第１回 セミナー・ワークショップ
開催レポート

令和５年度 中小企業サイバーセキュリティ対策継続支援事業

中小企業サイバーセキュリティ対策継続支援事業とは

本事業は、現代社会で進むデジタルトランスフォーメーション（DX）の流れの中で、中小企業のセキュリティ強化を支援するプログラムであり、昨年から継続して行われている取組みで、今年で２年目を迎える東京都の事業です。

新型コロナの影響でデジタル化が急速に進展するなか、セキュリティの重要性は一層高まっています。しかしながら、中小企業は人手不足や知識の不足から、適切な対策を講じることが難しいという現実に直面しています。

このプログラムは、中小企業が基本的なセキュリティ対策を講じ、次のステップに進むためのサポートを行います。専門家の指導のもと、実際の課題に取組みながら学べる環境を提供し、実践的なセキュリティ知識やスキルをわかりやすく伝えます。同時に、参加企業同士の情報交換や他社の成功事例からの学びを共有できるプラットフォームも提供します。

約７か月間にわたるこのプログラムにより、中小企業のセキュリティ対策が強化され、企業の成長と安定をサポートします。また、支援の過程で使用するテキストや事例集などは、広く社会に公開され、中小企業が自社のセキュリティ対策を実施する際の貴重な手引きとなることで、中小企業全体のセキュリティ体制強化を目指します。

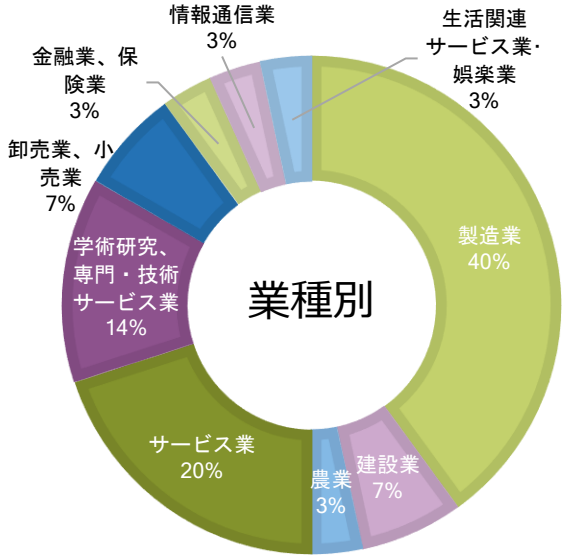
＜お問い合わせ先＞ 中小企業サイバーセキュリティ対策継続支援事業運営事務局 ※当事業は東京都より委託を受け、アデコ株式会社が運営しています。

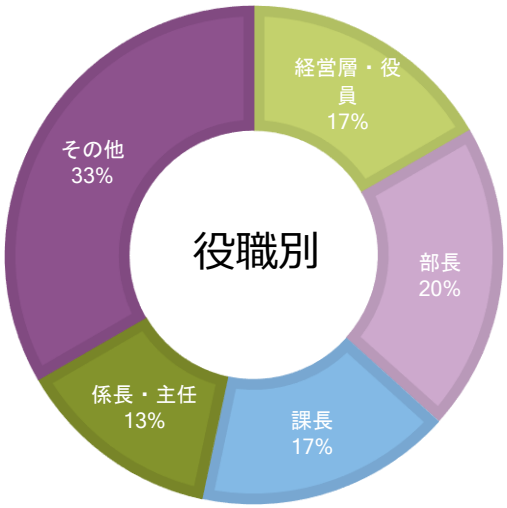
TEL：0120-138-166 MAIL：ade.jp.cybersecurity@jp.adecco.com

令和5年度中小企業サイバーセキュリティ対策継続支援事業

参加者の属性

令和５年度の本事業へは、抽選で選ばれた 30 社、30 名が参加されています。





登壇者紹介

■**講師**：星野 樹昭（ほしの しげあき）氏
■**専門分野**：IT インフラ設計・構築・テスト、移行設計、セキュリティ製品導入支援、ISMS 導入支援
■**業務経験**：25 年（セキュリティ経験：19 年）
■**保有資格**：情報処理安全確保支援士、Microsoft 認定資格プログラム
■**講師からひとこと**：
官公庁から中小零細企業を対象に、オンプレミス/クラウドを問わず、幅広い環境での IT インフラストラクチャーの導入や移行の経験がございます。これまで ISMS の導入支援やコンサルティングなど、多岐にわたる活動を行ってまいりましたが、近年ではセキュリティ対策の支援に重点をおいております。
皆さんと同じ視点でセキュリティについてお話しできればと思っております。

第 1 回セミナー　開催日：令和５年７月 25 日（火）13:00～15:00

サイバーセキュリティを取り巻く環境および中小企業に求められるサイバーセキュリティ対策

近年、サイバー攻撃はますます巧妙に進化しており、中小企業でもサプライチェーンを通じたサイバーセキュリティに関連する被害の広がりが懸念されています。多様なクラウドサービスが普及し、IoT や DX などの新たなテクノロジーに対するセキュリティ対策が必要とされています。これらの課題を踏まえ、企業は組織幹部自身が果たすべき役割を理解し、リーダーシップを発揮して対策を強化し、適切な対応を取る必要があります。

こうした社会的な背景を考慮し、セミナーでは政府が推進するサイバーセキュリティ対策（「サイバーセキュリティ経営ガイドライン（経済産業省）」）などの基本施策を参考にしつつ、IPA Security Action（二つ星宣言）の内容も取り入れました。また、IT パスポート、基本情報処理技術者、情報セキュリティマネジメントなどの基本的な知識についても解説しました。

第 1 章. デジタル時代の社会と IT 情勢

セミナーの冒頭では、デジタルトランスフォーメーション（DX）の重要性やデータの活用、そしてセキュリティの必要性について分かりやすく説明が行われました。また、経営者の視点からのアプローチが強調され、セキュリティ対策において「サイバーセキュリティ経営ガイドライン」の三つの原則（リーダーシップ、サプライチェーン、コミュニケーション）が大きな役割を果たすことが示されました。さらに、重要なセキュリティインシデントへの対応策が詳しく解説され、攻撃の失敗を未然に防ぐ努力と予算の適切な配分の重要性が認識されました。社内セキュリティの向上を促進する方法や外部対策の成功事例が共有され、参加者はセキュリティ強化の重要性と具体的な手法について深く理解を深める機会となりました。

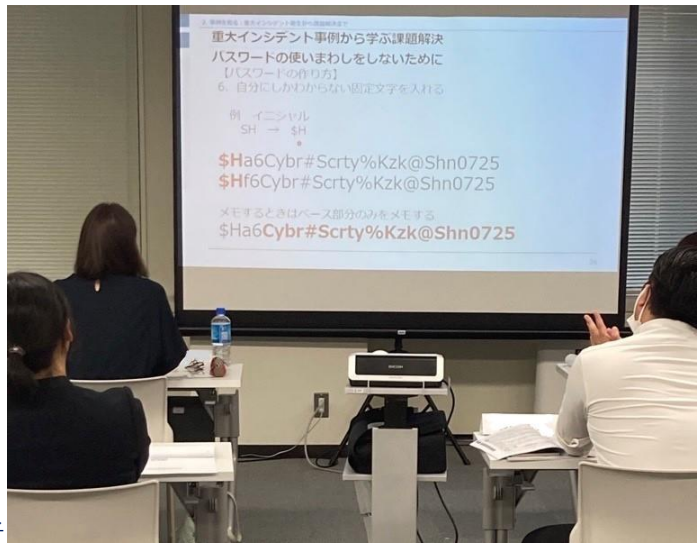
第 2 章. 事例を知る：重大インシデント発生から課題解決まで

第 2 章では、対策を施すことでインシデント発生のリスクを低減するため、IPA から発行されている「情報セキュリティ白書」や「情報セキュリティ 10 大脅威」の活用が提案されました。これにより、攻撃手口を理解し、適切な予防策や対策を講じ、優先順位を付けて対応することが重要であることが示されました。テレワーク時のサイバー脅威やクラウドサービス利用時の注意点についても具体的な方式と対策とともに詳しく説明されました。VPN 接続時の多要素認証の導入や特権パスワードの定期的な変更、パッチマネジメント、EDR の導入などが提案されました。また、過去の事例を通じて予防策の理解やリスクの認識を高める重要性が示され、アクセス元の信頼性を重視し、ゼロトラストセキュリティの考え方を取り入れる必要性についても触れられました。

第 3 章. サイバーセキュリティの基礎知識

第 3 章では、社員に取得を推奨する資格として、「IT パスポート」と「情報セキュリティマネジメント」の 2 つが取り上げられました。最初に、「IT パスポート」は社員全員の IT リテラシー向上を促進し、基本的な IT 知識や法律上の重要事項（例：知的財産権）について学ぶ機会として紹介されました。その後、「情報セキュリティマネジメント」資格の目的と重要性が説明され、セキュリティアクションの宣言についての内容が述べられました。また、対策基準のレベルに関する話題も取り上げられ、Lv.1 の「クイックアプローチ」から Lv.3 の「網羅的アプローチ」までの 3 つのアプローチについて概要が説明されました。第 1 回セミナーは、これらの内容で締めくくられました。

新宿会場の様子



セミナー受講中の様子

※セミナーで使用したテキスト等資料は、以下の本事業 Web サイトで公開しています。

https://security-keizoku.metro.tokyo.lg.jp/

＜お問い合わせ先＞ 中小企業サイバーセキュリティ対策継続支援事業運営事務局 ※当事業は東京都より委託を受け、アデコ株式会社が運営しています。

TEL：0120-138-166 MAIL：ade.jp.cybersecurity@jp.adecco.com

令和5年度中小企業サイバーセキュリティ対策継続支援事業

第 1 回ワークショップ　開催日：令和 5 年 7 月 25 日（火）15:15～17:15

セミナーに続くワークショップでは、参加企業がサイバーセキュリティに関する基礎知識を整理し、自社の IT 活用状況やセキュリティ状況を分析しました。この過程で、現在直面している課題に対する具体的な洞察を得ることができました。さらに、情報セキュリティ自社診断の実習を通じて、自社の情報セキュリティに関連するリスクを評価しました。この評価によって、セキュリティ上の脆弱性や攻撃リスクが明確になり、経営者を巻き込んだセキュリティ対策の策定に進むことができました。

ワークショップの最後では、参加者同士がグループで意見交換を行い、今後の情報セキュリティ対策に向けたアイデアや課題を熱心に共有しました。こうした活発なディスカッションを通じて、各企業は異なる視点からのフィードバックを受け、より効果的なセキュリティ対策を模索する手助けとなりました。

ディスカッションの展開とテーマごとのグループ発表

本セッションでは、個人ワーク、グループワーク、発表とフィードバックのサイクルを通じて、有益なディスカッションが展開されました。第 1 回のワークショップでは、3 つのゴールに基づくテーマを設定し、それぞれのテーマで活発なディスカッションを行い、深化させていくこととなりました。以下では、各テーマごとにグループから出た意見をご紹介いたします。

テーマ 1．自社で活用している IT および実施できているセキュリティ対策について整理する

<ゴール> 自社の IT 活用状況を理解する

「情報共有」と「意見交換」という観点でディスカッションを行いました。異なる会社規模や環境であるにもかかわらず、共通して「トップの意識がサイバーセキュリティの強化において重要であること」、「資源の一元管理がセキュリティ対策の効率化に繋がること」、「標的型訓練の実施が従業員の警戒心向上に寄与すること」などの意見がチームメンバーから出ました。

自社で使用しているセキュリティ製品・インフラの現状と、その中で実施している対応策について共有しました。具体的な事例として、「スプリットトンネリングの実装による通信の暗号化」、「標的型訓練の実施による従業員の教育と警戒心向上」、「セキュリティ保険の加入によるリスク軽減策」などが挙げられました。

グループ発表のポイント

資産の一元管理の重要性
一貫したセキュリティ対策を進める上で、自社の IT 資産と守るべき情報資産を正確に把握することが不可欠です。自社の IT 資産と守るべき情報資産を把握することは、将来的に ISMS フレームワークに基づいたセキュリティ実装とルールの整備に繋がる重要なステップです。

標的型メール訓練の効果
巧妙な日本語を用いた怪しいメールが増えている現状を踏まえ、積極的な訓練を通じて従業員がリスクを認識し、適切に対処できるようになることが重要です。

テーマ 2. 自社のセキュリティ課題について整理する

<ゴール> IT 活用に対して実施できているセキュリティ対策を整理する

パスワードの適切な管理や BitLocker の導入に関するメリットとデメリットについて意見交換が行われました。特に、パスワードの管理方法やツールの利用に関する情報が共有され、さらにはパソコンのキッティングを担当するスタッフについても話題が取り上げられました。

ベンダーに全てを任せると、自社の能力が制限される可能性があるという気づきがありました。この機会を通じて、皆さんと意見を交換することで、自社でも一定のことは実施できるようになるかもしれないと感じました。

グループ発表のポイント

BitLocker の適切な管理について
BitLocker の管理方法（アクティブディレクトリ管理か個別管理か）は重要で、誤った設定は重大な問題につながる可能性があります。セキュリティ対策は単に厳格にするだけでなく、適切な管理方法と工数を考慮する必要があります。

自社内でのキッティングとチケットシステムの関係
自社内でキッティングを行う場合、効果的な運用を確保するためには、ITIL（Information Technology Infrastructure Library）に基づくチケットシステムを導入することが考えられます。ただし、このシステムはコストがかかるため、慎重な運用設計とセキュリティ対策が重要です。

ベンダー依存の回避と情報源の信頼性
健全な情報セキュリティにおいて、ベンダーへの過度な依存は避けるべきです。信頼性のある情報源を慎重に確認し、適切な情報を選別するスキルが重要です。

テーマ 3. 取組むことができるセキュリティ対策を整理する

<ゴール> 自社のセキュリティ課題および取組むことができる対策内容を整理する

トップの意識が重要であり、定期的な社員教育とシステムのバックアップ体制の整備を進める予定です。最低 10 文字のパスワード設定や情報資産の管理にも着手する予定です。

USB メモリの取扱いについては無効化や制限を検討し、VPN のパッチも定期的に実施する予定です。また、ベンダーに頼らず自社の状況を改善し、ログインパスワードの強制変更設定も検討しています。

グループ発表のポイント

USB メモリの管理制御
USB メモリの無効化や細かな管理制御には、アクティブディレクトリのグループポリシーや専用の管理ソフトウェアを活用する方法があります。

パッチマネジメントとファームウェアのアップデート
バックヤードで動作する機器については、パッチマネジメントとともにファームウェアのアップデートも必要です。

セキュリティにおける BCP
最新のガイドラインでは、バックアップに関連してセキュリティに焦点を当てた事業継続計画（BCP）が取り入れられています。

代表してグループの意見を発表いただきました。

ワークショップ終了後は、名刺交換や歓談が行われました。

参加者からの声

※参加者アンケートより抜粋

「増加するパスワードをどう作って管理したらいいか困っていたので、具体例を示していただけてよかったです。」

「漠然とした自分の知識に対して、資料としてまとめてもらえたので系統立てて理解することができました。再度資料を見直して理解を深めたいと思います。」

「体系立ててセキュリティ対策の知識の講義をしていただき、自分がわかっていること、わかっていないことの地図がそれぞれ少しずつ繋がってきた気がしました。」

「具体的なセキュリティインシデントの事例が自社の環境でも起こりうるようなことで、解説を聞き改めて危機感を持つことができました。また、実施すべきセキュリティ対策へのアプローチ方法などの知識を深めることもできました。」

「どのようなセキュリティ対策を実施しているのかを他社様と共有し、自社がどういった部分で不十分であるのか、どういった部分は対策が進んでいるのかを客観的に認識することができました。」

「経営層からの意識・意思の伝達や、組織のルーティンを策定することで組織全体のセキュリティ意識を向上させることの大切さを認識できました。」

「今までは無計画にセキュリティ対策をしてきましたが、今後はあるべき姿を明確にし、１つ１つの対策の意味を考えながら進めていく必要があると感じました。」

「社内教育や個々のセキュリティレベルの向上は、すぐにでも対応できると感じています。」

<お問い合わせ先> 中小企業サイバーセキュリティ対策継続支援事業運営事務局 ※当事業は東京都より委託を受け、アデコ株式会社が運営しています。
TEL：0120-138-166 MAIL：ade.jp.cybersecurity@jp.adecco.com

運営事務局より編集後記

梅雨明け直後の猛暑の中、第 1 回セミナー・ワークショップが無事に開催されました。参加者の皆様は熱心にご参加いただき、活発な議論と意見交換が行われる中で、セミナーでは熱心にメモを取る姿が印象的であり、ワークショップ中には笑い声も交えながら有益な時間を共有しました。

講師からは、サイバー空間と現実空間の融合が描かれた 2009 年公開のアニメ映画「サマーウォーズ」が紹介されました。AI の暴走が引き起こす仮想空間の混乱が現実世界に及ぼす影響についての描写は、今の社会の課題と重なる部分が多く、細田守監督の先見性に感銘を受けました。

新型コロナの 5 類移行後のこの夏、多くの方がお休みを取って旅行や帰省を楽しまれることでしょう。平常とは異なるこの時期だからこそ、ウイルス感染や不正アクセスなどのリスクに適切に備え、セキュリティ対策と準備を怠らずに過ごすことが重要です。

ご参加いただいた皆様に心より感謝申し上げます。今後も引き続き、より良いセキュリティ対策の普及と情報共有に努めてまいります。ご支援賜りますようお願い申し上げます。

運営事務局一同

次回（第 2 回）セミナー・ワークショップのご案内	**日時**：令和 5 年 8 月 22 日（火）　13 時 00 分～17 時 30 分 **会場**：東京都新宿区西新宿 1-22-2　新宿サンエービル 7F **テーマ**：これからの企業経営で必要な攻めと守りの IT 活用およびサイバーセキュリティ対策

本件に関するお問い合わせ

中小企業サイバーセキュリティ対策継続支援事業運営事務局
TEL：0120-138-166
受付時間：平日 9:00～17:00（祝日を除く）
メール：ade.jp.cybersecurity@jp.adecco.com
URL：https://security-keizoku.metro.tokyo.lg.jp/
Facebook: https://www.facebook.com/cys.keizoku