス導入体制でバックアップを強化し、企業協力指向で人の不足にも対応する。シェアオフィスの安全性を確認し、モバイル端末の管理ルールも整備するなど情報管理体制を継続的に強化することとしている。

背景と課題

背景

法人契約に向けた体制整備と、事務所移転に伴うセキュリティ基盤構築に向けた検討

現在は個人で医療系コンサル業務を受託していますが、今後は法人契約へ切り替え、事業を安定化させる展望を持っていました。そのため、取引先の要求水準を満たす体制整備が急務でした。また、事務所移転に伴うインフラ構築や資産管理の必要性が生じ、自身の知識のみでは適切なリスク策定や対策が不十分だと感じていました。

- 法人契約への切り替えと事業の安定化
- 取引先の要求水準を満たす体制の整備
- 事務所移転に伴うインフラと管理

課題

1. 法人契約への切り替えに際し、取引先の求めるセキュリティ水準が未把握
2. データのバックアップ対策が実施されておらず、資産管理台帳も未整備な状態
3. 事務所移転に際し、セキュアなインフラに関する知見が不足

取組内容

取組1

取引先指定の質問シートに対応する、IPA(※1)ガイドラインに準拠した情報セキュリティ規程類の整備と策定

入手した取引先指定の質問シートに対応するため、IPA※1のガイドラインを指標とした体制構築を進めています。具体的には、情報セキュリティ基本方針や関連規程、ハンドブックの作成、さらにリスク分析シートを用いた現状把握を行い、翌年度の法人取引開始に向けて、客観的な安全性を証明する各種資料の整備を計画しています。

取組2

ローカルデータの紛失リスク低減に向けた、独自クラウドサービスの早期導入とデータ管理体制の強化

ローカルPCに保存されている業務資料の紛失や破損を防ぐため、独自のクラウドサービス活用によるデータ管理を強化しました。シェアオフィスではNAS※2等の物理デバイス利用が制限され、取引先貸与PCではUSB利用が制限されるため、移転を待たず早期にクラウド保存を完了し、場所を問わず安全に業務が継続できる環境を導入しました。

取組3

シェアオフィス利用時の情報漏洩防止策と、業務用モバイル機器の物理的な紛失対策および運用ルールの構築

移転先のシェアオフィスにおける情報漏洩対策として、オンライン会議時の個室利用を徹底する運用を検討しました。また、業務用スマートフォンは通信キャリアのセキュリティオプションによる保護に加え、物理的な紛失や置き忘れを防ぐため、ストラップ装着やスマートタグの活用など、ハード面と運用面の両面から対策をしました。

※1 独立行政法人情報処理推進機構
※2 Network Attached Storage(ネットワーク接続型ストレージ：ネットワーク経由で複数端末からデータを共有・保存できる装置)

結果と今後

結果1

IPA※1ガイドライン等の資料を通じて、セキュリティに対する企業の取組を学ぶ良い機会となりました。これらの情報を参考に、取引先指定の質問シートへの対応資料を次年度の契約更新時(来年度早々)までに作成し、次年度は法人契約を締結したうえで業務を継続する予定です。

→ 継続

結果2

クラウド型のファイル共有・ストレージサービスを活用したデータバックアップを実施する予定です。データバックアップの「3-2-1ルール」を満たすよう運用を調整しました。また、情報資産管理については今後も継続的に見直しを行う方針ですが、人的リソースの不足が顕著であることから、IT・セキュリティ分野における協力会社を選定し、次年度以降の体制強化を図る予定です。

→ 継続

結果3

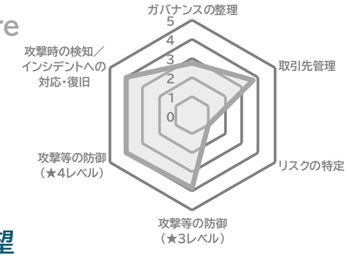
シェアオフィスを選定し、今年度中に契約予定です。事前に利用環境の調査を行い、業務上問題のないレベルであることを確認しました。また、追加的に実施可能な対策として、業務用モバイル端末の管理方法(ストラップ携帯の徹底等)について運用ルールを定めました。

→ 継続

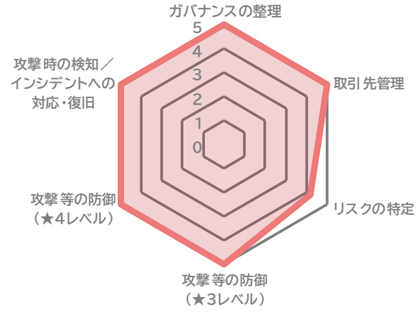
取組テーマ

ガバナンスの整理 / 取引先管理 / リスクの特定 / 攻撃等の防御 / 攻撃時の検知 / インシデントの対応・復旧

Before



After



今後の展望

現状は代表者一名のみの体制ですが、今後は人員の増加が見込まれます。これに伴い、環境や機材の状況を随時確認し、セキュリティレベルについても継続的に見直し・点検していく必要があります。
一方で、人的リソースが制約となることが想定されるため、早期に委託可能な協力会社を確保し、可能な業務から外注することで、バランスの取れた業務遂行が可能になると考えられます。

経営者の声

半年間の講義と4回の1on1(専門家派遣)を通じ、漠然とした不安が具体的な経営課題へと変わりました。ひとり会社ゆえ後回しにしていた対策も、専門家の伴走で自社に最適な形に整備でき、大変貴重な機会となりました。学んだ「自ら守る力」を糧に、今後も信頼される事業運営に邁進します。感謝申し上げます。

参加者の声

業務優先で通学が困難な中、オンデマンド学習の完備に救われました。手厚いサポートのおかげで、多忙な「おひとりさま経営」でも挫折せず完走でき感謝しています。より深く学びたいと感じるほど充実した内容でした。この学びを糧に、来期は体制を拡充し、組織的な対策へ繋げることを目指します。

サービス・その他　社会保険労務士業　C社

個人情報保護・クラウドサービス安全活用に向けたセキュリティ社内体制の整備

企業プロフィール
従業員数：1～5名

セキュリティ体制
1名体制／兼務

事業内容
労働・社会保険手続き、給与計算、組織人事コンサルティングなどを提供する専門事務所です。社労士と中小企業診断士の知見を生かし、中小企業の実務運営を総合的に支援しています。

背景と課題

過去、クラウドサービス業者のインシデントに遭遇した際に初動対応は実施できていたが、より組織的なセキュリティ対策を模索していました。

取組内容

クラウド業者の選定を含めた情報セキュリティ規程を作成しました。また、情報セキュリティ規程をベースにSRPⅡ認証(※1)を取得しました。

結果と今後

既存・新規含めたクラウドサービスの精査を実施することで、サプライチェーンリスクマネジメント力を強化しました。また、SRPⅡ認証(※1)を取得することで、組織としてのセキュリティ力強化をより実感しています。引き続き、今回確保したセキュリティ体制をベースに、さらなる業務発展を目指します。

背景と課題

背景

クラウドサービス業者のインシデントをきっかけに、セキュリティ対策の強化を検討

セキュリティ対策や考え方について、ある程度検討をしていましたが、属人化された状況にあり対策の強化を模索していました。今回、クラウドサービス業者のインシデントをトリガーに、サプライチェーンに関わるセキュリティ強化を見直す事の必要性とともに、組織的な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。

- クラウドサービス活用の品質・基準が未定義
- 個人情報保護関連の問い合わせの増加
- 組織的なセキュリティ管理体制の未整備

課題

1. クラウドセキュリティを活用するにあたり規程が未整備
2. 個人情報保護強化に向けた管理強化が必要だが、着手に遅延
3. リモート業務など、社外での働き方を実現するためのセキュリティ対策が未整備

取組内容

取組1

本事業の専門家とともに、既存のクラウド運用状況を可視化し、管理規程を作成

現行運用しているクラウドサービスの洗い出しを実施しました。また、各クラウドサービスを活用するうえでのリスク評価を行い、新規活用を踏まえたセキュリティ規程を作成しました。

取組2

個人情報取扱の組織的強化に向けた、SRPⅡ認証(※1)の取得

今回、クラウドセキュリティの運用を考慮した情報セキュリティ規程に改訂し、SRPⅡ※1認証取得に必要なセキュリティ管理策とリンクさせることで、SRPⅡ認証※1の取得を実現しました。

取組3

通信セキュリティを保護するために、RAS(※2)オプションを追加導入し、多様な働き方の実現に向けて準備

社外・在宅勤務においては、会社貸与端末を活用することで運用してきましたが、ネットワーク通信経路におけるセキュリティリスクがあることが判明しました。そこで、現行ファイアウォールのRAS※2オプションを追加契約することで、通信経路の特定とセキュリティ強化を図りました。

※1 SRPⅡ認証（社労士事務所向けの個人情報保護認証制度）
※2 Remote Access Service（社外から社内ネットワークへ安全に接続するためのリモートアクセス基盤）
※3 SCS評価制度（サプライチェーン強化に向けたセキュリティ対策評価制度）

結果と今後

結果1
取組の結果、クラウドサービスを活用することで発生するセキュリティリスクの可視化と、今後さらなる活用を含めた対策・選定基準を策定することで、組織として一定の管理下でクラウドサービスを活用できる体制が整いました。
→ 解決

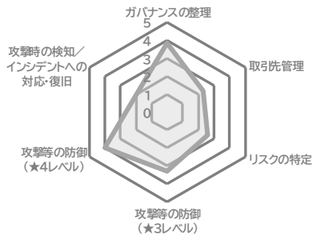
結果2
今回、本事業で作成した情報セキュリティ規程を活用し、かねてより検討していた、全国社会保険労務士会連合会創設：SRPⅡ認証※1を取得することができました。これにより、個人情報取扱事業者として、安心・安全なサービス拡充を進めていきます。
→ 解決

結果3
社内ファイアウォール配下と同様のネットワーク・セキュリティを外部からも活用できるよう、リモートアクセスサービスオプション導入を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。継続して、タブレット端末等の紛失時リスク対策や、データ保護についてのセキュリティ対策強化のために、今後も製品導入は継続検討していきます。
→ 継続

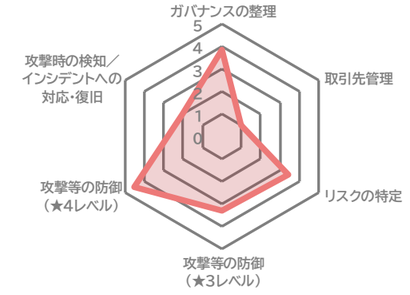
取組テーマ

ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

来年度は、規程の「作成」から「運用」へ軸足を移し、機器廃棄の手順整備や必要ソフトウェアの導入を含めた運用体制を確立します。あわせて、第三者機関による規程運用状況の定期監査を実施し、指摘事項を改善サイクルに組み込みます。さらにSCS評価制度※3の★3取得を目標に、自己評価と是正を計画的に進め、継続的にセキュリティ水準を高めます。

経営者の声

情報セキュリティの向上が関与先の安全・安心を確保する手段となり、経営成績によい影響を及ぼすと考えています。この事業を通じてセキュリティレベルが一層高まることを期待していました。認証取得など明確な成果を得られて満足しています。今後の課題も整理できたので着実に実行していく予定です。

参加者の声

10回の座学研修は負担も大きかったのですが、得られた情報は貴重なものばかりでした。さらに情報セキュリティの向上に取り組む際に、参照できる情報を得る機会になりました。専門家派遣では事前に伝えておいた要望に対して、的確かつ簡潔に対応策を示して頂き、効率的に取組を実施できました。

サービス・その他　環境・企画支援業　D社

代表取締役がハンドブック等を策定し、全従業員に拡げるセキュリティ管理体制構築に向けた取組

企業プロフィール
従業員数：1～5名

セキュリティ体制
1名体制／兼務

事業内容
定款公開情報では、環境関連の調査・分析や会議運営、企画制作、教育関連事業などを目的とする法人です。地域性のある活動も含め、多面的な事業展開を志向する事業体とみられます。

背景と課題

代表者のみであったが、会社組織の変革に伴う事業開始をきっかけに、情報セキュリティを基本から整え、ハンドブックを整備した運用を検討していました。

取組内容

情報セキュリティ基本方針を策定しホームページに公開すると共に、情報資産を明確にしリスク対応に応じたハンドブックの作成を行いました。

結果と今後

情報資産管理台帳を基に、取り扱いのある情報資産の洗い出しからリスク分析を行い、重要情報資産を明確にしました。その資産に対して管理方法等について規程すると共に、具体的なセキュリティ対策やルールを明記したハンドブックの作成を行いました。

背景と課題

背景

代表者がハンドブックの整備等を行い、従業員へ周知し意識の醸成を図るのが課題

サイバー攻撃の増加を踏まえ、情報資産管理台帳を整備し、リスク分析で重要情報と管理方法を明確化し、体制とマニュアルを整えてきました。一方で周知と定着が課題のため、説明会や定期教育で全社の意識を根付かせ、年間を通じて点検・改善まで回る継続的な運用サイクルを早急に確立する必要がありました。

- 代表者のセキュリティ知識等が不足
- ハンドブックの整備と周知
- 実効性のある運用

課題

1. セキュリティ知識やハンドブック等の整備に関わる知識が不足
2. ファイルサーバとして利用している、複数あるクラウドストレージの用途が未定
3. 従業員のセキュリティ対策の遵守による実効性のある運用

取組内容

取組1　情報資産管理台帳を整備し重要資産を明確にして、対応ルールを決めハンドブックを整備

情報資産管理台帳で情報資産を洗い出し、資産ごとにリスク分析を行って重要資産を明確化しました。さらに重要資産についてインシデント対応シートを基に対応方法を整理し、具体的な対策ルールを定めた情報セキュリティハンドブックを作成しました。

取組2　複数あるクラウドストレージの用途の明確化

クラウド業務環境で提供される法人向けオンラインストレージをファイルサーバとして利用する一方、同種の無償オンラインストレージも併用しており用途が不明確でした。そこで利用目的を整理し、保管先の使い分けルールを策定しました。あわせてアクセス権限に基づくフォルダ構成へ再編し、適切な共有・管理ができる運用を整備しました。

取組3　従業員のセキュリティ対策の遵守による実効性のある運用の実施

作成した情報セキュリティハンドブックを従業員へ周知し、定期教育と運用状況の確認を実施しました。さらに監査やマネジメントレビューを計画に組み込み、結果を改善へ反映するPDCAサイクルが継続的に回るよう、年間計画として体系化しました。

※1 ISO/IEC 27001 に基づき、組織の情報セキュリティマネジメントシステムが適切に構築・運用されていると第三者が認証する制度

結果と今後

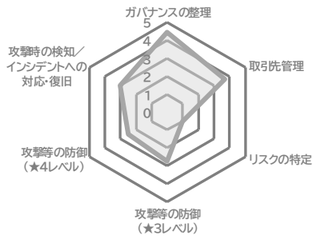
結果1　情報資産管理台帳で情報資産を洗い出し、資産ごとのリスク分析により重要情報資産を特定しました。特定した重要資産に対して、取扱い・保管・アクセス管理等の対策ルールを整理し、実務で対応できる形に落とし込んだうえで情報セキュリティハンドブックへ反映しました。今後は年間計画に基づき棚卸しと見直しを継続し、運用定着と改善を図ります。　→ 継続

結果2　インシデント対応シートを基に、クラウド業務環境で提供される法人向けオンラインストレージをファイルサーバと同種の無償オンラインストレージの用途を整理し、保管対象ファイルの区分を明確化しました。あわせて各オンラインストレージ内でアクセス権限に応じたフォルダ構成へ見直し、閲覧・編集範囲を統制できる状態を整備しました。　→ 解決

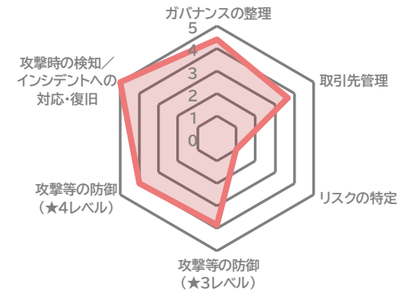
結果3　情報セキュリティハンドブックを全従業員へ周知し、運用ルールや遵守事項の理解促進を図ることができました。今後は年間計画を策定し、定期教育・内部監査・マネジメントレビューを体系的に組み込みます。あわせて点検結果の記録と是正対応の流れを明確化し、運用状況を継続的に監視・改善できる仕組みを整備して、実効性あるセキュリティ運用の定着を図ります。　→ 継続

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ **攻撃等の防御** ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

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たと感じています。今後は従業員へのセキュリティ意識の醸成を図り、また維持して、年間を通して適切に運用して行けるよう取り組んでいきます。

経営者の声

サイバーセキュリティについての全般的な知識が増え、数年前に見様見真似で作成していた情報セキュリティ基本方針や報告書の内容についての理解が深まった。ISMS認証※1取得を目指して体制を構築することで、さらにサイバーセキュリティに実際に対応していくため実践力も強化されると考えている。

参加者の声

とても良い学びになったし、他企業の状況を知ることができたことも、ありがたいことだった。仕事が忙しい時期と重なったので、しっかりと取り組むことはできていなかったが、来月以降、この研修で10回にかけて学んだ内容を思い出しつつ、テキストを再度確認しつつ、弊社内での体制づくりを進める予定でいる。どうもありがとうございました。

サービス・その他　水産資材開発業　E社

IPA(※1)ひな形を活用した規程整備と情報資産管理強化の取組

企業プロフィール
従業員数：1～5名

セキュリティ体制
複数名体制／兼務

事業内容
魚礁や増殖礁、多目的礁の開発・設計・製作指導などを行う企業です。魚の生活環境の整備を目的とした製品開発に取り組み、水産資源や沿岸環境の保全・活用に貢献しています。

背景と課題

ベンダーから提案いただきセキュリティ関連機器を導入してきたが、対策として十分なのか心配でした。機器導入の他に実施すべき取組を再確認したかった。

取組内容

IPA(※1)の情報セキュリティ関連規程（サンプル）をベースに関連規程の再整備や情報資産管理台帳の作成を進めました。進める過程で、不明点について確認しました。

結果と今後

情報セキュリティ関連規程や情報資産管理台帳を作成しました。作成する中で気になった点、例えば今まで導入した機器や加入したサイバーセキュリティ保険の内容について、問題ないことを確認しました。今後は、クラウドの利用を促進しつつ、セキュリティ環境を見直していく予定です。

背景と課題

背景

社員数2名の会社で目指すべきセキュリティ水準とはどの程度なのか

社員数2名の企業ですが、重要なデータを扱っているので、ベンダーに相談し提案されたセキュリティ機器を導入してきました。この対応で十分といえるのか、他に不足しているものがあれば対策することで、より万全なセキュリティ環境にしたいと思っていました。また、アプリケーションのクラウド化も検討したいと考えています。

- セキュリティ機器の過不足
- 情報セキュリティ関連規程が未完成
- クラウド化に関する検討

課題

1. 情報セキュリティ関連規程が未完成
2. 情報資産管理台帳の作成が未着手
3. クラウド化の進め方とその後のセキュリティ環境見直しが不明

取組内容

取組1　情報セキュリティ関連規程（サンプル）をベースに情報セキュリティ規程を作成

IPA※1の提供する情報セキュリティ関連規程（サンプル）をベースにして、情報セキュリティ関連規程を再作成することにしました。以前作ったものは古いバージョンだったので、最新のバージョンを使用して全面的に見直しました。

取組2　情報資産管理台帳を作成し、社内に点在している重要情報を整理・評価して管理強化

IPA※1の提供する「リスク分析シート」を利用して、情報資産管理台帳を作成しました。情報資産の洗い出しと分類を行い、重要情報の区分を明確化しました。

取組3　クラウドサービスの情報セキュリティ要件の明確化とセキュリティ関連機器の見直し

情報セキュリティ関連規程を再作成する中で、クラウドサービスの情報セキュリティ要件を明確化しました。クラウド化が進展した後は、社内サーバも不要となる見込みなので、その際のセキュリティ機器の見直しについて検討しました。

※1　独立行政法人情報処理推進機構
※2　Business Continuity Plan（事業継続計画：災害・事故・障害発生時でも重要業務を継続または早期復旧するための計画）

結果と今後

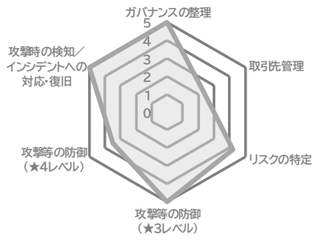
結果1　情報セキュリティ関連規程を完成させることができましたので、社内に周知しました。今後は、役割に応じた教育・研修を実施し、理解度を高める必要があると考えています。また、規程に基づく運用手順書の整備や、インシデント対応フローの明確化、アクセス権限やログ管理などの点検も検討していきたいと思います。　→ 継続

結果2　保有する情報資産を正確に把握し、重要度やリスクに応じた適切な管理を行うため情報資産管理台帳を整備しました。インシデント発生時には影響範囲を迅速に特定でき、対応の効率化や復旧時間の短縮にも寄与するものと考えています。　→ 継続

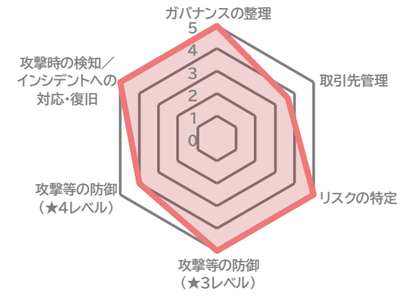
結果3　明確化したクラウドサービスの情報セキュリティ要件を使って評価し、適切なクラウドサービスの導入を進めていきたいと思います。クラウド化が進めば、社内サーバも不要となる見込みですので、クラウド運用時に「残すべき」機器と要素について検討していきたいと思います。　→ 継続

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

今後は、策定した情報セキュリティ関連規程および情報資産管理台帳を基盤として、実運用の高度化を進めていきます。次年度の取組として、インシデント発生時においても事業を継続できるよう、IT-BCP※2の整備を進め、役割分担や対応手順の明確化、定期的な見直しを行います。また、明確化したセキュリティ要件を踏まえ、業務アプリケーションのクラウド化を段階的に推進し、可用性や保守性の向上を図りながら、対策の最適化を継続的に検討していきます。

経営者の声

情報セキュリティの重要さは解っており、セキュリティ関連機器の導入を進めて参りましたが、ベンダーに頼り過ぎており、どの程度まで整備を進めたら良いのか、また現状のセキュリティ関連機器で対応が可能なのか等、社内でのセキュリティ意識が低かった。そのため、セキュリティ関連知識の習得と意識の向上を期待した。

参加者の声

今回のセミナーを通して、他社と比較して、セキュリティ関連機器や用語等知識が不足していたことを痛感し、自社に持ち帰り対策を講じられた事が良かった。また、サイバーセキュリティについては、日々新しい事案が発生する事が予想されるため、これらに対応出来るようさらなる更新が必要と思った。

サービス・その他　不動産業　F社

規程整備と教育の継続で実現する実効性あるセキュリティ体制の構築

企業プロフィール
従業員数：6～20名

セキュリティ体制
複数名体制／兼務

事業内容
不動産の売買・賃貸仲介、管理など幅広く手がける地域密着型企業です。住まいや土地に関する総合支援を通じて、地域の暮らしと資産活用を支えています。

背景と課題

積極的にIT導入を進めてきましたが、クラウド利用やインシデント発生時の規程を明文化しポリシーを定める必要性や、社員教育の必要性を感じていました。

取組内容

情報資産のバックアップやアクセス制限の状況について確認し、情報セキュリティ規程の策定を行いました。また、社員教育の計画や教材選定を行いました。

結果と今後

情報セキュリティ規程の整備を通じ、未作成だった運用ルールを明文化し、現状に即した規律を定めました。また、ネットワークや端末の整備の基本対策確認、EDR(※1)やモバイル管理も検討。さらに教育コンテンツを活用し、毎月配信を行うことで、社員のセキュリティ意識向上を醸成します。

背景と課題

背景

IT導入のポリシー策定とクラウド活用を見据えたセキュリティ体制の構築が必要

リモートワークを一部導入し、今後のクラウド導入計画を持っている状況で、IT導入に統一したポリシーが不足していました。ガバナンスや資産管理を明文化すること、アクセス制御の現状について確認することに加え、クラウド利用や不測の事態への対応ルールの整備、および社員教育の計画が必要でした。

- ガバナンスや資産管理の明文化と現状把握
- 重要システムへの適切なアクセス制御の確認
- 不測の事態に備えた対応ルールの早期整備

課題

1. IT資産や体制の明文化・最新化がされておらず、現状の把握や定期的な監督が困難
2. 重要システムのパスワード設定状況が不明確、可搬媒体の持込みなどのルールが未整備
3. クラウド導入を検討中だが、情報漏洩を防ぐ指針や事案への対応体制が未策定

取組内容

取組1　実態に即した情報セキュリティ規程の策定と運用ルールの明文化

IPA(※2)のサンプルを基に、自社の実態に即した規程作りを進めました。情報セキュリティ規程を実際に実施可能にするため、実情に合った体制や機密区分を検討し規程に反映すること、重要と考えられる部分は加筆する取組を進め、特に、クラウド利用やインシデント時の対応手順について、運用方法の策定に取組んでいます。

取組2　ネットワーク構成の可視化と重要システムへのアクセス制御の確認

最新のネットワーク構成図を作成し、専門家と共に確認しました。また、社内システムについてはベンダーの協力を得つつ、承認済みPCのみが利用できること、アクセス制御が行われていることを確認しました。

取組3　社員の意識向上に向けた教育用コンテンツの選定と学習体制の構築

学習意欲のある社員が、自由に学習できる社員教育コンテンツをすでに持っており、このコンテンツ、およびIPA(※2)の動画・プレゼンテーション資料を精査し、セキュリティ教育に使える教材をリストアップしました。また、セキュリティ教材は、社員の自発性に任せるのではなく、定期的な学習を行えるよう、計画の策定を実施しました。

※1　Endpoint Detection and Response(端末上の不審な挙動を検知し、攻撃の侵入・拡散を早期に把握して対応するための仕組み)
※2　独立行政法人情報処理推進機構
※3　SCS評価制度(サプライチェーン強化に向けたセキュリティ対策評価制度)

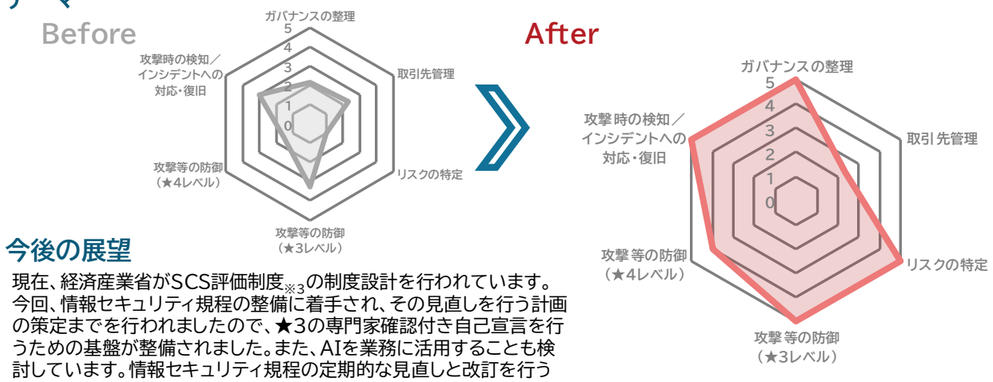
結果と今後

結果1　継続
情報セキュリティ規程を作成する中で、これまでは目を向けていなかった分野や、明文化されていなかった部分が明らかになりました。これらの部分についても経営者と担当者が一体となって議論を重ねたことにより、単にサンプルをコピーしただけで実効性のない規程ではなく、実態に即し社内で改訂が可能なレベルの規程を作成していきます。

結果2　解決
基本的なセキュリティ対策がネットワークおよびエンドポイントに適切に設定されていることを確認できました。そのうえで、追加のセキュリティやモバイル端末にも目を向け、EDR(※1)導入やモバイルデバイスの管理を検討していきます。

結果3　解決
利用している社員教育コンテンツの中には、セキュリティについてのものが複数あり、トレンドを扱ったものなど興味をひきやすいものもあり、管理者からの配信も可能であることから月1度配信される形で社員の意識向上を図っています。

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ **リスクの特定** ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧



今後の展望

現在、経済産業省がSCS評価制度(※3)の制度設計を行われています。今回、情報セキュリティ規程の整備に着手され、その見直しを行う計画の策定までを行われましたので、★3の専門家確認付き自己宣言を行うための基盤が整備されました。また、AIを業務に活用することも検討しています。情報セキュリティ規程の定期的な見直しと改訂を行うことで、AI利活用の検討を安全に進めていきます。

経営者の声

IT資産の見える化、資産管理の明文化、アクセス制御の再認識、不測の事態発生時のルールと共有、社内教育環境の契機を本事業に期待していた。満足の行く成果を得る事ができた。今後はより一層の社内体制の拡充や教育を行い、セキュリティ格付の適正なレベルを取得することに力を入れたい。

参加者の声

技術的な対策だけでなく、社員教育による意識改善の重要性を再認識いたしました。専門家派遣による支援を受け、セキュリティ体制を整備できたことは大きな前進です。今後も変化するリスクに応じた継続的な見直しと教育に取り組み、維持管理に努めていきたい。

サービス・その他　情報通信業　G社

認証取得に向けた課題解決と体制強化を進めるための規程整備・運用改善とセキュリティ意識向上の取組

企業プロフィール
従業員数：6～20名

セキュリティ体制
複数名体制／兼務

事業内容
決済代行や収納代行、システム開発、コンサルティングを手がける企業です。決済領域の業務効率化と利便性向上を支えるサービスを提供し、企業の継続的な運営改善に貢献しています。

背景と課題

セキュリティ認証取得の要求がある一方、従業員の意識不足やデータ管理・漏洩対策への不安、自己点検力の弱さが重なり、基盤強化が急務でした。

取組内容

情報セキュリティ規程を作成し一部を先行適用、PDCAで運用を試行しました。主要リスクのヒューマンエラー対策も実施し、規程整備と運用強化を進めました。

結果と今後

規程は途中まで作成し一部施行したものの、検証が十分に進まず徹底には至りませんでした。一方で、効果が出た対策と改善が必要な点が可視化され、認証取得に必要な規程運用の経験と課題整理を得ました。今後は運用しやすさを重視して改訂と教育を継続し、継続改善で着実に認証取得を目指します。

背景と課題

背景

セキュリティ認証の取得を求められている一方、社内体制が整っていない

取引先からセキュリティ認証の取得を求められ、Pマーク※1等を検討していました。しかし社内に運用経験者が不在で、自己点検の力量不足により手順が曖昧になり、正しく回らず形骸化する懸念がありました。既存規程も形式的で平時の意識が高いとは言えず、取得するなら実効性を伴う運用定着が急務でした。

- セキュリティ認証取得の要求
- 従業員のセキュリティ意識が希薄
- 業務データ管理の統制・装備に不足

課題

1. Pマーク(※1)等の認証制度取得にあたり、自己点検の実施能力に不安
2. 業務上PC持ち出しを頻繁に行うが、業務データや個人情報管理の情報漏えい対策が不十分と認識
3. 従業員にセキュリティ意識が浸透しておらず、ヒューマンエラーによる事故の不安

取組内容

取組1　認証取得を目指す土台としての情報セキュリティ規程の作成

IPA※2の情報セキュリティ関連規程ひな形を基に、自社の業務実態に沿った情報セキュリティ規程を策定しました。IPA※2のひな形は従業員が日々の業務内でやるべきことを明確にできるので、実効性を持たせやすい内容にしやすいと期待しました。

取組2　情報セキュリティ規程を実際に現場に適用し、PDCAを回す経験の蓄積

セキュリティ規程作成にあたり、IPA※2のひな形を一度に全部を作成するのではなく、社内状況を踏まえ重要と考える4章分をピックアップし先行実施することで、早期にPDCAループを回し、運用の勘所をつかめるようにしました。

取組3　ヒューマンエラー対策で技術的対策と組織的対策のそれぞれの実施経験の蓄積

ヒューマンエラー対策を通じて、技術的対策と組織的対策の両方の経験を得ていきます。現在導入を検討しているクラウドストレージを利用した紛失・消失対策および、メール送信でのダブルチェックルールなどを作ることで、実際の対策効果を得つつ導入のノウハウを習得しました。

※1　プライバシーマーク（個人情報を適切に管理・運用している事業者として認定されたものに付与される制度）
※2　独立行政法人情報処理推進機構
※3　SCS評価制度（サプライチェーン強化に向けたセキュリティ対策評価制度）

結果と今後

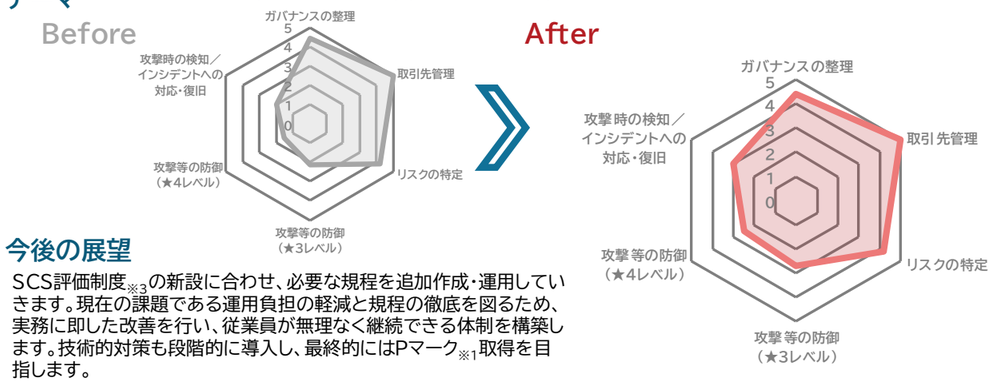
結果1
作成したセキュリティ規程の社内配布・説明会を行い、ルールを施行（Do）しました。クリアデスクが実施されているなど対策状況がよくなっている感触があります。SCS評価制度が新設されることを受け、今後はSCS評価制度※3に合わせる形で必要な規程を作成・運用していきます。
→ 継続

結果2
上記のように規程を作成・実施したものの、担当者の入院により検証（Check）までは実施できませんでした。実施状況の感触としては、一部実施されているものの徹底まではできておらず、改善（Act）の必要性を感じています。今後は徹底のやりやすさも踏まえて進めていきたいと考えています。
→ 継続

結果3
メール送信のダブルチェックルールを作り、説明会実施・運用開始をしました。実施状況の検証はできていませんが、様子を見る限りは運用負担が重く、改善の必要性を感じています。また、技術的対策は作業時間を取れず計画どまりとなったため、今後継続して続けていきます。
→ 継続

取組テーマ

ガバナンスの整理 ／ **取引先管理** ／ **リスクの特定** ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧



今後の展望

SCS評価制度※3の新設に合わせ、必要な規程を追加作成・運用していきます。現在の課題である運用負担の軽減と規程の徹底を図るため、実務に即した改善を行い、従業員が無理なく継続できる体制を構築します。技術的対策も段階的に導入し、最終的にはPマーク※1取得を目指します。

経営者の声

本事業を通じて、組織全体のセキュリティ文化の醸成と、Pマーク※1等の認証取得に向けた知識習得を期待しておりました。今後は外部機関や他社との連携・情報共有を積極的に推進するとともに、認証取得に向けて組織一丸となって取り組んでまいります。

参加者の声

講師の専門的な知識・解説から最新の脅威動向や実践的な対策を学ぶことができました。また、同じ課題意識を持つ参加者との交流を通じて視野が広がり、セキュリティへの意識がより一層高まりました。今後はこの学びと繋がりを最大限に活かし、組織全体のセキュリティ強化に積極的に貢献していきたいと思います。

サービス・その他　教育サービス業　H社

教育の仕組み化と権限統制で委託先連携・公開面まで漏えいリスクを低減し、ISMS認証(※1)取得へ段階的に準備

企業プロフィール
従業員数：6～20名

セキュリティ体制
複数名体制／兼務

事業内容
英語学習アプリなどの学習サービスを開発・運営するEdTech企業です。AIやアダプティブラーニングを活用し、個々に合った学習体験の提供を目指しています。

背景と課題

省庁・大手向け対応で対策説明と証跡が求められる一方、規程は整備済でも教育・端末管理・権限、委託先共有が定着せず、ISMS認証(※1)取得にも不安があった。

取組内容

ハンドブックと動画で教育を週次運用化し、端末統制・期限付き共有・WAF(※2)導入を実施。併せて認証取得・運用支援サービスとISMS(※3)コンサルで体制整備を開始。

結果と今後

教育は週次問いかけと年次/入社時で継続運用の枠組みを整備しました。端末・認証・期限付き共有で委託先連携の統制を強化し、WAF(※2)で公開面も防御に取り組みました。認証取得・運用支援サービスで証跡を整え月次で進捗管理を定例化し、ISMS認証(※1)取得に向け内部監査とマネジメントレビューを着実に運用していきます。

背景と課題

背景

規程の実務上での運用の確保、ISMS認証(※1)取得と取引先要件に耐える運用体制に不安

省庁・大手向けサービスを提供する上で、取引先より対策説明と運用証跡を求められる機会が多くなってきました。一方で情報セキュリティ関連規程は作成したものの、運用が徹底できておらず、端末の整備や公開サービスに対するセキュリティ対策に加えて、委託先への個人情報の共有方法にも課題を抱えていました。

- 規程は整備済だが運用フローが未定着
- 情報管理の対策が仕組・運用共に不十分
- 端末対策未整備などISMS認証(※1)取得に不安

課題

1. 教育を継続運用する仕組みがなく、社長が主催する単発の学習機会のみで提供が限定的
2. PC管理や委託先との個人情報共有、公開サービスに対するアクセス統制が不十分で漏えいの懸念
3. ISMS認証(※1)取得の進め方や必要な会議体・証跡の理解が不足し、運用負荷に不安

取組内容

取組1　誰でも参照可能な社内向けハンドブックを整備、各種動画も活用し定期的な教育を実践

教育は継続実施が効果の前提である点を共有し、規程を要点化したセキュリティハンドブックを「すぐ確認できるルール集」として導入しました。また、IPA※4や認証取得・運用支援サービスの動画も教材として活用し、週次会議での問いかけと年次/入社時教育の実施計画を策定しました。

取組2　クラウド運用と委託先連携を前提に、権限管理と公開防御を標準化し、漏えいリスクを低減する仕組みを確立

PCは会社管理端末に統一しBYOD※5を禁止しました。クラウドアカウントには多要素認証を全適用し、委託先への個人情報共有はオンライン表計算を継続しつつ、最小権限でのファイル共有と閲覧期限による自動失効を徹底する運用に統一しました。あわせて、自社Webサイトや公開サービスの保護対策として、WAF※2の導入も実施しました。

取組3　ISMS認証(※1)取得を中心に、認証取得・運用支援サービスで規程・記録と会議体・内部監査運用を整備

年度内からISMS※3コンサルを導入し、認証取得・運用支援サービスも導入して規程・記録を一元管理化しました。適用範囲、リスク評価、文書化、内部監査、マネジメントレビューまでの運用手順を確認し、月次の進捗管理と証跡の残し方を含めて取得までのロードマップを整理しました。

※1 ISO/IEC 27001 に基づき、組織の情報セキュリティマネジメントシステムが適切に構築・運用されていると第三者が認証する制度
※2 Web Application Firewall(Webアプリへの攻撃を検知・遮断するアプリ層専用の防御仕組み)
※3 情報セキュリティマネジメントシステム：組織の情報資産を守るために、リスク評価・管理策・運用・改善を体系的に管理する仕組み
※4 独立行政法人情報処理推進機構
※5 Bring Your Own Device(従業員が私物デバイスを業務利用する形態)
※6 政府情報システムにおいてクラウドサービスのセキュリティ水準を評価・登録する制度
※7 Mobile Device Management(モバイルデバイス管理：端末を一元的に管理し、設定・アプリ・セキュリティを遠隔で制御する仕組み)

結果と今後

結果1
教育の定期運用に向け、ハンドブックと動画教材を軸に「ミーティングを活用した週次問いかけ＆年次／入社時教育」の実施計画を整備し、単発依存から継続運用へ移行する土台を構築しました。今後は教育の受講率・理解度を記録する運用や、セキュリティ教材の定期見直しを行い、委託先を含む周知徹底と運用定着を図りたいと考えています。
→ 継続

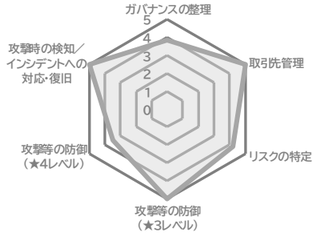
結果2
端末を会社管理に統一し、2段階認証を採用することでセキュリティ強化を図れました。また、最小権限・期限付き共有を標準化したことで、委託先のアクセスが整理され、公開サービスもWAF※2で防御できる体制が整いました。今後は権限棚卸しと期限設定の遵守確認、WAF※2ログ監視も実施することで安定運用を目指し、継続的改善を行っていきます。
→ 継続

結果3
1月よりISMS※3コンサルが開始し、複数回の伴走支援を実施中。認証取得・運用支援サービス導入で規程・記録を整備し、適用範囲・リスク評価・是正管理を運用に乗せています。まずはISMS認証※1取得に集中し月次で進捗を管理しつつ、内部監査とマネジメントレビューの実施計画を策定。取得後はISMAP※6も視野に、必要に応じてログ取得やMDM※7導入を段階的に進めます。
→ 継続

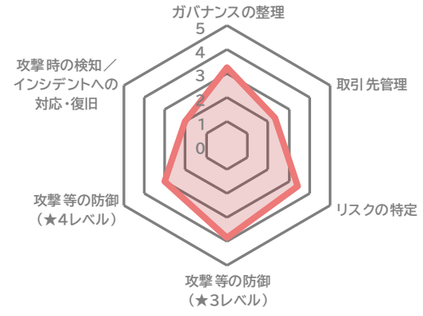
取組テーマ

ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

まずISMS認証※1を取得し、官公庁・大手企業からの信頼獲得と新規受注拡大の基盤を構築します。それに併せて、従業員教育を定期的に実施することで組織への定着を図っていきます。また、端末統制、最小権限原則に基づく期限付き共有、WAF※2監視を標準化し、ログ管理やMDM※7などの仕組みを適宜導入することも検討していきます。ISMS認証※1取得後は内部監査とマネジメントレビューを定例化し継続的改善体制を確立してまいります。

経営者の声

顧客のセキュリティ意識の高まりもあり、会社としてISMS認証※1取得を目指しております。そのステップとして、参加させて頂きました。参加した結果、非常に有意義な内容であり、おかげさまでISMS認証※1取得へ準備を進めておりますので、取得に向けて進めていきます。ありがとうございました。

参加者の声

セキュリティ知識についてはほぼ初心者の状態で参加しましたが、サイバーセキュリティの重要性や知識から会社としての体制構築まで一気通貫で教えて頂くことで、今後会社のセキュリティ対策を行う担当者として大変勉強になりました。グループワークを通じて理論だけでなく具体的な事例を考える訓練もできたと感じます。

サービス・その他　調査研究・コンサルティング業　I社

限られたリソース下で進める、情報資産管理とセキュリティ体制整備

企業プロフィール
従業員数：6～20名

セキュリティ体制
1名体制／兼務

事業内容
官公庁・自治体・民間企業向けに、環境分野・サステナビリティを中心に調査研究・コンサルテーションを行う企業です。

背景と課題

1名体制下で、リモートワークや官公庁案件等による業務形態の多様化、資産台帳の不備、PC課題があり、継続的なセキュリティ強化と体制整備を模索していました。

取組内容

MDM(※1)/EDR(※2)導入検証とポリシー強化、情報資産台帳の精緻化と分類再定義、委託契約の見直しと教育訓練の強化を進めました。

結果と今後

今回の支援を通じ、情報資産管理台帳の整理やバックアップ体制の確認など、今後継続的に取り組むべき課題を明確化しました。一方で、外部委託時のセキュリティ責任分担の明確化やMDM(※1)導入方針の整理など、一定の成果も得られており、次年度以降の計画的なセキュリティ強化につなげる基盤が整いました。

背景と課題

背景

1名体制下での対策限界と複雑化するセキュリティ強化の必要性

1名体制でありながら、リモートワークやクラウド併用、官公庁案件の受託等により、セキュリティ対策の複雑性が増していました。情報資産台帳の不備や貸与PCへの自由なソフトインストール等の課題認識から、限られたリソースの中で専門的かつ継続的なセキュリティ強化と体制整備の実現について模索していました。

- 1名体制における限界
- セキュリティ対策の複雑化
- 継続的な強化と体制整備の必要性

課題

1. 貸与PCへのソフトインストールが自由なため、シャドーIT(※3)やマルウェア感染の懸念
2. 情報資産台帳が整備途中かつ粒度に問題があり、保護すべき資産の正確な把握が未実施
3. 外部協力者への委託契約書において、セキュリティインシデント発生時の責任分担の標準化が不徹底

取組内容

取組1　MDM(※1)/EDR(※2)の本格導入に向けた検証とポリシー強化の検討

全所員分のセキュリティ統合クラウドサービスを契約し、MDM※1とEDR※2の本格導入に向けた検証を推進しました。導入後のセキュリティスコア向上を目的として、推奨ポリシーからの更なる強化策を検討し、特に利便性と安全性のバランスが必要なUSB利用制限は、実務影響を考慮しつつ、最適なセキュリティポリシーの適用を目指しました。

取組2　情報資産管理台帳の詳細精査と分類の再定義

情報資産管理台帳を作成後、運用効率と情報セキュリティの両立を目的に内容を見直しました。現状の管理区分を、運用柔軟性の向上を目的に3区分から4区分への変更を検討しました。また、ネットワーク構成図に基づき情報資産の保管場所を再確認し、クラウドを含む精緻な台帳整備と管理方法の決定を計画しています。

取組3　外部委託時のセキュリティルールの明確化と教育訓練の追加

外部協力者への業務委託契約において、セキュリティ上の役割と責任を明確化するため、最低限のセキュリティルールを盛り込んだ契約書へ見直しました。併せて、情報リテラシー向上と属人化防止を目的に、社内研修のセキュリティテストへ可用性に関する問題追加を検討しています。

※1 Mobile Device Management（モバイルデバイス管理：業務端末を一元管理し、設定・アプリ・セキュリティを遠隔で制御する仕組み）
※2 Endpoint Detection and Response（端末上の不審な挙動を検知し、攻撃の侵入・拡散を早期に把握して対応するための仕組み）
※3 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

結果1　継続

情報資産管理台帳については、全体像の把握に向けた整理に着手したものの、資産の分類や粒度にばらつきが残る状況であることを確認しました。今後は、業務実態に即した分類ルールを整理し、保護すべき情報資産が明確に可視化されるよう台帳整備を継続して進めていく必要があります。

結果2　継続

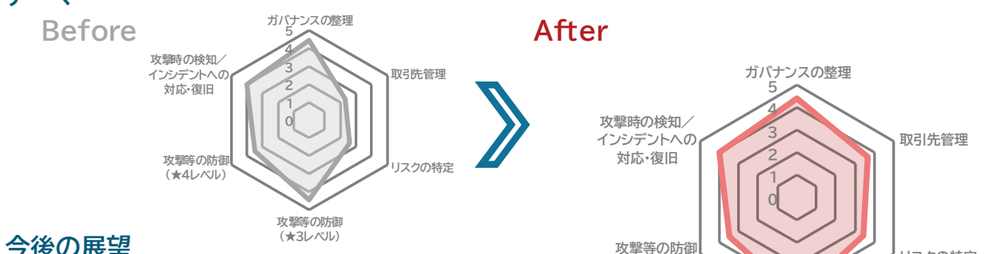
サーバーおよびクラウドサービスにおけるバックアップ状況を確認し、一定の対策が講じられていることを確認しました。一方で、障害やインシデント発生時の復旧手順や対応訓練については未実施であるため、今後は復旧体制の整理やインシデント対応訓練の実施に向けた検討を継続して行う必要があります。

結果3　解決

外部協力者への委託時におけるセキュリティ対応について、これまで明文化されていなかった責任分担を契約書上で明確化する検討を行いました。その結果、セキュリティに関する役割および責任を記載する標準的な考え方を整理し、今後の契約に反映できる状態となりました。

取組テーマ

ガバナンスの整理 / **取引先管理** / **リスクの特定** / 攻撃等の防御 / 攻撃時の検知 / インシデントの対応・復旧



今後の展望

今後は、これまで検討してきた技術的・運用的対策に加え、入退室管理等の物理的セキュリティ対策についても検討を進めていく予定です。また、情報セキュリティ管理者の役割や責任範囲を明文化し、所内で共有することで、セキュリティ対応の属人化を防ぎ、組織として継続的にセキュリティ水準を維持・向上できる体制の構築を目指します。

経営者の声

情報セキュリティ担当者が専門家や他社の担当者の方とのコミュニケーションを通じて、自信をもって対策を推進できるようになることを期待した。今後、担当者への類似の機会の継続的な提供、一般社員向けの教育の充実、取引先の要請を先回りした対策レベルの引き上げに注力したい。

参加者の声

これまで手探りで場当たり的に進めてきたセキュリティ対策を、今回フレームワークに沿って体系的に学ぶことができた。実践的なワークショップや参加者同士の交流を通じ、今後の対策の方向性と優先度を具体的に描けるようになった。専門家の助言も得られたことで今までの対策に対する評価もできた。

サービス・その他　社会保険労務士業　J社

間借りサーバの管理整理と規程整備によるリスク低減の取組

企業プロフィール
従業員数：6～20名

セキュリティ体制
複数名体制／兼務

事業内容
東京都を中心に、労務相談や手続き支援を通じて企業経営を支える社会保険労務士法人です。相談しやすさを重視し、実務に寄り添った継続支援で組織運営をサポートしています。

背景と課題

業界大手のシステムがランサムウェアの被害に遭い、弊社に被害はなかったものの大きな損失を出した同業他社もあることから、対策状況を確認したいと考えました。

取組内容

セキュリティ規程を整備する中で、グループ企業から間借りしているサーバの環境や、セキュリティの人的・組織的対策について理解を深めることができました。

結果と今後

情報セキュリティ関連規程や情報資産管理台帳を整備することができました。また、セキュリティ対策についてのセミナーに参加し職員に内容を周知したほか、IPA(※1)の動画を見ることを推奨して、社内のセキュリティ意識を高めました。今後はIT-BCP(※2)について検討していきます。

背景と課題

背景

間借りしているグループ企業のサーバ環境を理解し、セキュリティ対策を進めたい。

グループ企業から間借りしているサーバについて、どのようなセキュリティ対策をしているのか理解していませんでした。最近はサイバー攻撃が増えているので、現状のままで問題ないか危機感を感じていました。また、セキュリティの知識を持った職員がいないので、本事業に参加し知識を習得したいと思いました。

- セキュリティ規程がなくルールが不明確
- ランサムウェアで同業他社が大きな損失
- IT-BCP(※2)対策が不十分

課題

1. グループ企業のサーバーを間借りしており、運用やセキュリティ対策は任せきりの体制
2. 体系的な知識がなくセキュリティ規程などが未整備であり、ルールを明確化する必要性
3. IT-BCP(※2)について検討できていないので、インシデント発生時の対応が不明確

取組内容

取組1　セキュリティ規程を整備する中で機器の管理状況を確認・整理

導入済みのネットワーク機器やサーバの管理はグループ企業に依存しているため、管理状況を把握できていませんでした。そのため、セキュリティ規程のIT機器利用やIT基盤運用管理について整理する中で、管理状況を確認・整理しました。

取組2　自社のセキュリティ状況と必要な対策を明確化

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

取組3　BCP(※2)（事業継続計画）の検討開始

インシデントが発生した際でも重要な事業を止めず、また早期に復旧させるためBCP※2（事業継続計画）の検討を開始しました。まずは、専門家の指導のもと、セキュリティインシデント対応のミニ演習を行い、インシデント発生時のとるべき対応についてディスカッションしました。

※1　独立行政法人情報処理推進機構
※2　Business Continuity Plan（事業継続計画：災害・事故・障害発生時でも重要業務を継続または早期復旧するための計画）

結果と今後

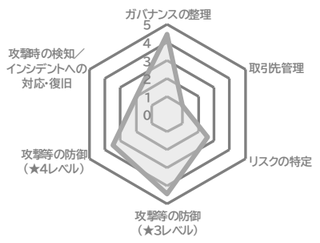
結果1　間借りしているグループ企業のサーバについて、どのようなセキュリティ対策をしているのか、設置している機器とその目的など、理解を深めることができました。今後はインシデント発生時の対応責任・連絡手順の確認、セキュリティレベルの妥当性評価など、サーバの管理責任と運用ルールを明確化し、必要な追加対策と情報共有体制を構築していきます。　→ 解決

結果2　IPA※1が公開しているサンプルをひな型として情報セキュリティ関連規程と情報資産管理台帳を本事業の専門家によるアドバイスを受けながら完成させました。この作業を進める中で、セキュリティの知識も習得することができました。作成した規程の内容については、来年度、職員向けに教育していく予定です。　→ 解決

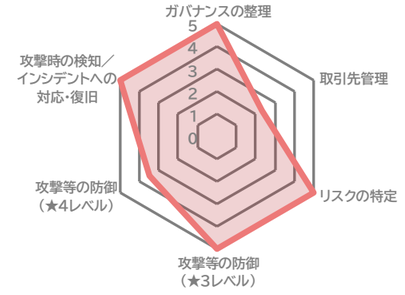
結果3　BCP※2（事業継続計画）の策定に着手し、IPA※1のサンプルをベースに情報セキュリティインシデント対応及び事業継続管理を作成しました。今後は、災害や障害が発生した場合でも給与計算や労務手続きが滞らないよう、必要な組織体制の整備やIT環境の確保、さらに緊急時の具体的な対応手順など、事業継続に不可欠な仕組みづくりを進めていく予定です。　→ 継続

取組テーマ　ガバナンスの整理 ／ 取引先管理 ／ **リスクの特定** ／ **攻撃等の防御** ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

今後は、整備した情報セキュリティ関連規程を着実に運用へと落とし込み、全社的なセキュリティ水準の底上げを図っていきます。定期的な教育や訓練、内部点検を通じて実効性を高めるとともに、リスク評価を継続的に実施し、環境変化や新たな脅威に対応できる体制を強化します。あわせて、IT-BCP※2との連動を進め、事業継続力の向上にも取り組んでいきます。

経営者の声

社会保険労務士事務所の経営においても、セキュリティ対策は切り離せない重要課題であると改めて認識しました。本事業への参加を通じ、その重要性を一層実感しております。今後は優先順位を明確にした上で適切な投資判断を行うとともに、職員への継続的な教育・研修にも積極的に取り組んでまいります。

参加者の声

専門家からのアドバイスやセミナー・ワークショップで得た知識を活用して、社内ルールの整備やセキュリティ対策の強化を進めることができました。他社担当者との意見交換でも多くの気づきが得られました。今後は、学んだ内容を社内へ共有するとともに、相談対応にも活かしていきたいと考えています。

サービス・その他　国際物流業　K社

管理規程整備と技術・人的対策で築く全社統制強化の実践

企業プロフィール
従業員数：6～20名

セキュリティ体制
1名体制／兼務

事業内容
国際複合一貫輸送や輸出入手続き代行を行う物流企業です。外航海運を活用した輸送体制を整え、国際取引に伴う物流実務を円滑に進めるための支援を提供しています。

背景と課題

情報セキュリティ対策の重要性が高まる中、社内規程が未整備で運用基準が不明確な状態にあり、体系的な規程整備と全社的セキュリティ対応が必要でした。

取組内容

IPA(※1)の中小企業向け情報セキュリティ対策ガイドラインを基に、管理規程案を作成し、各章ごとに内容の確認と実情も踏まえ運用を重視した修正指導を実施しました。

結果と今後

情報セキュリティ対策ガイドラインをベースに管理規程の内容整理と変更箇所の確認を行うことで、管理規程への理解が深まり、社内で共有可能な情報セキュリティ管理の基礎を整備されました。今後は、全章の最終的なレビューを行い、正式運用と定着を図る予定です。また従業員への周知教育を進め、継続的な見直し体制の構築を目指します。

背景と課題

背景

情報セキュリティ規程未整備による管理体制の脆弱化と事業継続リスクの顕在化への懸念

サイバー攻撃や情報漏えいのリスクが高まる中、情報セキュリティに関する社内規程や運用ルールが十分に整備されていなかった状況でした。このため、組織全体で統一した管理ができず、事故発生時の対応や事業継続への影響が懸念されている状況でした。経営リスクとして早急な対策が求められていました。

- 情報セキュリティ規程が未整備
- サイバー攻撃リスクの増大と脅威
- 組織的な管理体制の未整備

課題

1. 規程未整備により判断基準が統一されておらず、現場対応のばらつきや正確性に問題があり、サイバー攻撃時の影響拡大が懸念
2. 攻撃手法の高度化に対し、技術的・組織的・人的対策が追いつかず、被害発生時の影響拡大への懸念
3. 明確化されていない運用により全社横断の把握ができず、継続的改善や教育展開が進まず、全社の管理体制が不十分

取組内容

取組1
全社を統合した情報セキュリティ管理規程整備と運用基準の明確化による、統制強化と攻撃時の対応の正確性の向上

情報セキュリティ管理規程を新設し、判断基準と平時・緊急時の対応手順を文書化して、サイバー攻撃時の対応を正確かつ一貫した対応を可能としました。加えて役割分担と責任所在を明確にし、事故発生時も迅速に判断・対処できる管理体制を構築し、教育・訓練で水準向上を継続する仕組みを確立しました。

取組2
脅威動向を踏まえた実効性ある技術的対策と人的対策の両立による サイバー攻撃対応力の向上施策推進

最新のサイバー攻撃動向を踏まえ、必要な技術的対策を整理するとともに、作成した管理規程の周知を行い、人と組織の役割を明確化しました。従業員向けの教育や訓練を実施し、技術と人・組織の面から対策を講じることで、攻撃への対応力を高め、被害の未然防止と影響最小化を図りました。

取組3
属人化を排除した全社横断型の情報セキュリティ管理体制構築と継続的改善を目的とする推進施策

管理責任者を軸に全社横断の運用体制を整備し、リスク共有と情報連携を強化して組織全体の水準を向上させました。規程の定期見直しと継続的な教育訓練を実施し、脅威や技術変化に対応する運用を確立しました。これらの取組を通じて、長期的かつ安定したセキュリティガバナンスの確立を目指します。

※1　独立行政法人情報処理推進機構

結果と今後

結果1
情報セキュリティ管理規程を体系的に整備したことで、担当者や部署ごとに異なっていた判断や対応が統一され、一貫した運用の方向性が定まりました。事故発生時の手順や責任分担も明確化され、初動対応の迅速化と正確化が期待されます。今後は規程の具体化を進め、全従業員への周知と教育を徹底し、実効性の高い運用定着を図ります。

→ 継続

結果2
サイバー攻撃の脅威動向を整理し、技術面と人的面の対策を両輪で検討したことで、組織としての対応方針の基礎が定まりました。攻撃を前提とする考え方が共有され、被害を防ぐだけでなく最小化する視点も醸成されました。今後は最新事例の収集と定期的な教育・訓練により、対応力を維持向上させ、変化する脅威へ柔軟に対応できる体制を構築します。

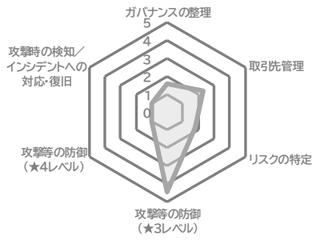
→ 継続

結果3
情報セキュリティ管理責任者を中心に全社横断の管理体制を整備し、担当者依存の属人化運用を解消したことで、組織としての管理・統制が可能になりました。状況把握や課題抽出、改善検討を定常的に行える基盤も整いました。今後は定期点検と評価で運用を可視化し、教育・啓発を継続して全社的な取組として定着させ、変化する脅威にも備えます。

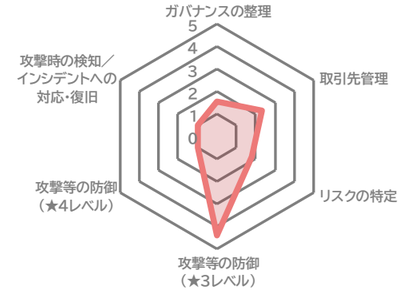
→ 継続

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ **リスクの特定** ／ **攻撃等の防御** ／ 攻撃時の検知 ／ **インシデントの対応・復旧**

Before



After



今後の展望

本取組により情報セキュリティ管理の基本的枠組みは整備されましたが、目的は規程や体制を作ることではなく、継続的に機能させることにあります。今後は規程に基づく運用を社内に周知し、状況を定期的に点検・評価し、社会情勢や攻撃手法の変化、法令改正等を踏まえた見直しを継続します。さらに教育・訓練で意識向上を図り、自律的に行動できる人材育成を進め、経営課題として実効性ある管理体制へ発展させます。

経営者の声

今やセキュリティ対策は、現金や大事な書類を保管する金庫と同等かそれ以上に必要不可欠な投資であると考えます。開業間もないこのタイミングで手取り足取り教えていただいたこと、とても有難かったです。改めまして感謝申し上げます。

参加者の声

本事業のセミナーでセキュリティ対策の基本を習得しました。講師の説明も分かりやすく、他社の前向きな取り組みや意見交換から多くを学びました。専門家の助言で自社規程も作成でき、大きく前進しました。今後も対策強化に努めます。

サービス・その他　BPO・翻訳支援業　L社

資産管理表整備・標準ルール策定・インシデント対応フロー確立による体制強化

企業プロフィール
従業員数：6～20名

セキュリティ体制
複数名体制／兼務

事業内容
海外IT企業向けに翻訳、ローカライズ、マーケティングBPO、教育・トレーニングを提供する企業です。製品理解を基にした一体型支援で、営業と顧客対応の質向上を支えています。

背景と課題

資産管理やインシデント対応方法などの運用ルールが十分ではなく、データの重要度を可視化・分類し、リスクに応じた標準ルールと対応フローの確立が必要でした。

取組内容

データ資産の棚卸しと重要度評価を実施し、リスク検討を行いました。また、対策の優先順位を明確化し、継続的な改善が可能な体制の構築を支援しました。

結果と今後

リスクの定量化により対策の優先順位が明確になり、社内の意識向上という成果を得ました。今後は策定したルールを社内ポータル等で仕組み化し、運用の定着を実施していきます。さらにSCS評価制度(※1)★3獲得などを見据え、組織的なガバナンス強化を推進します。

背景と課題

背景

全社データ資産の可視化と重要度分類に基づく、組織的セキュリティ管理体制の構築

取引先や社員のクラウド利用が広がる一方で、セキュリティの具体的な運用ルールやテレワーク時の対策が十分ではありませんでした。また、インシデント時の対応手順や、重要情報の管理やアカウント情報が特定の人に依存しているため、全社的なセキュリティ体制の早急な見直しが急務となっていました。

- データ資産の棚卸しと重要度の明確化
- 個人に依存しない標準的なルールの策定
- 有事の迅速な対応を可能にする体制構築

課題

1. データの所在や重要度に応じた資産管理表が未整備のため、対策の優先順位が不明確
2. データの運用手順が十分に社内に浸透しておらず、標準ルールとして未定着
3. インシデント発生時の報告・対処フローが不明確

取組内容

取組1　データ資産の重要度分類と優先順位を明確にした資産管理表の整備

社内にあるデータの所在を網羅的に調査し、その機密性や重要度を格付けした「資産管理表」を作成しました。データの価値に応じた適切なセキュリティ強度の設定と、対策を講じるべき優先順位を決定しました。これにより、限られたコストやリソースを最もリスクの高い箇所へ重点的に投入できる環境が整いました。

取組2　標準ルールの策定と社内浸透の推進

データの取扱い、社外との情報共有、テレワーク環境での注意事項など、個人に任せていた手順を全社共通の標準ルールとして明文化することを検討しました。作成したルールを現場の業務フローに即した形で定着させるため、セキュリティ意識を高めるために朝会での周知等を実施しました。

取組3　有事の被害を最小化するインシデント報告・対処フローの定義

万が一のインシデント発生時に備え、発見から報告、緊急措置、復旧に至るまでの役割分担と連絡体制を明確に定義することを検討しました。また、すでに使用しているクラウドストレージの接続制限や2要素認証を導入することでセキュリティ強化を図りました。

※1　SCS評価制度（サプライチェーン強化に向けたセキュリティ対策評価制度）

結果と今後

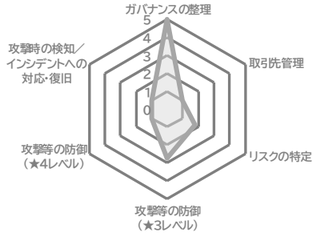
結果1　個人情報を扱う機器やファイルの棚卸しとリスクの定量化を完了し、優先的に対策すべき対象が明確になりました。今後は特定したリスク値に基づき、具体的な防護策を順次実行します。また、資産管理表を定期的に更新する運用を定着させ、常に最新のリスクを把握できる体制を維持します。　→　継続

結果2　全社会議等を通じて意識向上を図り、不要情報の削除や共有化の周知を開始しました。今後は、これらを「個人の意識」に依存させず、標準ルールとして文書化します。これにより、組織全体で統一されたデータ管理の仕組み化を推進します。　→　継続

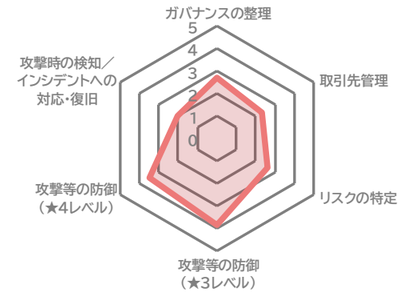
結果3　自社で起こり得るリスク事象の特定を完了し、特に「バックアップからの復旧手順」の確立が最重要課題であると定義できました。今後は特定した事象への具体的な初動対応フローをマニュアル化します。さらに机上演習を重ねることで、有事の際に迅速かつ正確に動ける組織対応力を養います。　→　継続

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ **リスクの特定** ／ **攻撃等の防御** ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

本支援で確立したリスク管理の土台を実運用へと昇華させ、組織自走型のセキュリティ体制を目指します。短期的には、社内ポータルなどを活用したルールの仕組み化とインシデント対応力の強化に注力し、全社員の行動変容を促します。その上で、中長期的にはSCS評価制度※1での★3獲得などを見据えた高度なガバナンスを構築し、対外的な信頼性を強固なものとすることで、事業の持続的成長を支える安全な経営基盤を確立する準備が整いました。

経営者の声

社員十数人の小さな会社なので、各々の性格が見えることからみんなセキュリティについての意識はあるだろうと考え、楽観的に対策を後回しにしてしまっていたと思います。今回のプログラムで学んだことを活かし、組織としてインシデントが発生しても慌てず対応できる体制を整えていこうと思います。

参加者の声

具体的な例や資料参照先を挙げてセキュリティ対策の進め方と考え方を毎回詳しく解説していただき、大変有意義なプログラムだったと思います。提供された資料を読み返しながら、社内セキュリティの強化に役立てていきたいと思います。

サービス・その他　出版業　M社

社内ネットワーク脆弱性対応と属人化解消を進めるためのマニュアル整備と教育強化

企業プロフィール
従業員数：6～20名

セキュリティ体制
1名体制／兼務

事業内容
社会科学・人文科学の学術書や大学向け教科書を刊行する専門出版社です。教育・研究を支える出版活動を通じて、知の蓄積と学びの基盤づくりに継続的に取り組んでいます。

背景と課題

社内ネットワークのセキュリティ管理・整備、ならびにセキュリティ担当者の業務属人化への対応、社内教育の具体的な題材や社員への動機づけが課題でした。

取組内容

緊急度の高いネットワーク内脆弱性への対応、初動マニュアル作成、属人化解消に向け業務マニュアル整備の洗い出し、動機づけ教育の準備等の検討を進めました。

結果と今後

社内ネットワーク脆弱性への優先対応、業務・初動対応マニュアル整備、動機づけを重視した教育準備により、技術面と運用面の両軸でセキュリティ体制を強化しました。今後は整備内容の定着と教育実施を通じ、全社的な対応力向上を図ります。

背景と課題

背景

社内ネットワークのセキュリティ強化対応と属人化解消、社員教育や動機づけの整備が必要

社内システム全般の業務をセキュリティ担当者一人で対応する必要があり業務が属人化していること、ウイルス感染等があった際に各社員が初動対応できるかの不安があること、社員全体のセキュリティ意識を上げる教育や動機づけが十分に行えていないことなどの課題があり、抜本的な整備が必要でした。

- 継続的な社内ネットワークの脆弱性対応
- 属人化業務や初動対応のマニュアル整備
- 社員教育の抜本的な整備

課題

1. 社内ネットワークの脆弱性への対処が不十分
2. 属人化業務や初動対応のマニュアル整備
3. 社員教育の整備と、教育を実施する前段階での動機づけが必要

取組内容

取組1　緊急度の高い社内ネットワークリスクへの対応

UTM※1の設置等基本的な対策は構築済みではあったものの、社内に旧OSで外部からアクセスされる可能性のあるサーバーがあることが判明、緊急度の高い課題として早急に検討、対応の方法を考慮しました。該当機器は自社と取引先両方の判断が必要でしたが様々な方法から現状で最適な対策を洗い出し、脆弱性への対処を検討しました。

取組2　属人化解消やインシデント初動対応に向けたマニュアル化

セキュリティ担当者業務の属人化解消のため、まず業務の洗い出しと必要なマニュアルの検討を開始しました。また、社員がインシデントに見舞われた際にセキュリティ担当者が報告を受けるまでの適切な初動対応が行えるかどうかに不安があり、まず特定の事象に関するマニュアルを専門家との確認を通して、作成しました。

取組3　社員のセキュリティ教育と並行したポリシー遵守の動機づけの検討

セキュリティ教育が他人事に感じないように、具体的・実践的なセキュリティ教育、自分事と捉える動機づけを専門家と検討しました。IPA※2にある動画やSECURITY ACTION※3に関連する教材、サポート詐欺への対応サイト、離席時のスクリーンロックに加え、同業種事例や担当者のご経験等、動機づけとなる資料を検討し体制を整えました。

※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 SECURITY ACTION（セキュリティアクション：中小企業が情報セキュリティ対策に取り組んでいることを自己宣言する制度）

結果と今後

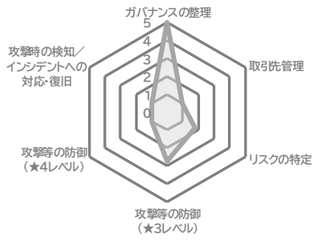
結果1　社内ネットワークリスクへの対応として旧OSサーバー等の脆弱性を特定し、関係先と調整のうえ実行可能な対策を整理・実施する準備を整えることができました。インシデント誘発リスクの低減に寄与し、優先度に基づく対応の計画を策定できたため、今後はその計画に則り継続的な脆弱性点検を進めます。　→ 継続

結果2　担当者業務の洗い出しを起点にマニュアル整備を推進し、特定事象の初動対応手順を文書化しました。専門家確認により実効性も担保され、報告前対応の不安を軽減できました。今後は社員への周知や訓練を実施し、対象範囲拡張と更新運用を進めます。　→ 継続

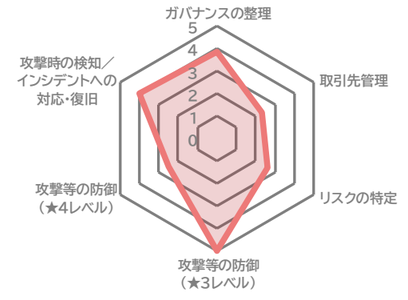
結果3　外部教材や事例を活用し、実践性と当事者意識を高める教育設計を準備しました。ポリシー遵守を自分事化する動機づけについても資料を検討し社員周知を行いました。今後はセキュリティ教育の定期化と効果検証を実施予定です。　→ 解決

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

本事業を通じ、技術対策・運用整備・教育準備を一体で見直すことができ、属人化に依存しないセキュリティ運用への基盤を構築する準備に入ることができました。社員へのセキュリティ対応への動機づけから教育による意識醸成、実践のためのインシデント訓練までの流れが整理されたことで、自社主導で改善を継続できる準備が整いました。今後は実運用と教育実施を通じ、更なる体制成熟を目指します。

経営者の声

本事業には、属人化した対応を組織として扱える体制づくりを期待して参加しました。知の継承と信頼を守る出版社の責任として体制を再定義し、初動整備も前進しました。改善を止めず、組織全体の対応力を高めていきます。

参加者の声

セミナーで理解が深まり、参加各社の皆さまと意見を交わすなかで優先課題を整理できました。伴走いただいた先生方の示唆により残された課題にも道筋が生まれ、落ち着いて改善を進められる状態へと整いました。

サービス・その他　情報通信業　N社

生成AI時代に対応するガバナンス再構築、説明責任を軸にしたログ管理と規程見直し

企業プロフィール
従業員数：21～50名

セキュリティ体制
複数名体制／兼務

事業内容
Webやアプリの開発・運用支援を中心に、インターネットサービスの企画・改善を支援する企業です。運用フェーズまで伴走し、顧客の状況に応じた実務的な技術支援を提供しています。

背景と課題

Pマーク(※1)取得済みだが、クラウド利用や生成AIなど新技術への対応不足と、有事の際の説明責任を果たすためのログ管理が明確でないことが課題でした。

取組内容

生成AI独自ガイドライン策定、ログの保存範囲と目的の明確化、システム運用ガイドの作成方針決定、規程類のISO27001(※2)参照、見直しを行いました。

結果と今後

「全て保存」から「説明責任重視」へログ管理方針を転換し運用負荷を適正化しました。また、生成AIリスクへの対応力を強化しました。さらに、規程と運用手順を分離することで、実効性の高いセキュリティ体制の基盤を確立し、SCS評価制度(※3)★3を目指す道筋がつきました。

背景と課題

背景

Pマーク(※1)取得済みだが実務面の対応に不安

Pマーク※1を取得し基本的な規程は整備されていたが、クラウドサービスや生成AIの普及に伴い、既存のルールではカバーしきれない領域が増加していました。また、ログ管理やバックアップについても、ツールは導入済みでしたが「何のために、何を保存するか」という目的や責任分界点が曖昧で、有事の対応に不安がありました。

- クラウド活用の拡大
- 生成AIの業務利用
- ログ管理の形骸化

課題

1. 生成AIの利用リスクに対し、既存規程では具体的な対策や禁止事項が不明確
2. ログやバックアップの取得目的が曖昧で、有事の際の説明責任や復旧が保証できない状態
3. セキュリティ規程に詳細手順が含まれ、実務に即した柔軟な改訂や運用が困難

取組内容

取組1　生成AI利用ガイドラインの策定とリスク対応

経産省のガイドラインを参考に、自社の業務実態に即した独自の「生成AI利用ガイドライン」を策定しました。特に、今後普及が見込まれるAIエージェントやブラウザ型AIにおける認証情報の悪用リスクについても議論し、入力禁止データや利用時の注意点を明確化しました。

取組2　説明責任を重視したログ管理とバックアップ方針の策定

ログ管理において「全て保存」から「説明責任・事業継続に必要な情報の重点管理」へ方針を転換しました。クラウド利用における事業者と利用者の責任分界点を整理しました。業務用クラウドツールの監査ログ保持期間や、バックアップの要否についても、リスクの大きさに基づきルールを再定義しました。

取組3　規程の見直しと情報システム運用ガイドの分離

既存のセキュリティ規程をISO27001※2等の視点で点検しつつ、過度なドキュメント化を回避しました。変更頻度の高い手順は規程から切り離し、新たに「情報システム運用ガイド」として策定する方針としました。これにより、規程の硬直化を防ぎ、現場が運用しやすい標準化された手順書の整備に着手できました。

※1　プライバシーマーク（個人情報を適切に管理・運用している事業者として認定されたものに付与される制度）
※2　ISO/IEC 27001（情報セキュリティマネジメントシステムの国際規格）
※3　SCS評価制度（サプライチェーン強化に向けたセキュリティ対策評価制度）

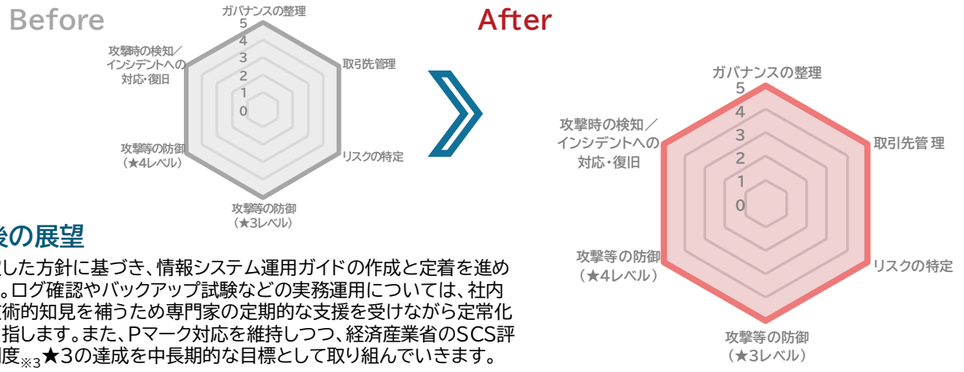
結果と今後

結果1　解決
生成AIガイドラインの整備により、従業員が安全に新技術を活用できる環境が整いました。AIエージェント等の将来的なリスクも予見したルール作りができたことで、技術革新に対する組織的な対応力が向上しました。

結果2　解決
ログ管理とバックアップの目的が「説明責任」と「事業継続」に絞られ、過剰な管理コストを削減しつつ実効性を高めることができました。クラウド利用時の責任範囲も明確になり、経営層がリスクの所在の把握が可能になりました。

結果3　継続
規程と運用ガイドを分離する方針により、実務に即した運用改善が可能となりました。ただし、実際のガイド作成やログ・バックアップの実務的な定着には技術的な知見が必要なため、次年度以降も継続的な取り組みが必要です。

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧



今後の展望

策定した方針に基づき、情報システム運用ガイドの作成と定着を進めます。ログ確認やバックアップ試験などの実務運用については、社内の技術的知見を補うため専門家の定期的な支援を受けながら定常化を目指します。また、Pマーク対応を維持しつつ、経済産業省のSCS評価制度※3★3の達成を中長期的な目標として取り組んでいきます。

経営者の声

生成AIやクラウド活用が進む中、従来の規程では不十分だと感じていました。本プログラムを通じて、説明責任を軸にログ管理方針を再整理し、実効性あるガバナンス体制へと転換できました。今後も継続的に強化していきます。

参加者の声

ログやバックアップの取得は行っていましたが、目的や優先順位が曖昧だったと気づきました。本プログラムで説明責任と事業継続の視点から整理できましたが、運用の定着には今後も継続的な取組が必要だと感じています。

サービス・その他　システム開発業　O社

認証基盤統合とEDR(※1)導入で進めるゼロトラスト(※2)移行推進と生成AI活用に向けた利用ガイドライン整備

企業プロフィール
従業員数：21～50名

セキュリティ体制
複数名体制／兼務

事業内容
システム開発を中心に、導入コンサルティングや運用・保守まで対応するIT企業です。顧客課題に応じた実装と継続支援を通じて、安定した業務システムの活用を支えています。

背景と課題

政府系の要件でクローズド環境を利用していたが、開発効率低下と最新技術への追従が困難になっていました。

取組内容

クローズド環境と一般環境の統合に向け、ディレクトリサービス(※3)の認証設計やEDR(※1)導入基準策定、生成AI活用ルール整備を行いました。

結果と今後

認証統合の方針検討とEDR(※1)等の導入準備が完了し、次年度の実装に向けた体制が整いました。
今後はゼロトラスト(※2)型への移行を推進し、業務効率と高セキュリティの両立を実現していきます。

背景と課題

背景

クローズド環境の限界と最新技術への追従が課題

政府関連など高セキュリティが求められる顧客に対し、開発環境を外部から遮断したクローズドネットワークで運用していました。しかし、開発効率の低下や最新のセキュリティ事情への追従が困難となり、安全性と効率性を両立する新環境への移行が必要でした。

- クローズド環境の限界
- ゼロトラスト(※2)への移行
- 生成AIの活用ニーズ

課題

1. クローズド環境での開発が限界を迎え、業務効率と安全性の両立が困難
2. 生成AIを業務に導入したいが、セキュリティ確保のための運用策が未整備
3. 高度な脅威への対策としてEDR(※1)が必要だが、評価基準や運用方法が未策定

取組内容

取組1　ディレクトリサービス(※3)による認証基盤の統合とセキュリティ設計

開発用クローズド環境と一般環境を同一ドメインで統合管理するため、ディレクトリサービス※3の導入設計を実施しました。最小権限の原則やパスワード管理、ログ監査等の設定指針を策定し、セキュリティレベルを維持した統合環境の構築を推進しました。

取組2　生成AI活用のためのリスク評価と利用ガイドラインの検討

最新のAI技術動向やリスク事例を調査し、品質・安全基準に基づいた利用ルールを検討しました。社内情報の安全な蓄積方法や活用事例も参考に、情報漏洩リスクを低減しつつ活用するための環境整備方針を明確化しました。

取組3　EDRおよびウェブフィルターの導入検討と評価基準の策定

エンドポイント監視強化のため、EDR※1の評価基準を明確化し製品選定に着手しました。併せて、ランサムウェア対策としてのウェブフィルター導入も検討し、具体的な製品特徴や運用方法について詳細な計画を立案しました。

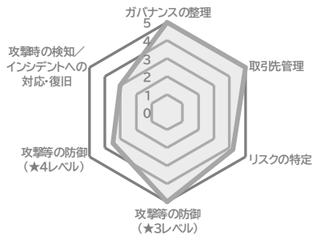
※1 Endpoint Detection and Response（端末上の不審な挙動を検知し、攻撃の侵入・拡散を早期に把握して対応するための仕組み）
※2 ゼロトラスト（Zero Trust：すべてのアクセスを「信用しない」ことを前提に、常に検証し続けるセキュリティモデル）
※3 ディレクトリサービス（ユーザー・端末・権限などの情報を一元管理し、認証とアクセス制御の基盤となる仕組み）

結果と今後

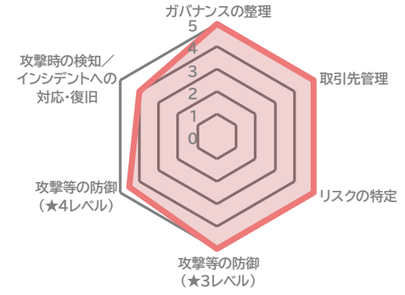
結果1	ディレクトリサービス導入についての具体的助言により認証統合の設計が完了し、クローズド環境とのセキュアな接続方針が明確化されました。次年度はサーバー構築とポリシー適用を進め、運用フェーズへの移行を目指します。	継続
結果2	生成AI活用のメリットとリスクへの理解が深まり、安全な導入に向けた社内規程の整備方針が固まりました。今後は策定したガイドラインに基づき、実際の業務への段階的な適用を推進します。	解決
結果3	EDR※1およびウェブフィルターの運用要件と評価ポイントが明確になり、導入に向けた準備が整いました。次年度は具体的なツール導入と設定・チューニングを行い、全社的な監視体制の稼働を実現します。	継続

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ **リスクの特定** ／ **攻撃等の防御** ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

今後はディレクトリサービス※3による認証基盤の統合と、EDR※1やウェブフィルターの導入を完了させ、境界防御型からゼロトラスト型への移行を目指します。また、生成AIの安全な活用により、業務効率とセキュリティ確保の両立を推進します。

経営者の声

当社の状況分析と対応の検討を的確に進めていただき、大変感謝しております。課題の「見える化」が喫緊の課題でしたが、現状を整理し端的な文言に纏めていただきました。今後の方向性が明確になりましたので、予算を確保して精力的に取り組んでまいります。ありがとうございました。

参加者の声

日常の業務に追われ、これまでは十分な取り組みができていませんでした。社内ではクローズド開発環境の限界、生成AIを業務にどう取り込んでいくかなど、セキュリティ関連の課題は山積みでした。専門家との面談を通して状況分析と現状認識が進み、「やるべきこと」が明確になりました。今後は具体的作業への落とし込みを進め、会社に予算と日程確保を依頼した上で、急ぎセキュリティアップの取り組みを進めていきます。

サービス・その他　情報通信業　P社

海外テレワークとCRM(※1)社外利用を想定したリスク洗い出しからの対策強化と教育改善による体制確立

企業プロフィール
従業員数：21～50名

セキュリティ体制
複数名体制／兼務

事業内容
ソフトウェア開発やITソリューション提供を行うテクノロジー企業です。国内外の体制を生かした開発力を強みに、企業のデジタル化や新規サービスづくりを支援しています。

背景と課題

海外を含むテレワーク拡大に伴い、想定すべきリスクの検討が十分か不安があり、教育訓練も内容の固定化が課題となっていました。

取組内容

海外テレワークや社外でのCRM(※1)利用に伴うリスクを整理し、専門家と対策を検討するとともに、教育訓練の内容を見直し実践検証を行いました。

結果と今後

海外・国内のテレワークに伴うリスクをISMS(※2)手順に基づき台帳へ反映し、PC故障や盗難、通信障害など重要項目の対処手順を整備しました。加えてCRM(※1)機能の検証や備品補填を行い、リスク低減を確認しました。さらに、フィッシング訓練で把握した課題を改善へ反映し、継続的な対策強化と運用定着を図ります。

背景と課題

背景

海外・国内テレワークのリスク検討不足と教育体制のマンネリ化が課題

ISMS※2は取得済みであるものの、テレワーク運用の安全性確保や実務への定着に不安がありました。あわせて、形骸化しつつある教育内容の見直しやIT-BCP※3の策定も重要な課題となっていました。そのため、現状のリスク評価を踏まえつつ、実効性あるルール整備や具体的な運用方法について専門的な助言を求めたいと考えていました。

- 海外テレワークの要望
- 社外からの顧客情報へのアクセス
- 内製での教育訓練能力の確保

課題

1. 外国籍の社員が多く、母国でテレワーク対応を行うこともあるが、リスク検討が十分かどうか不安
2. 営業社員による社外からCRM(※1)へのアクセスに関するリスクが未検討
3. セキュリティの訓練実施について毎年似たような内容を実施

取組内容

取組1　海外テレワークを中心にリスクの洗い出しを行い、対策案を検討・実施

専門家と連携して海外テレワークに伴うリスクをブレインストーミングにより洗い出しました。整理した結果、適切な対策により対応可能と判断し、抽出したリスクのうち優先度の高い事項について具体的な対応策を立案・実行し、管理体制の強化を図りました。

取組2　国内営業のテレワークを中心にリスクの洗い出しを行い、対策案を検討・実施

海外テレワークと同様に、社外からのCRM※1アクセスに伴うリスクをブレインストーミングで洗い出しました。あわせてSaaS※4型CRM※1の機能を精査し、社外から安全に利用可能かを確認のうえ、必要な設定や運用面の対策を整理しました。

取組3　実際の教育コンテンツおよびフィッシングメール訓練ツールを確認し、社内の成熟度に見合った教育方針を具体的に立案

専門家よりIPA※5の教育コンテンツや、フィッシング訓練向けSaaS※4およびオープンソースツールの紹介を受けました。自社環境への適用可否を検証するとともに試行利用を行い、運用上の問題点や改善点がないかを確認しました。

※1 Customer Relationship Management（顧客情報を一元管理し、営業・マーケティング・サポートを最適化するための仕組み）
※2 情報セキュリティマネジメントシステム：組織の情報資産を守るために、リスク評価・管理策・運用・改善を体系的に管理する仕組み
※3 Business Continuity Plan（事業継続計画：災害・事故・障害発生時でも重要業務を継続または早期復旧するための計画）
※4 Software as a Service（ソフトウェアをインストールせずにインターネット経由で利用する提供形態）
※5 独立行政法人情報処理推進機構

結果と今後

結果1　継続

ブレインストーミングで抽出したリスクをISMS※2手順に沿って再整理し、リスク管理台帳へ追記しました。PC故障・盗難やWi-Fi環境など高リスク項目は対処手順を作成し、テレワーク申請フローへ組み込む準備を完了しました。ドラフトは整っており、関係者へ周知し訓練も実施したうえで定期点検を行い、春節までの本格実施を確実に目指します。

結果2　解決

海外テレワークと同様にISMS※2手順に沿ってリスクを再評価し、リスク管理台帳へ追記しました。その結果、CRM※1には必要機能が備わり重大なリスクは限定的と判断できました。一方でプライバシーフィルタ等の備品不足が判明したため追加購入で対処しました。今後は運用状況を定期的に確認し、ルール周知と改善を重ね安全性を維持していきます。

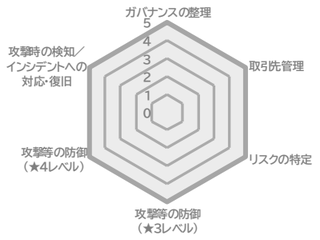
結果3　継続

フィッシング訓練を実施した結果、迷惑メール判定によりメールが届かず効果が上がりにくい課題に直面しましたが、配信設定や文面調整等の解決策を把握でき、次回から実践的に実施できる見通しです。併せて、セミナーで行った机上訓練を社内でも展開し、結果を分析して改善を重ねることで、全社の定期演習により対応力を継続強化します。

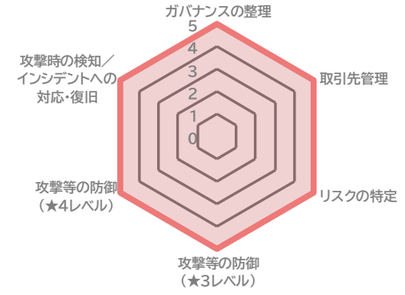
取組テーマ

ガバナンスの整理 ／ 取引先管理 ／ **リスクの特定** ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

本事業への参加により、既に整備していた社内ルールを現場手順へ落とし込み、担当者の判断基準や記録方法まで具体化して実務で迷わず運用できる状態にしました。今後はリスク管理台帳に基づき優先度を付けて低減策を継続的に実行し、効果を定期的に点検・レビューして改善します。さらにフィッシング訓練の結果を教育内容に反映し、実効性ある訓練を定期実施して組織全体の対応力を高め、着実に継続していきます。

経営者の声

柔軟な働き方を推進する上で、外部からのCRM※1アクセスにおけるリスクの可視化と対策が急務でした。今回の取組で安全性を再確認でき、ISMS※2への反映も進んだことを高く評価しています。今後はセキュリティ強化と利便性の両立をさらに追求し、変化に強い組織基盤の構築に一層注力してまいります。

参加者の声

海外テレワークやCRM※1の外部利用など、実態に即したリスクを網羅的に洗い出せたことが大きな収穫です。専門家の視点を交えたブレインストーミングや他社様との交流を通じ、SaaS※4のセキュリティ機能を改めて深く理解できました。今回整備した手順を基に、日々の業務でも高い意識を持って安全なデータ活用に努めます。

サービス・その他　人材育成支援業　Q社

会社構造変更に伴うセキュリティ・ガバナンス強化に挑戦

企業プロフィール
従業員数：21～50名

セキュリティ体制
1名体制／兼務

事業内容
グループ全体でIT・DX分野の研修や人材育成事業を展開する持株会社です。企業の技術力向上や人材育成基盤づくりを支え、変化に強い組織づくりに貢献しています。

背景と課題

国内事業・海外事業の持ち株会社設立に伴い、持ち株会社としてのセキュリティと子会社のガバナンスの強化に経営陣の理解を得ながら挑戦する必要がありました。

取組内容

当活動を通じて独自施策の再点検を行うと共に、他社事例などを使い経営陣に対しセキュリティやリソース増強への理解深化を行いました。

結果と今後

独自に進めていた親会社としてのセキュリティ強化策をセミナー・ワークショップを通じて再点検しました。また、当活動を通じて知り合った他社担当者の事例や専門家を通じて得た類似環境企業の事例を元に経営陣とのコミュニケーションを図り、セキュリティ強化への理解や、人員の強化を実現できました。

背景と課題

背景

親会社としてグループ全体のセキュリティ対策とガバナンス強化に挑戦

元々事業会社としてのセキュリティ対策は行っていました。会社組織が海外事業会社を含む持ち株会社体制に移行したことで、親会社としてのセキュリティ、および子会社に対するガバナンス強化を行う必要があり、限られたリソースの中でお客様の目から見ても十分な対策を行いたいと考えていました。

- セキュリティ対策の妥当性が判断出来ない
- 経営陣の理解・協力を得るのに苦労
- グループ社員のセキュリティ意識がバラバラ

課題

1. 独自に調査・決定したセキュリティ対策のため、形は対応出来ているが、十分か判断が困難
2. 既に子会社でセキュリティ対策を行っている中、親会社として子会社の事情を踏まえた、適切なセキュリティ支援を経営層に理解頂くための情報が不足
3. 多文化、多言語環境での事業展開のため、社員のセキュリティ意識の均一的な向上が不安

取組内容

取組1

セミナー・ワークショップを通じて既存活動の妥当性確認と最適化を実施

既にセキュリティに関する会議体の整備や情報資産管理台帳の整備、リスク対応計画の策定などは行っていましたが、セミナー・ワークショップを通じて管理資料の再整備や情報資産管理台帳を起点とした定期的な見直しフローの確認などを行いました。

取組2

他社事例を成功体験、失敗体験など実例を整理し、経営陣へ繰り返しの説明を実施

セミナー・ワークショップで知り合った他社セキュリティ担当の取り組み、および派遣された専門家から提示された類似企業でのインシデント対応事例や事前対策での成功事例を整理し、経営陣にセキュリティ確保やグループガバナンスの重要性を説明しました。

取組3

使用言語や文化の違う社員でも理解しやすい生成AIを使った教育動画の作成や階層別研修導入の検討

画一的な文章などでのセキュリティ研修だけではなく、生成AIを使って直感的に理解しやすいよう、IT人材育成企業ならではの教育コンテンツを作成したり、セキュリティインシデントが発生した際の影響度が階層ごとに異なる点に着目し、階層ごとのセキュリティ教育を検討しました。

結果と今後

結果1

今まで独自で行ってきたセキュリティ確保に向けた活動が概ね一般的な活動と差が無いことが確認出来たと同時に、他社の事例なども参考にすることで、管理に対するアプローチの幅が広がりました。また、内部管理体制の増強が発生した際に今までの対応を体系的に説明するための考え方の整理ができました。この活動を継続的に実施しようと考えています。

→ 解決

結果2

自社と同じ様な持ち株会社化している企業での取り組みや、持ち株会社としてのガバナンス事例の多い上場企業の事例を整理し、持ち株会社が対応すべきセキュリティの粒度や深度、問題点があった際の親会社への影響など経営陣の興味を引く話題を整理し、コミュニケーションを取りました。その結果、経営陣の関心度を高められ、内部統制体制の拡充も実現できました。

→ 継続

結果3

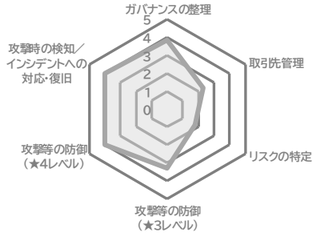
持ち株会社としての活動であり、非常に限られた人数でのセキュリティ確保となっているため、各タスクに掛けられる時間が限られていました。教育に関するコンテンツの作成にAIを使うことで効率的にコンテンツ種類が増やせ、効果測定に応じた改善にもスピーディーに対応が出来る様になりました。今後も効率的にセキュリティ確保を行う取り組みを継続しようと思います。

→ 継続

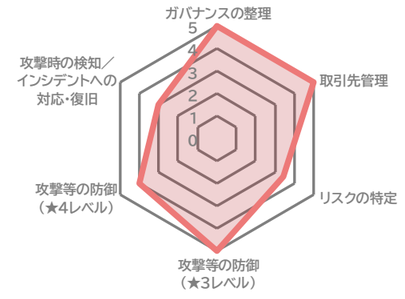
取組テーマ

ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

本事業を通じた取り組みで、自社が今まで行ってきた活動の妥当性が確認できました。また、事業を通じて知り合った他社ご担当の取り組みや知見により、従業員および経営陣へのアプローチの幅が広がりました。自社は法人向けの人材教育を行っており、個人情報保護に関しての感応度を常に高く持つことが重要と考えています。お客様に安心して仕事をお任せいただけるグループとなるようこの活動を継続・改善していきたいと考えています。

経営者の声

これまで実施してきたサイバーセキュリティ対策や投資が、経営判断として適切であったかを外部の知見を踏まえて確認したいと考えていました。本事業を通じて自社の水準を客観的に把握でき、今後の投資配分や施策の優先順位を検討するための指針を得ることができました。

参加者の声

専門家の訪問や講義、ワークショップを通じて他社の取り組みや自社の課題をより具体的に把握できました。参加企業との交流で横のつながりも生まれ、励まし合える関係ができたことで、継続して取り組む自信が高まりました。

サービス・その他　監査業 R社

委員会運営と規程整備を基盤に SCS評価制度(※1)★3認証取得を目指す全社体制構築の取組

企業プロフィール
従業員数：21～50名

セキュリティ体制
複数名体制／兼務

事業内容
監査法人として会計監査や関連専門サービスを提供する法人です。公認会計士による監査体制を基盤に、企業の信頼性向上や適正な情報開示を支える役割を担っています。

背景と課題

サイバー攻撃の急増を受けSCS評価制度(※1)★3取得の必要性を認識する一方、体制や規程の周知が不十分で、情報収集やインシデント対応も未整備でした。

取組内容

委員会設立に向けた資料整備を進め、攻撃動向の情報収集方法やインシデント対応手順を整理し、★3取得に向けた評価項目の把握と準備を行いました。

結果と今後

委員会設立に向けた骨子案を作成し、情報収集やインシデント対応の基本方針と運用の方向性を整理しました。今後は方針の文書化と社内周知を進めるとともに、★3取得計画の具体化、自己評価の実施、情報収集体制の確立、規程整備の継続を通じて、認証取得を目指します。

背景と課題

背景

サイバー攻撃急増と★3制度開始を踏まえた情報セキュリティ体制未整備と対応力不足の顕在化

情報セキュリティ委員会が未設置で、意思決定や情報収集、インシデント対応の仕組みも十分に整備されていない状況でした。近年サイバー攻撃が増加する中、組織的な管理体制の構築と対応手順・運用ルールの整備が急務となっていました。あわせて★3取得を見据えた体制強化が求められていました。

- 情報セキュリティ委員会の整備と社内体制の強化
- 情報収集と対応手順の明確化
- サプライチェーン対策評価制度への対応

課題

1. 情報セキュリティ委員会が設置されておらず、意思決定の仕組みや役割分担が曖昧で、全社的な意思決定と統制が機能不全
2. サイバー攻撃件数の急増に対し、情報の収集方法やインシデント対応方法が未整備であり、監視・予防・教育も不十分
3. サプライチェーン対策評価制度に合わせた★3取得に向けた計画の策定とセキュリティ体制の整備が必要

取組内容

取組1

情報セキュリティ委員会の体制と社内の役割やプロセスの検討と委員会設置準備書（方向性）の作成

情報セキュリティ委員会の設置に向け、会社と委員会の役割分担や業務プロセスを可視化しました。設置の目的や必要性、付与する権限、運営方法を整理し、方向性を示す設置準備書（骨子）を作成しました。あわせて設置までのマイルストーンも明確化しました。

取組2

サイバー攻撃に関する情報の収集項目と収集元、インシデント発生時の復旧方法等の対応策の検討

急増するサイバー攻撃に備え、社内情報資産の洗い出しと重要度区分を実施しました。あわせて攻撃傾向や侵入手口を把握するための情報収集項目と収集元を整理しました。さらにインシデント発生時の調査・復旧手順や顧客への報告経路も明確化しました。

取組3

サプライチェーン対策評価制度の分析と★3取得に向けたセキュリティ体制の整備、及びマイルストーンの検討

サプライチェーン対策評価制度の目的や対象、要件・評価項目を分析しました。あわせて現行の情報セキュリティ規程や業務プロセス、委託先管理ルール、情報資産管理台帳を洗い出し、★3取得に向けて求められる組織機能要件を満たす準備を進めました。

※1　SCS評価制度（サプライチェーン強化に向けたセキュリティ対策評価制度）

結果と今後

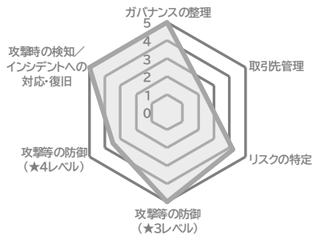
結果1
委員会の体制や役割を明確化したことで、これまで曖昧であった意思決定プロセスが整理され、全社的な統制基盤の構築に向けた準備が整いました。今後は委員会を正式に発足させ、規程整備や運用ルールの策定を着実に進めるとともに、各事務所との連携を強化し、防御水準の向上と★3取得を見据えた統制ある運用体制の確立を推進してまいります。 → 継続

結果2
急増するサイバー攻撃への備えとして、社内情報資産の分類と可視化を進め、重要度基準を策定しました。あわせて、攻撃手法や侵入経路を把握するための情報収集項目と収集元を整理し、インシデント発生時の調査手順や復旧フロー、顧客報告経路についても検討しました。今後は収集体制の本格運用と手順書整備、各事務所を含めた訓練実施により実効性の向上を図ります。 → 継続

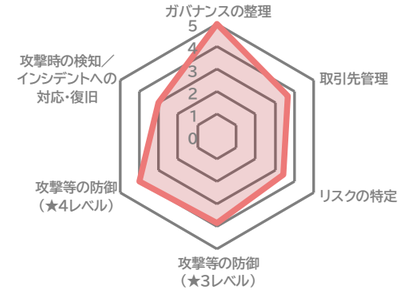
結果3
サプライチェーン対策評価制度（方針案）を分析し、★3認定に向けた組織の機能要件と今後の実施すべき項目を把握した。経済産業省による当該評価制度の設計に合わせ、マイルストーンの再設定を行い、自己評価を実施し、評価者選定や必要な改善策の具体化を進める。繁忙期を考慮した計画運用を行い★3取得を達成する体制を整えていく。 → 継続

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

情報セキュリティ委員会準備書に基づき、委員会の本格稼働と関連規程の整備を段階的に進め、全社的な統制と実効性ある運用基盤の確立を図ります。あわせて、増加・高度化するサイバーセキュリティ脅威に対応するため、情報収集体制の強化や継続的な教育を実施し、インシデント対応力の向上に努めます。さらに、経済産業省の制度に基づく★3取得を目標に自己評価と改善活動を重ね、認証達成と持続的なセキュリティ水準向上を目指します。

経営者の声

業務上秘匿性の高い情報を扱う弊法人としても、情報セキュリティへの取り組みと改善は継続的に行う必要があります。講義受講にとどまらず、ワークショップを通じたアウトプット、更に専門家派遣を通じた現在の取り組みの更なる改善に向けた質疑応答を通じ、組織的な対応への道筋が明確になりました。

参加者の声

講義、ワークショップ、専門家派遣に加え、情報セキュリティの同様な悩みを持つ仲間と共に、学び、意見交換出来る機会は多くはないため、自社実装しやすい取り組みや知見を得る事ができました。更に本講座参加者でのネットワークにも参加させて頂き、今後の情報交換も楽しみです。

サービス・その他　調査・環境支援業　S社

情報管理室設置に伴う、実効性のあるセキュリティ管理体制の構築

企業プロフィール
従業員数：51～100名

セキュリティ体制
1名体制／兼務

事業内容
シカ、クマ、サル、外来種などに関する調査や獣害対策、保護管理計画支援を行う企業です。地域課題から政策支援まで対応し、人と野生動物の共生に向けた実務を担っています。

背景と課題

ネットワークや基幹システムは整備済みだが、ファイルサーバの権限基準やリモートアクセス手順など運用ルールが未規程の状態でした。

取組内容

情報管理室の組織化を機に資産台帳を棚卸しし、リスク分析で重要情報を特定して管理方法を定義、規程・ハンドブック・体制を整備しました。

結果と今後

情報資産ごとのリスク分析で重要情報と管理要件を整理し、ファイルサーバの権限基準やリモートアクセス手順、取扱いルールを明記したハンドブックを先行作成しました。今後は本書を基に規程・体制を整え、周知教育と運用記録の整備も進め、PDCAで定期点検と改善を回し実効性を高めます。

背景と課題

背景

情報管理室がマニュアルの整備等を主導、従業員へ周知し意識の醸成を図るのが課題

サイバー攻撃や情報漏えいの懸念が高まる中、情報資産管理台帳を整備し、リスク分析で重要情報と管理方法を定め、規程・体制・ハンドブックまで整えました。一方、従業員への浸透に向けて、説明会や定期教育で意識を醸成する必要がありました。また、情報セキュリティ委員会の設置で運用監視を強化し、定期点検と改善を回す仕組みも早急な課題でした。

- 担当者のセキュリティ知識等が不足
- 規程、ハンドブックの整備と周知
- PDCAを回した実効性のある運用

課題

1. 情報管理室が組織化されたが、セキュリティ知識やハンドブック等の整備に関わる知識が不足
2. 重要情報資産として明らかになった「調査データ」である調査マニュアル、解析プログラムの漏えい対策
3. 従業員への周知と遵守状況の確認等の実効性のある運用

取組内容

取組1　情報資産管理台帳を整備し重要資産を明確にして、対応ルールを決めハンドブックを整備

情報資産管理台帳で資産を洗い出し、リスク分析により重要資産を明確化しました。重要資産ごとにインシデント対応シートを基に対応方法を検討し、規程整備に先立って具体的な対策ルールをまとめた情報セキュリティハンドブックを作成しました。

取組2　重要情報資産の「調査データ」である調査マニュアル、解析プログラムの漏えい対策方針策定

インシデント対応シートで明確化したリスクに対し、マスターフォルダを整備し、オリジナルの更新などの管理基準を策定しました。あわせて記録・ログ取得を運用化し、コピーは承認手続と保管・管理ルールを定め、同様に記録・ログで統制する体制を整えました。

取組3　従業員への周知と遵守状況の確認等の実効性のある運用の実施

作成した情報セキュリティハンドブック等の周知に向け、従業員向け説明会を開催しました。あわせて定期教育を実施する年間計画を策定し、運用状況を監視してPDCAを回す体制として情報セキュリティ委員会を設置し、継続的な改善を進めました。

※1　ISO/IEC 27001 に基づき、組織の情報セキュリティマネジメントシステムが適切に構築・運用されていると第三者が認証する制度

結果と今後

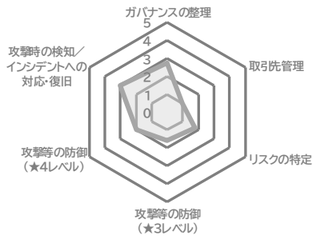
結果1　継続
情報資産管理台帳に情報資産を洗い出し、情報資産毎にリスク分析を行うことにより重要な資産が明確化でき、その情報資産に対するセキュリティ対策のルールを検討し対応することができました。またその内容を情報セキュリティハンドブックに定めることができました。今後、年間を通した運用で情報資産の見直しを行います。

結果2　継続
「調査データ」である調査マニュアル等に対して、インシデント対応シートを基に取組を行った結果、マスターフォルダを作成しオリジナルファイルがルールに則り管理でき履歴も残るようになりました。またコピーに対しても、ルールに則り管理していきます。

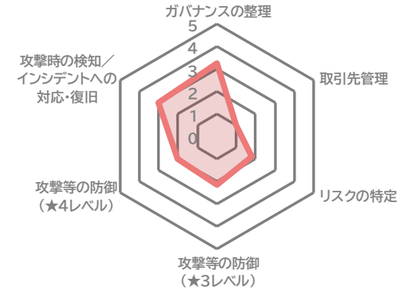
結果3　解決
情報セキュリティハンドブック等の従業員向け説明会を開催し、ルール等の理解と周知を図ることができました。また年間計画を作成し定期教育や監査等を盛り込み、情報セキュリティ委員会を設置して運用を監視する仕組みの構築を行うことができました。

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ **リスクの特定** ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

今後、ISMS認証※1の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、認証取得に向け大きく前進したと感じています。情報管理室での従業員のPCの設定やパスワード管理の運用方法等の課題は残っていますが、今後も継続して取り組んでいきます。

経営者の声

今回の取り組みで、経営者の意識は確実に醸成されつつあります。情報管理室による毎月の経営会議での議題提案、解決に向けた審議、関連情報のレクチャーなどが功を奏していると言えます。情報セキュリティ委員会の立ち上げを機に今後は、経営者・従業員が一丸となって必要な策を講じていきたいと思います。

参加者の声

今事業を通し、サイバーセキュリティ対策は全社で取り組むべきプロジェクトだと実感しました。様々なガイドラインを自社に落とし込む時、会社の現状や業務フロー、社員の意識や習慣を無視することはできません。セキュリティについて全社員が一丸となるための「場」になることがセキュリティ担当者の務めだと感じています。

サービス・その他　システム開発業　T社

属人化からの脱却：限られた人員で実現したセキュリティ体制強化

企業プロフィール
従業員数：101～300名

セキュリティ体制
複数名体制／兼務

事業内容
公共・金融・産業分野向けのシステム開発や、アプリケーションの企画・開発・製造・販売を行うIT企業です。業務に密着したシステム提供で企業活動の効率化を支援しています。

背景と課題

主管部の業務負担の増加、属人化解消に向けた社内でのセキュリティ連絡体制の整備、社員へのセキュリティ教育といった社内体制強化が課題でした。

取組内容

窓口一本化による連絡強化、短期サイクルでの社員教育、PC貸与システムの構築と社員への貸与ポリシー周知により主管部の業務負荷軽減や属人化防止に取り組みました。

結果と今後

窓口一本化やPC貸与管理の自動化、教育頻度見直しにより、情シス業務負荷の軽減と対応の平準化、社員のセキュリティ意識向上を実現しました。今後は運用定着と継続的改善により、全社的な自律運用体制の強化を図ります。

背景と課題

背景

リソース不足と属人化によるセキュリティ運用改善の必要性

基本的な運用に問題はありませんでしたが、情報システム室の稼働人数が少ないことによる対応の属人化、貸与PCの管理業務の煩雑さ等による業務負荷増が課題でした。また、社員教育が年一回のためタイムリーな教育や個人の対応力に不安があり、社内連絡体制改善や手順が明確にわかるマニュアルの作成等に課題がありました。

- リソース不足と対応の属人化
- 社内のセキュリティ連絡体制改善
- 手順の明確さと社員教育の課題

課題

1. 情報システム室の人員不足と兼務によりセキュリティ対策が属人化している
2. セキュリティに対する問合せ窓口や対応方法が各社員に明確でない
3. セキュリティ教育が年一回のみで社員の意識向上が十分でない

取組内容

取組1　リソース管理の効率化とシステム連携による人員不足解消

PC貸与ルールが徹底されておらず、PCアップデート監視が不十分で棚卸しに時間を要したため、自社内でPC貸与管理システムの作成、メールや他システム連動による自動化を実現すると同時に、社員に対する貸与ルールを明確化しました。セキュリティ担当社員の業務負担軽減によって得られたリソースを生かし属人化防止を図りました。

取組2　セキュリティ問合せ窓口の一本化やインシデント対応力の平準化

セキュリティ関連部署が二つあるため、社員からの問合せ先を明確化し、情報の蓄積を考慮し、窓口を一本化しました。社内で発生した問合せを適切に蓄積・管理・運用し、スムーズに対処する体制を整えました。また既存の初動対応マニュアルを精査し、複数社員への確認を通して、誰でも同様に対応できるようにしました。

取組3　頻度を変更した社員教育によるセキュリティ意識強化

既に取り組んでいた標的型メール訓練の結果と年1回の教育頻度に課題を感じ、全体のセキュリティ意識の底上げを図るため、教育サイクルの頻度を変更しました。社内ポリシーとの関連でIPA※1に直接連絡を取り動画やSECURITY ACTION※2に関連する対応教材を貰い、それに基づいたレッスンが実施できる運用体制を構築しました。

※1 独立行政法人情報処理推進機構
※2 SECURITY ACTION（セキュリティアクション：中小企業が情報セキュリティ対策に取り組んでいることを自己宣言する制度）
※3 Business Continuity Plan（事業継続計画：災害・事故・障害発生時でも重要業務を継続または早期復旧するための計画）

結果と今後

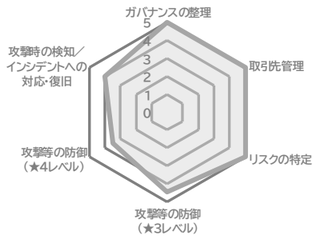
結果1　PC貸与管理の仕組み化と自動連携により、棚卸し・更新管理の工数を大幅に削減し、担当者負荷を軽減しました。創出したリソースを運用改善に充当でき、属人化防止にも寄与できたため、今後も継続的に管理部署内での水平展開し、運用精度向上を図ります。　→ 解決

結果2　セキュリティの窓口集約により報告経路が明確化し、情報集約とナレッジ蓄積を進めることができました。初動対応マニュアルも再整備され、誰でも一定水準で対応可能な体制を構築できました。　→ 解決

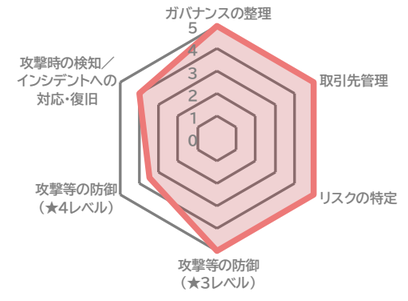
結果3　従来、年1回のセキュリティ教育に加え毎月の啓発動画公開により教育サイクルの短期化を実現すると同時に、最新脅威に即した学習機会を提供し社員意識が向上する準備が整いました。今後は社員の理解度の確認など含め継続的改善を図ります。　→ 継続

取組テーマ　ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ **攻撃等の防御** ／ **攻撃時の検知** ／ **インシデントの対応・復旧**

Before



After



今後の展望

本事業への参加により、限られた人員でも持続可能なセキュリティ運用を実現する基盤を整備できました。連絡・管理・教育の各機能が体系化されたことで、自律的に改善を回せる体制構築への準備が整いました。今後は蓄積データや運用実績を活用し、更なる高度化と全社的なセキュリティ文化の醸成を目指します。

経営者の声

参加する他の中小企業との情報交換を通じて、自社だけでは得られない「失敗事例や成功事例」を学ぶ機会を得、机上演習や実践的な演習などを通じて、「何をすべきか」を疑似体験し、インシデント発生時の対応力が向上する事を期待しました。今後は、IT-BCP※3の策定と運用に力を入れていきたいです。

参加者の声

本プログラムを通じ、セキュリティへの意識が一段と高まりました。講師の分かりやすい解説に加え、ワークショップでの他社の取り組みや生の声を聞けたことは、自社を振り返る上で非常に有益な刺激となりました。今回得た多角的な知見を、今後の実務やセキュリティ体制の強化に活かしていきたいです。

サービス・その他　採用支援業　U社

標的型メール訓練を起点に社長参画で進める 全社セキュリティ体制強化と★3取得を見据えた取組

企業プロフィール
従業員数：101～300名

セキュリティ体制
1名体制／兼務

事業内容
人材採用に特化した広告代理や採用戦略立案、求人広告運用、採用サイト制作などを行う企業です。採用活動の企画から実行まで幅広く支え、企業の人材確保を後押ししています。

背景と課題

情報セキュリティ関連規程は策定済みですが、現場の理解・遵守が徹底されず、教育・効果測定が未整備で、経営層関与が弱いという課題を抱えていました。

取組内容

標的型メール訓練を起点に、運用手順・結果共有を設計しました。教育ロードマップと会議体設立を検討し、会社として抱えるリスクを再確認しました。

結果と今後

訓練ベンダーを決定した上で目的・対象・費用・運用を整理し、1回目の訓練を実施しました。クリック率・報告率をKPI(※1)化し、今後の展開の仕方も準備しています。また、標的型メール訓練を起点に従業員教育へ展開するロードマップを作成し、セキュリティ委員会立上げも進める計画です。

背景と課題

背景

規程は整備済み。次は「人的対策」を現場に定着させ、事故を未然に防ぐ段階へ

EDR※2/UTM※3/資産管理等の技術対策は整備され、規程も策定済みである一方、営業はセキュリティへの意識が低く、ルール浸透の運用設計（周知頻度・教育計画・効果測定）と初動連絡手順の周知も不十分な状況でした。現場で例外判断が起きやすく、責任分担も曖昧で、定例の見直し場も不足していました。

- 規程周知と遵守徹底 全社定着へ
- 教育定例化と 効果測定(KPI(※1))強化
- 属人化解消と 見える化の整備

課題

1. 従業員教育（頻度・教材・効果測定）に関する仕組みの未整備と規程の現場定着不足
2. 危機感不足と経営層巻き込みの不在に起因する優先度低下とトップダウン不徹底
3. 運用が担当者1名に集中し、異動・退職時の引継ぎや BCP(※4)観点での継続運用に不安

取組内容

取組1　社長参画の全社標的型メール訓練による意識改革と対策強化の第一歩としての実践的取組

従業員の意識の低さを改善するため、標的型メール訓練を全社で実施しました。結果を社長・管理職と共有し、課題を可視化したことで、会社全体のセキュリティ対策強化に向けた共通認識を形成することができました。まずは一歩踏み出す実践的な取組としてスタートできました。

取組2　単発対策から脱却し標的型メール訓練を起点に教育を体系化する取組

標的型メール訓練を起点に外部研修サイトを組み合わせ、全社員を対象とした継続的な教育施策の検討を開始しました。単発施策に留めず、社長を含む関係者が関与する運用体制を前提に、実行可能な仕組みづくりへ一歩踏み出す取組として動きだしました。

取組3　現状対策を棚卸しし、運用手順・権限・例外運用を整理して属人化リスクと管理範囲を見える化する取組

各種セキュリティ対策は導入済みだが、設定や運用、権限管理、例外判断が特定担当に集中していたため、導入範囲と実運用を棚卸しが必要でした。対応漏れや例外運用を洗い出し、ブラックボックス化した属人化リスクを可視化し、改善に向けた第一歩として取り組みました。

※1 Key Performance Indicator（重要業績評価指標：組織や業務の目標達成度を定量的に測定するための指標）
※2 Endpoint Detection and Response（端末上の不審な挙動を検知し、攻撃の侵入・拡散を早期に把握して対応するための仕組み）
※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 Business Continuity Plan（事業継続計画：災害・事故・障害発生時でも重要業務を継続または早期復旧するための計画）
※5 SCS評価制度（サプライチェーン強化に向けたセキュリティ対策評価制度）

結果と今後

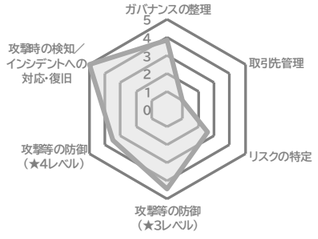
結果1　都の訓練枠に依存せず民間サービスを比較しスモールスタートした結果、全社統一の訓練運用（回数・報告書・再教育）を短期に確立し、クリック率・報告率の実測値を取得できました。今後はKPI※1推移を可視化して継続的に月次で社長・管理職へ共有し、改善施策と再訓練を反復して対象部門を拡大、全社教育へ段階展開します。 → 継続

結果2　今回実施できた標的型メール訓練と外部研修サイトを活用した「3か月3時間」学習ルールを活用し、定期周知→学習→訓練→社員教育の体系の構築を目指しています。また、現セキュリティ担当と部門長に社長を加えたセキュリティ委員会にあたる枠組みを年度内までに立上げてKPI※1確認・是正を回す仕組みの構築を行います。 → 継続

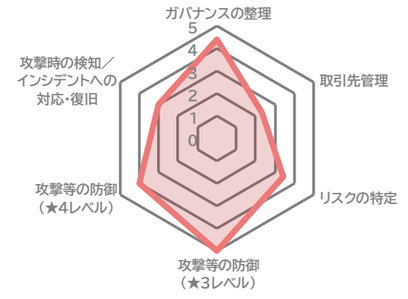
結果3　棚卸しの結果、設定値の未統一や例外運用の判断基準不足など具体的な課題を把握でき、属人化リスクを関係者間で共有することができました。今後は運用手順と権限管理を文書化し、セキュリティ委員会で定期的に確認・是正を実施するとともに、複数名で運用できる体制へ移行し、継続的な改善と安定運用を進めていきます。 → 継続

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

標的型メール訓練をきっかけに、従業員の意識課題を可視化し、教育・訓練を継続的に回す全社的な仕組みづくりを進めていきます。今後は社長が参画するセキュリティ委員会を組成し、KPI※1確認と是正を通じて運用を定着させます。併せて運用手順や権限管理の標準化を進め属人化を解消することで、体制と実効性を高め、SCS評価制度※5の★3取得につながるセキュリティ成熟度向上を段階的に実現していきます。

経営者の声

ランサムウェア攻撃による被害で経営リスク管理が問われる中、先ずは対策強化の為に担当者からセキュリティ知識の向上に期待をしました。今後はこの研修で得た知識を社内の従業員へ広め、不足分は教育することにより、社内におけるセキュリティ意識の向上も図って貰いたいと思っています。

参加者の声

普段は交流の無い他社の社内SEの方と一緒に研修やワークショップを実施でき、他社のセキュリティに関する考え方やセキュリティの重要性を肌で感じました。また、標的型メール訓練を足掛かりとして、社内のセキュリティ教育への第一歩も踏み出せたことは大きな収穫となりました。

サービス・その他　人材支援業　V社

IPO(※1)準備と事業拡大に対応するための規程整備・教育強化と情報資産管理体制構築

企業プロフィール
従業員数:101～300名

セキュリティ体制
1名体制／兼務

事業内容
アスリート・体育会学生のキャリア支援や、スポーツ人材を軸にした教育・IT・部活動支援などを展開する企業です。スポーツと社会をつなぐ独自の人材活用モデルを強みとしています。

背景と課題

IPO(※1)準備と事業急拡大で更なる対策が必要な中、メール誤送信やPC紛失が発生。ガイドライン未策定などの体制不足を解消し、強固なセキュリティ体制の確立が必要でした。

取組内容

Pマーク(※2)研修・テスト実施とファイル保管・共有サービスの権限・バックアップ検討、情報資産台帳作成を進めました。生成AIの制限付利用とガイドラインを策定しました。

結果と今後

情報資産管理台帳の整備や管理者権限ルールの明文化など、ISMS認証(※3)取得を見据えた基盤整備を進めました。一方で、台帳の精緻化や社内研修内容の改善、ファイル保管・共有サービスの可用性対策については継続的な検討が必要であり、次年度以降の計画的な取組につなげていきます。

背景と課題

背景

上場準備と事業急拡大に伴うインシデント発生と不十分なセキュリティ体制強化の必要性

上場準備を進める中で事業が急拡大した結果、従来のセキュリティ対策は現状に追い付かない状態でした。過去にはメール誤送信やPC紛失が発生し、インシデントへの体制やガイドラインの整備不足が明らかとなり、早急な対策強化が急務となっていました。IPO※1達成に必要な、専門的知見に基づく網羅的かつ強固なセキュリティ基盤の確立が最重要課題であると考えていました。

- IPO(※1)に向けたセキュリティ対策の強化
- インシデント発生と体制・ガイドライン不足
- 専門知見を要するセキュリティ基盤の確立

課題

1. 情報セキュリティガイドラインの未策定および社員向けリスク分析の未導入といった管理体制上の不備
2. 情報資産管理台帳を作成するにあたり、情報資産の洗い出しが不十分
3. 過去のPC紛失とメール誤送信の事象から従業員への教育内容の改善が急務

取組内容

取組1　Pマーク(※2)準拠の研修・テスト実施と業務に即したインシデント事例の整備に着手

Pマーク※2更新に必要なセキュリティテスト(必須)と研修(任意参加)を実施しました。研修資料は基本的な内容から普及している脅威まで含み、セキュリティの重要性を理解するのに十分な内容と確認されました。次回研修も予定し、より実際に即したインシデント対応事例を作成し、内容のカスタマイズを進める方針です。

取組2　ファイル保管・共有サービスの権限整理・バックアップ方法検討、情報資産管理台帳作成を推進

可用性が求められるファイル保管・共有サービスのアクセス権限管理を明確にし、第三者が見てわかるフォルダ階層案を検討・確認し、オンプレミスを含めた具体的なバックアップ方法も検討しました。さらに、ISMS認証※3取得を見据えた機密性・完全性・可用性を評価する情報資産管理台帳の作成を進め、内容の確認と統合を実施しました。

取組3　生成AI利用時の設定制限と注意喚起、今後の利用ガイドライン作成

生成AIサービスの利用は個別許可制とし、データの学習は「されない」設定で運用を開始しました。また、投入する情報は、社内情報を入れず一般的な内容に留めるよう注意喚起を行い、社員への社内周知も実施しました。現在のAI活用ルールはPマーク※2の範囲外ですが、今後を見据え社内の利用実態に即したガイドラインを作成しました。

※1 Initial Public Offering(新規株式公開:企業が株式を証券取引所に上場し、一般投資家に売り出すこと))
※2 プライバシーマーク(個人情報を適切に管理・運用している事業者として認定されたものに付与される制度)
※3 ISO/IEC 27001 に基づき、組織の情報セキュリティマネジメントシステムが適切に構築・運用されていると第三者が認証する制度
※4 Software as a Service(ソフトウェアをインストールせずにインターネット経由で利用する提供形態)

結果と今後

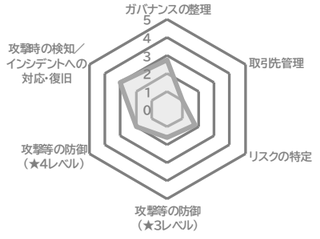
結果1　ISMS認証※3取得を見据え、個人情報管理台帳を統合した情報資産管理台帳の作成を進め、機密性・完全性・可用性の観点から重要度評価を実施しました。全体像の可視化は進んだ一方で、情報資産の洗い出しや分類粒度については今後も継続的な見直しが必要であり、台帳を運用しながら精度を高めていくことが求められます。　→ 継続

結果2　管理者権限の付与について、これまで明確な基準が存在しなかったため、業務上の必要性を踏まえた発行基準および運用ルールを整理・明文化しました。これにより、権限管理の属人化を防止するとともに、権限付与・剥奪の判断を組織的に行える体制を整備しました。　→ 解決

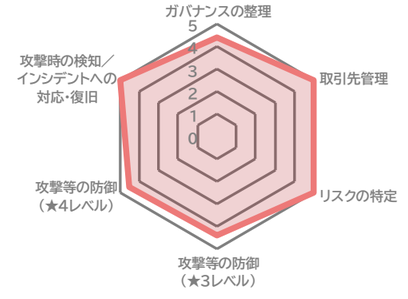
結果3　Pマーク※2準拠の研修・テストを実施し、セキュリティ意識向上に一定の効果が確認されました。また、生成AIの利用については注意喚起および基本的な利用ルールを整理し、暫定的な対応を完了しました。一方で、実際の業務形態に即したインシデント事例の反映や、研修内容の継続的な改善については今後も検討を進める必要があります。　→ 継続

取組テーマ　ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

今後は、ファイル保管・共有サービスのオンプレミスバックアップを含めた可用性確保策を検討し、業務停止リスクの低減を図ります。また、社員が個別に利用しているSaaS※4やアプリケーションの把握を進め、社内規程の整備を検討します。さらに、社員PCへのEDR導入についても検討を行い、将来的には他部署へのISMS拡充を視野に入れ、組織全体のセキュリティ水準向上を目指します。

経営者の声

弊社は社内に技術者はいるものの、上場時に求められる情報セキュリティの水準がわかる人間がいない状況。こちらの事業を通じてこれらの知見を持った人材が育ってくれればと思い、今回の研修に参加。今後は今進めているISMSの取得・維持やJ-sox対応等で今回の学びを活かしていただければと考えている。

参加者の声

社内のセキュリティ管理体制を強化すべく、担当者として研修に参加しました。受講前は漠然としていた対策知識が、実務に即した具体的な対応策として定着し、大きな成長を実感しています。今後はこの知見を社内に還元しつつ、継続的な学習を通じて組織の安全に貢献していけるよう日々努めます。

サービス・その他　飲食業　W社

属人化・シャドーIT(※1)課題を解消した情報セキュリティ改革

企業プロフィール
従業員数：301名以上

セキュリティ体制
1名体制／専任

事業内容
飲食店経営を中心に、クラフトビールの醸造やEC販売も展開する企業です。多様な飲食ブランドを運営し、食の楽しさと日常性を両立させた店舗づくりで顧客価値の向上を図っています。

背景と課題

会社拡大の体制強化のため、資産管理、アカウント管理、手順の整備、社内連絡体制の強化が必要でした。

取組内容

マニュアル作成、アカウント統制を整備してシャドーIT(※1)を抑止しました。社内ポータル作成や各PCへのブックマークによる連絡周知体制の確立に取り組みました。

結果と今後

窓口やサービスの統制強化、業務のコミュニケーション／文書共有をクラウド統合基盤のアカウント整備、情報システム部と運用ユーザ間の信頼構築により、シャドーIT(※1)抑制と連絡周知体制の基盤整備、属人化リスクの低減を実現しました。今後は運用定着と管理ルールの継続的改善により、全社的なセキュリティ統制の更なる強化を図ります。

背景と課題

背景

会社拡大に伴う資産管理やアカウント管理、社内連絡体制の強化を検討

会社拡大の一環として、セキュリティ体制を抜本的に強化する必要があり、特に、情報システム部内での属人化を防ぐマニュアル作成や資産管理、各社員が使用しているサービスの統制、セキュリティ連絡周知体制の強化が課題となっていました。

- シャドーIT(※1)への対応
- 属人化を防ぐマニュアル強化
- セキュリティ連絡周知体制強化

課題

1. シャドーIT(※1)への対応や社員が使用しているサービスの整備が不十分
2. 情報システム部の属人化を防ぐマニュアルの整備が不足
3. 全社員へのセキュリティ連絡周知体制の明確化が必要

取組内容

取組1　クラウド業務基盤のアカウント整備によるシャドーIT(※1)防止とサービス提供

各社員が自由にサービスを利用していた結果、個人／会社アカウントの混在やシャドーIT※1が課題でした。そこで統制ポリシー整備の第一歩として、業務のコミュニケーション／文書共有をクラウド統合基盤へ集約し、情報漏洩リスクの高いサービスや個人アカウント利用の制限に着手しました。

取組2　セキュリティ担当としてのマニュアルや管理図書の整備

情報システム部が少人数制で、マニュアルが未整備のままだと突発的な問題が発生した場合対応できない可能性があり、部分的にでもマニュアル化しておく必要がありました。現状のネットワーク機器論理構成図が適切か、また管理図書の過不足について確認を行い、特定の部署に資産の洗い出しを依頼するアクションを実施できました。

取組3　社内ポータルサイトサービスを利用した連絡周知体制の構築

各店舗を含めた全社に迅速に連絡周知体制を提供する必要があったため、クラウドサービスを活用した社内ポータル機能を提供しました。各店舗PCのブックマークに登録し、報告手段の乱立を防いでサービス一本化の土台を作れました。セキュリティ担当者は各店舗に足を運びヒアリングする等実践的なセキュリティ体制強化も行えました。

※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

結果と今後

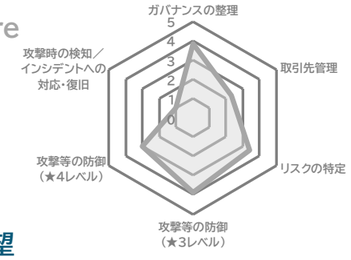
結果1　業務のコミュニケーション／文書共有をクラウド統合基盤にサービス統合したことで管理側ユーザ側共に企業用アカウントを利用し情報を一元管理できるようになりました。シャドーIT※1対策については、社内の情報資産を守りつつ社員の利便性を実現する形で段階的な調整を今後も行い、情報漏えいへの対策や取引先やお客様から信頼される情報セキュリティ体制を構築していきたいと思います。　→ 継続

結果2　ネットワーク機器論理構成図や管理図書の現状整理を行い、資産洗い出しに向けた具体的なアクションを開始したことで、属人化リスク低減に向けた基盤構築を進めました。今後はこれを基にした実際の整備の推進、洗い出し結果を反映した管理図書の充実や運用手順の標準化を継続していきたいと思います。　→ 継続

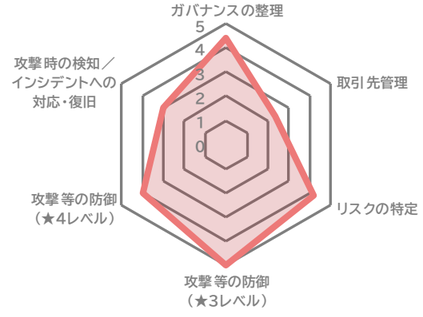
結果3　クラウドサービスを活用した社内ポータルの提供と各拠点PCへの導線整備により、全社への連絡周知基盤を構築しました。これにより情報共有の窓口が一本化され、迅速かつ確実な周知が可能な体制が整いました。今後は本基盤を活用した安定運用により、全社的な情報伝達の効率化を維持していきます。　→ 解決

取組テーマ　ガバナンスの整理 ／ 取引先管理 ／ **リスクの特定** ／ **攻撃等の防御** ／ 攻撃時の検知 ／ **インシデントの対応・復旧**

Before



After



今後の展望

本事業への参加により、アカウント統制、管理図書整備、連絡周知基盤の各機能が段階的に整備され、拡大フェーズに対応可能なセキュリティ運用の土台が構築されました。今後は運用定着と管理ルールの継続的改善を進めるとともに、資産管理の精度向上や教育施策と連動させ、自律的に改善が回る全社的なセキュリティ体制の高度化を目指します。

経営者の声

全社的にサイバーセキュリティへの取り組みが遅れているため、本事業に参加することで自社の規模や状況に合わせた対策を期待していました。今回、客観的な立場からのご意見や評価をいただいたことで、現状の把握ができました。経営課題の一つとして、今後もセキュリティ対策を推進します。

参加者の声

本事業の講義ではセキュリティ対策について体系的に学ぶことができ、ワークショップや専門家派遣では社外のセキュリティ担当者や専門家の方々と交流することで、自社の課題や自身に不足している知識が明確になり大変勉強になりました。今後も継続してセキュリティ対策に取り組んで参ります。

サービス・その他　国際物流業　X社

人的リソース不足で停滞していたセキュリティ対策を進めるため、組織的対応を強化

企業プロフィール
従業員数：301名以上

セキュリティ体制
複数名体制／兼務

事業内容
国際複合一貫輸送、輸出入、ロジスティクス、航空輸送、危険物輸送などを手がける総合物流企業です。国内外をつなぐ輸送と物流情報システムで、企業のサプライチェーンを支えています。

背景と課題

情報セキュリティインシデントが発生した時の影響について社内認識が不足しているので、本事業で得た知識を活かして全社で理解を深め、強化したいと考えました。

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、来季に向けて組織的対応を協議して、全社一体のセキュリティ意識・知識・体制の強化に取り組みました。

結果と今後

情報セキュリティ関連規程、情報資産管理台帳やデータのバックアップ手順について整備を進めています。
今後は、本事業を通して得た知識をもとに、必要な予算を確保しMDR(※1)など新たなセキュリティ対策ツールの導入やサイバーセキュリティ保険への加入、そして組織的な対応に取り組んでいきます。

背景と課題

背景

委員会廃止と人員不足で対策停滞し、SCS評価制度(※2)★3へ向け規程見直しが急務

以前からサイバー攻撃への対処など多くのセキュリティ課題がありましたが、近年は情報セキュリティ委員会の廃止や担当部署の人員不足、専任者不在により対策が停滞していました。さらに、来年度のSCS評価制度※2で成熟度★3に対応したいため、社内規程の見直しなど早急な改善が求められていました。

- サイバー攻撃への対処方法がわからない
- 社内でインシデント発生影響の認識不足
- 経営層のセキュリティ意識が十分でない

課題

1. セキュリティ検討・推進体制が未整備
2. セキュリティ対策の実施方法と優先順位が不明瞭
3. サイバー攻撃による影響や体制強化の重要性など経営層を含めた共通理解が不足

取組内容

取組1

情報セキュリティ委員会の再設置と情報セキュリティ組織内の各役職の役割と責任を明確化し組織的対応を強化

情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施して情報セキュリティ対策を着実に推進するため各役職の役割と責任を明確化しました。

取組2

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、セキュリティ関連規程類を整備

来年度のSCS評価制度※2で成熟度★3の取得を目指し、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、情報セキュリティ関連規程、情報資産管理台帳、バックアップの手順書の整備を進めました。

取組3

サイバー攻撃による影響や体制強化の重要性など専門家による経営層向け説明会を開催し取組の意義を共有

経営層はセキュリティへの認識が十分でなく、どのように対策を進めるべきか迷いがありました。そこで本事業の専門家が、サイバー攻撃の影響や攻撃の目的、体制強化の重要性を説明したことで、経営層全体が必要なセキュリティ対策を明確に理解し、取組の意義を共有できました。

※1 Managed Detection and Response（専門家が24時間体制で脅威の監視・分析・対応を代行するセキュリティ運用サービス）
※2 SCS評価制度（サプライチェーン強化に向けたセキュリティ対策評価制度）

結果と今後

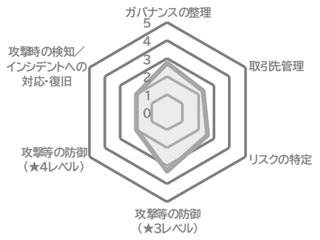
結果1
再設置した情報セキュリティ委員会を活用して情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有などマネジメントサイクルをしっかりと回してセキュリティを強化していきたいと思います。 → 継続

結果2
バックアップの手順書は完成、情報セキュリティ関連規程、情報資産管理台帳も来年度初には完成する見込みです。関連規程の内容は全社員に教育し、セキュリティ意識の向上を図ります。また来年度のSCS評価制度※2では、成熟度★3の取得をできるだけ早期に達成し、最低限必要なセキュリティ対策は完了したいと思います。 → 継続

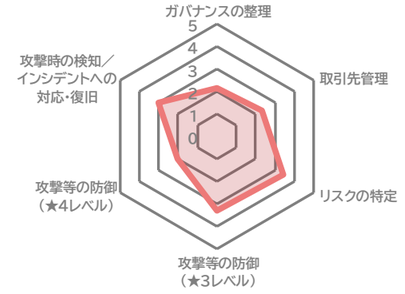
結果3
経営層全体が必要な情報セキュリティ対策を明確に理解し、取組の意義を共有できました。情報セキュリティ対策に必要な予算を確保し、MDR※1など新たなセキュリティ対策ツールの導入やサイバーセキュリティ保険への加入、そして組織的な対応に取り組んで行く予定です。 → 継続

取組テーマ：ガバナンスの整理 ／ 取引先管理 ／ リスクの特定 ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

サイバー攻撃でシステムが停止した場合に、重要業務とそれを支えるITシステムの特定、バックアップ方法や代替システムの確保、対応手順と体制の明確化、復旧訓練や定期的な見直しなど、しっかりと対応できる体制づくりを優先して進めていきます。その中で、SCS評価制度※2における成熟度★3の要求事項に対し、自社のリソースや現在の対応状況を踏まえて、実現可能な項目から対応を進めていく予定です。

経営者の声

サイバーセキュリティインシデント発生時の対応準備やBCPの整備が不足していることを認識いたしました。不足している部分を組織的に強化していく為、体制の整備に取組んでまいります。

参加者の声

中小企業に必要なセキュリティ対策全般の知識を習得できました。ワークショップは、参加企業同士の交流による情報交換・インシデント事例の共有が盛んに行われ自社環境との比較を得る貴重な場となりました。また、専門家派遣でのインシデント事例の解説は説得力のある内容で経営陣への意識改革に効果的でした。

サービス・その他　情報サービス業　Y社

統制基盤整備と情報収集・対応力強化による全社的セキュリティ運用高度化の実践

企業プロフィール
従業員数：301名以上

セキュリティ体制
複数名体制／兼務

事業内容
各種マーケティングリサーチの企画、実施、運用管理、情報処理やシステム開発を行う企業です。データ集計・分析を通じて、意思決定を支援する専門会社です。

背景と課題

サイバー攻撃の高度化を受け、親会社と連携した体制整備や社内ルール周知、情報資産台帳の整備と管理方法の明確化が課題でした。

取組内容

組織変更に伴い、親会社を含むグループ全体の情報管理体制を整理し、管理ルールの運用方法を検討するとともに、情報資産管理台帳の整備を推進しました。

結果と今後

親会社との役割分担や責任範囲、社内ルールの運用状況、情報資産管理台帳の整備状況などの課題が明確になりました。今後は親会社と連携し、役割の可視化と統制強化を図るとともに、ルールの周知徹底と台帳の継続的な更新管理を進め、実効性ある管理体制の確立を目指します。

背景と課題

背景

情報セキュリティ保全活動に関する役割や責任範囲、ルールの明確化の検討

親会社の情報セキュリティ管理体制との連携において、グループ全体の役割分担や責任範囲が十分に整理されておらず、インシデント発生時の対応フローも明確ではない状況でした。また、自社内の管理ルールについても運用基準が曖昧で、統一的な資産管理や台帳整備が課題となっており、グループ一体での統制強化が求められていました。

- 管理体制の役割分担と責任範囲の明確化
- 管理ルールの理解浸透と運用の徹底
- 統一的な情報資産管理体制の確立

課題

1. グループ全体の情報セキュリティ管理体制における役割分担と責任範囲の明確化、およびインシデント発生時の連携体制の強化
2. 親会社で整備された情報セキュリティ保全ルールについて、グループ全体での理解浸透と適切な運用の徹底
3. 現状は部門ごとに情報資産を管理しているため、グループ全体で統一的に情報資産を把握・管理できる体制の構築と維持管理ルールの確立

取組内容

取組1　情報セキュリティ管理体制の現状把握と役割分担の明確化

グループ全体で一体管理している情報システム基盤や親会社主導の開発案件への参画状況を踏まえ、横断的な情報セキュリティ活動における自社の役割と責任範囲を整理しました。あわせて必要な組織機能や連携体制を検討し、関係部署間で円滑に協働できる管理体制を整備しました。

取組2　情報セキュリティ管理ルールのグループ全体への浸透と運用徹底

親会社と事業領域が異なる独立運営の中で重大な事故は未発生であるものの、親会社ルールの徹底や周知に課題が見られました。そのため研修や社内ネットを活用した周知方法を再設計し、理解度向上と遵守徹底を図る仕組みを整備しました。

取組3　全社的な情報資産管理台帳の管理項目の明確化と運用ルール（作成、更新等）の策定と定着化の検討

事業特性に応じた独自の情報資産やクラウド上の資産を部門別に管理していたため、全社で統一的に把握・管理する体制を検討しました。管理台帳の整備や作成・更新・廃棄の運用基準、重要度設定、管理体制と教育による定着策を整理しました。

結果と今後

結果1　継続

グループ全体の情報セキュリティ管理体制の現状を整理し、各社の役割分担と責任範囲を明確化する方向性を共有しました。あわせて、体制を形骸化させないための維持管理手法や見直しの仕組みについても検討を進めました。今後は検討結果を踏まえ、親会社と連携しながら統一的かつ実効性のある情報管理体制の整備と運用定着を図ってまいります。

結果2　継続

グループ全体でのセキュリティインシデント対応力向上を目的に、親会社ルールの理解促進と効果的な周知方法を整理しました。あわせて、自社業務への適用範囲を明確化し、研修や訓練の具体的な実施手法についても検討しました。今後は検討内容を踏まえ、統一ルールの確実な運用と計画的な教育・訓練を通じて、実践的な対応力の強化と定着を図ります。

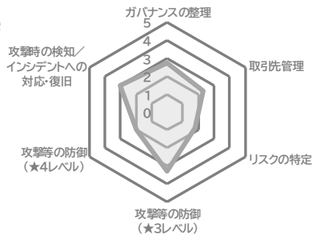
結果3　継続

保有する情報資産の棚卸しを実施し、重要度に応じた分類基準と作成・更新・廃棄に関する運用ルールを整理しました。あわせて、適切に管理するための体制整備と教育方法についても検討を進めました。今後はクラウド利用分を含めた定期的な見直しと改善を行い、部門横断で統一的に把握・管理できる仕組みを構築し、グループ全体のセキュリティ水準向上に貢献してまいります。

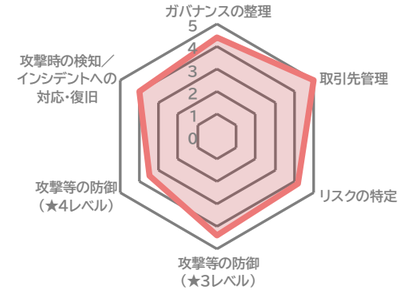
取組テーマ

ガバナンスの整理 ／ 取引先管理 ／ **リスクの特定** ／ 攻撃等の防御 ／ 攻撃時の検知 ／ インシデントの対応・復旧

Before



After



今後の展望

本取組により、グループ全体の役割分担と責任範囲が整理され、親会社の管理ルールの理解も進みました。しかし重要なのは、整備した仕組みを継続的に機能させることです。今後は全社的な情報資産管理台帳の整備と運用徹底を図り、クラウドを含む資産の定期的な棚卸しとレビューを実施します。さらに教育と周知を継続し、最新の基準や法令改正に対応しながら、事業成長とリスク低減を両立できる管理体制の強化を進めます。

経営者の声

昨今のセキュリティリスクの高まりを受け、グループ会社全体の情報セキュリティガバナンス強化が重要な経営課題となっています。本事業を通じて整理した運用ルールを、持続的成長の基盤として全社で確実に実行・定着させていくことを期待します。

参加者の声

担当者ごとに管理レベルのばらつきが見られ、全体としての統一が難しい状況でした。引き続き情報資産の整理に取り組むことで、属人化していた作業を是正し、業務の標準化を図っていきたいと考えています。