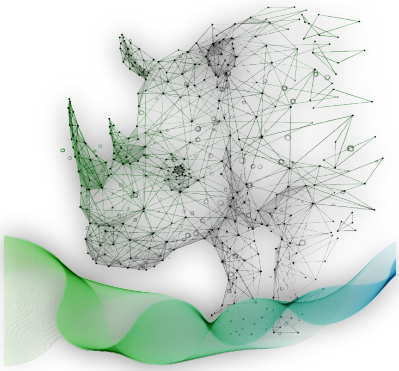
第７回
セミナー・ワークショップ
開催レポート



令和６年度 中小企業サイバーセキュリティ社内体制整備事業

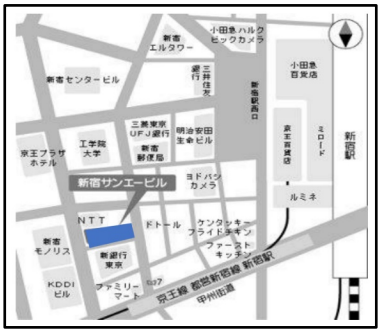
開催概要

令和６年１０月２２日(火)、東京都主催「中小企業サイバーセキュリティ社内体制整備事業」第７回セミナー・ワークショップが開催されました。

第７回セミナーでは、「具体的な構築・運用の実践」と題し、政府が策定したガイドラインを参考に情報システムを導入する流れとセキュリティ対策の実装と運用ポイントを解説しました。ワークショップではセミナーで学んだ知識や情報を活用し、システム導入におけるセキュリティ対策の検討を行いました。参加者はセミナーでインプットした学びをワークショップでアウトプットし、実践的なアイデアや対策を具現化しました。また、今回はワークショップ後にセミナー講師を交えた座談会を開催し、参加企業間で交流をはかりました。

開催日時と場所

【日時】：令和６年１０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
【アクセス】：JR・私鉄各線 「新宿駅」 西口・南口より　徒歩 5～8 分



当日のタイムスケジュール

13:00 ～ 15:00　セミナー（※途中 5 分休憩あり）
15:00 ～ 15:15　休憩
15:15 ～ 15:40　ワークショップ（内容説明・個人ワーク）
15:40 ～ 16:40　ワークショップ（グループワーク）
16:40 ～ 17:15　全体発表・講師からのフィードバック
17:15 ～ 17:30　事務局からの案内

17:45～18:30　座談会（※希望者のみ）

＜お問い合わせ先＞ 中小企業サイバーセキュリティ社内体制整備事業運営事務局　※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.shanaitaisei@jp.adecco.com

セミナー内容　　講師：星野 樹昭氏

全 10 回開催される本セミナーでは、サイバーセキュリティの最新情報や実践的な対策内容を盛り込んだオリジナルテキストを使用して講義を進めていきます。今回のセミナーでは、情報システムを導入するにあたり、EC サイト構築を例に企画から要件定義、調達、設計・開発、運用保守までの流れと、セキュリティ機能の実装方法について解説しました。

第８編　具体的な構築・運用の実践

第２１章. 人的、組織的、技術的、物理的対策の実施手順に基づいた実施

第２１章では、「デジタル・ガバメント推進標準ガイドライン」に準拠した手順で、情報システムを導入する工程および中小企業が主体的に関与するポイントを紹介しました。また、導入工程で作成するべきドキュメントについて解説し、各工程においてセキュリティ機能を実装・運用する方法について詳説しました。情報資産におけるリスクを踏まえ適切なセキュリティ要件を定めることが、情報システムのセキュリティ対策強化につながると総括し、第７回セミナーは終了しました。

セミナー風景

参加者のプライバシーに配慮し画像を加工しています

※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://shanaitaisei.metro.tokyo.lg.jp/

セミナー参加者の声　※参加者アンケートより一部抜粋

セミナー受講で得た学びの成果

- ✓ 「社内でのシステム開発時に参考となる講義内容でした」
- ✓ 「セキュリティやシステムを導入する際、要件定義をしっかりと時間をかけて行うことが大切だと理解しました」
- ✓ 「システム導入における実用的な内容が多く勉強になりました」
- ✓ 「例示した EC サイトを別のシステムに置き換えることによって汎用的に使える内容で参考になりました」
- ✓ 「難しい内容でしたが、講師の説明がわかりやすく理解が進みました」

セミナー受講で得た自社の課題・気づき

- ✓ 「他社と比べ社内の IT 化が遅れていることが課題です」
- ✓ 「ベンダーとのコミュニケーション不足が課題だと気づきました」
- ✓ 「社内で使用しているクラウドサービスの可視化ができていないため、管理表を作成したほうがいいと気づきました」

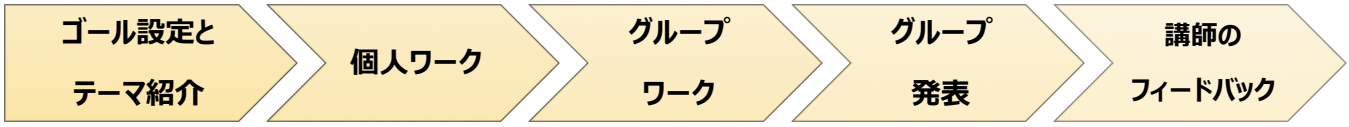
セミナー受講で得た活用できそうな施策・アイデア

- ✓ 「セキュリティを高めるソフトやツールの導入を検討し、適切なデータ管理、アクセス管理対策を実施していきたいです」
- ✓ 「今回のテキストを自社システム導入時の参考資料とするべく、内容を整理しておきたいです」
- ✓ 「経営層へのセキュリティ対策予算申請の裏付けに、講義内容が活用できそうです」

ワークショップ内容

第７回ワークショップでは、セミナーで学んだ情報システム導入の流れとセキュリティ対策の実装時のポイントを活用します。講師が提示したテーマは「Web で利用できる勤怠管理システム」の構築です。このシステムを自社で構築するにあたり、システムを安全に利用するためのセキュリティ機能について考えました。さらに、その機能を実装した場合の課題や不安について検討しました。個人ワークで各自の考えをまとめた後、グループワークでそれぞれの考えやアイデアを展開しました。その後、課題や不安への解決策をグループメンバー間で協議しました。各グループは活発な意見交換を行い、最後に行われた全体発表では各グループならではの視点や実際に取組を実施している他社事例を参加者全員が共有しました。

【ワークショップの進め方】



ゴール
要件定義を考えてみる
他社が実施している取組について、自社でも取り入れられるか考える
２つのテーマ
１．必要なセキュリティ機能について考える **個人ワーク**＿勤怠管理システムを実現するための必要な 10 機能*をより安全に利用するために、どのようなセキュリティ機能が役に立つでしょうか。機能ごとに役に立つと思うセキュリティ機能について考えてみましょう。 **グループワーク**＿皆さんの意見やアイデアをグループで共有しましょう。
２.セキュリティの運用上の課題と解決策を考える **個人ワーク**＿１で考えたセキュリティ機能を実装したとしても、運用する上でどのような課題や不安があるか考えてみましょう。 **グループワーク**＿個人ワークで検討した「運用する上での課題や不安」について、解決策を検討しましょう。解決策を検討後、さらに実装することで強化されるセキュリティ機能や技術的な対策以外でのアプローチによる解決策について考えてみましょう。

*【勤怠管理システムを実現するための必要な 10 機能】

No	機能名	内容
1	出退勤記録機能	従業員の出勤や退勤時間を正確に記録する機能。打刻方法として、PC、スマートフォン、IC カード、指紋認証などがあります。
2	勤務時間集計機能	各従業員の勤務時間を自動的に集計し、残業時間や休暇日数も含めて管理します。週次、月次、年次の労働時間の確認が可能です。
3	シフト管理機能	シフト制の企業向けに、従業員の勤務シフトを作成、管理し、従業員が自分のシフトを確認できる機能。
4	休暇・有給管理機能	休暇申請や有給休暇の管理、残日数の自動計算ができる機能。従業員が休暇をオンラインで申請し、承認ワークフローを通じて管理者が承認します。
5	残業管理機能	残業時間をリアルタイムで記録し、法定の上限を超えないように管理する機能。残業時間が一定値に達した場合のアラート機能も含まれることがあります。

6	勤怠データのレポート機能	勤怠データをもとに、管理者向けにレポートを作成する機能。これにより、全従業員の勤務状況を一目で把握でき、労務管理の効率化に寄与します。
7	法令遵守機能	労働基準法などの法令に基づき、適切に労働時間を管理するための機能。休憩時間の管理や法定残業時間の監視が含まれます。
8	給与システム連携機能	勤怠データを給与計算システムに自動で連携し、正確な給与計算を支援します。
9	マルチデバイス対応機能	PC だけでなく、スマートフォンやタブレットなど複数のデバイスで勤怠を管理・記録できる機能。
１０	リアルタイム更新と通知機能	勤怠情報の更新やシフトの変更をリアルタイムで反映し、従業員や管理者に通知する機能。

【グループ発表内容（抜粋）】

セキュリティ機能	運用上の課題や不安	実装することで強化されるセキュリティ機能や技術的な対策以外でのアプローチによる解決策
アクセスログ記録機能	・大量のログデータの発生により管理や分析に時間がかかる	・ログの保存期間決定 ・ログファイルのバックアップ ・分析期間の検討
パスワード管理	・安易なパスワード設定、パスワード使いまわし、付箋の利用	・パスワードルールの策定、二要素認証
不正アクセスの防止	・情報流出の不安 ・アクセス制御、アクセス権の設定	・定期なバックアップ ・サイバー保険 ・アクセスログの定期的な確認
データへのアクセス制御 （従業員ごとに権限で管理）	・なりすましログイン ・異動・昇進時の権限変更の未対応	・社内の情報連携を整備

課題解決のヒント

アクセスログ分析の方法は、毎月の定常性を確認する他、接続元の IP アドレスが国外のものや日本時間で夜間のアクセスのものに注意を払うなど、社内で指針を作るのがポイントです。

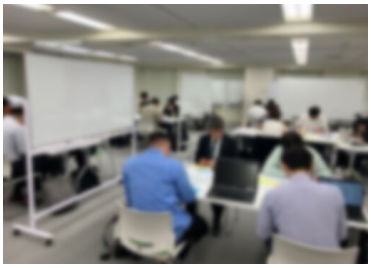
パスワード管理は、パスワードを使わないという選択肢もあります。持っているもの（スマートフォンなどのデバイス）と生体認証の二要素で認証の仕組みを整えることも考えてみましょう。

不正アクセスの防止策として、会社経由の VPN 接続を行って安全性を確保するというソリューションも検討してみましょう。

データへのアクセス制御は、定期的な権限の棚卸し作業が必要です。運用として、誰がどこにアクセスできているのか、またそれは正しいアクセス権限なのかを台帳を用いて管理することが重要です。

ワークショップ風景

個人ワークに取り組んでいます



付箋を使いグループで内容検討中

全体発表の様子

参加者のプライバシーに配慮し画像を加工しています

ワークショップ参加者の声 ※参加者アンケートより一部抜粋

- ✓ 「システムを構築する時に必要なセキュリティ機能、課題や解決策など、各社と意見交換できました」
- ✓ 「各社の状況を共有することができ、参考になりました」
- ✓ 「個人ワークで自分の考えをまとめ、グループワークで様々な意見を聞くことができ、有意義な時間となりました」
- ✓ 「普段の業務では考えることがないテーマなので、よい機会だと捉え取組みました」
- ✓ 「他社の実例を聞けたことで、知見が広がりました」

次回のご案内	**日時**：令和６年１１月１９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

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社内体制整備事業運営事務局
TEL：0120-138-166
受付時間：平日 9:00～17:00（祝日を除く）
メール：ade.jp.shanaitaisei@jp.adecco.com
URL： https://shanaitaisei.metro.tokyo.lg.jp/
Facebook: https://www.facebook.com/cys.shanaitaisei/