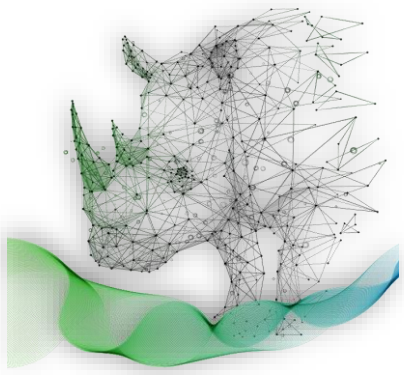
第２回
セミナー・ワークショップ
開催レポート



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８月６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２回セミナー・ワークショップが開催されました。

第２回セミナーでは、「これからの企業経営で必要な IT 活用とサイバーセキュリティ対策・セキュリティ事象に対応して組織として策定すべき対策基準と具体的な実施・各種ガイドラインを参考にした対策の実施」の３つを主題に据え、レベルに応じたセキュリティ対策のアプローチ手法を解説しました。また、ワークショップではセミナーでの学びを踏まえ、仮想企業のインシデント事例を用いて、対策基準の策定に取り組みました。セミナーでインプットした知識や情報をワークショップでアウトプットし、参加者全員でアイデアを共有することで、相乗効果が期待でき、中小企業の社内体制強化を目指します。

開催日時と場所

【日時】：令和６年８月６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

セミナー・ワークショップ会場

当日のタイムスケジュール

13:00 ～ 14:55　セミナー（※途中 5 分休憩あり）
14:55 ～ 15:00　質疑応答
15:00 ～ 15:15　休憩
15:15 ～ 16:25　ワークショップ（グループワーク）
16:25 ～ 17:25　全体発表・講師からのフィードバック
17:25 ～ 17:30　事務局からの案内

＜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の情報や網羅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。２回目となる今回のセミナーでは企業経営で必要な IT 活用とサイバーセキュリティ対策、セキュリティ事象に対応した対策、各種ガイドラインを参考にした対策について詳しく説明を行いました。

第３編　これからの企業経営で必要な IT 活用とサイバーセキュリティ対策

第７章. セキュリティ対策の概要（全容）

第７章では、ISMS 認証を前提としたセキュリティ対策における基準を 3 段階にレベル分けし、各基準の手法について紹介しました。まず、セキュリティ対策基準を策定するためのアプローチ方法として、Lv.1 のクイックアプローチ、Lv.2 のベースラインアプローチ、Lv.3 の網羅的アプローチがあることを解説しました。また、それぞれの特徴と想定される適用ケースについてテキスト資料を基に説明を行いました。

第８章. 用語定義および関係性と識別方法

第８章では、ISO/IEC 27000 に記述されている「リスク」、「脅威」、「脆弱性」、「管理策」といったセキュリティ対策実施のために重要な用語の定義、また、それらの用語の関係性、脅威や脆弱性の識別方法について、テキストに記載された図や表を用いて参加者の理解を促す説明をしました。

第４編　セキュリティ事象に対応して組織として策定すべき対策基準と具体的な実施

第９章. 具体的手順の作成（Lv.1 クイックアプローチ）

第９章では、Lv.1 のクイックアプローチ手法における対策基準・実施手順の策定方法について解説しました。クイックアプローチは、即時の対応や緊急事態への対処が必要な事例に対して実施する手法であることを解説しました。さらに、概要やメリット、デメリットについて触れ、実際の事例に基づいた対策方法の紹介を行いました。

第５編　各種ガイドラインを参考にした対策の実施

第１０章. 具体的手順の作成（Lv.2 ベースラインアプローチ）

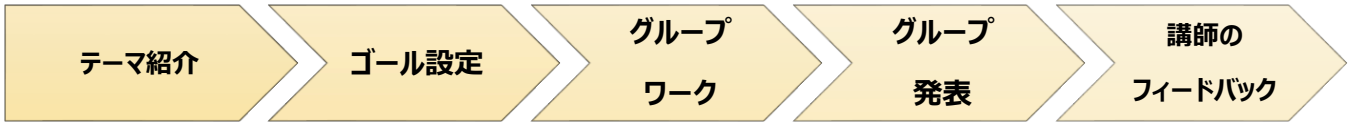
第１０章では、ガイドラインやひな型などの資料を参考にする Lv.2 のベースラインアプローチにおける対策基準・実施手順の策定方法について解説しました。ベースラインアプローチは、IPA や総務省などが発行しているガイドラインやひな型を参考にすることにより、組織全体で対策の一貫性を確保でき、最低限の対策を講じることが可能である手法であることに言及し、第２回のセミナーは終了しました。

セミナー参加者の声　※参加者アンケートより一部抜粋

- ✓ 講師の説明がわかりやすかったです。「脅威」や「リスク」などの説明のときに一般的な例えを用いて解説いただき用語の理解が深まりました。
- ✓ 社内で対策基準の見直しを検討中でしたので、今回のテーマはタイムリーで参考になりました。
- ✓ セキュリティポリシーの改訂にあたり、様々なテンプレートやガイドラインを紹介いただき社内で活用できそうです。
- ✓ 取引先に向けたサプライチェーン対策の実施にあたり、どのように情報資産を管理するべきか検討していました。今回学んだアプローチ手法を使った対策は参考にできそうです。
- ✓ 最新のインシデント事例を踏まえたセキュリティ対策を学ぶことができ、社内の体制強化につなげていきたいと考えています。
- ✓ テキストに記載のある参照資料について、スクリーンに投影していただき内容の理解が進みました。

ワークショップ内容

セミナーに続くワークショップでは、講師よりテーマとゴール設定が紹介された後、1 チーム４～５名で構成された参加メンバーが３つのゴールを目指し、グループワークに取り組みました。今回のワークショップでは、仮想企業で発生したインシデント事例の対策について検討していきます。今回から検討結果発表の可視化向上のため、各チームに 1 台ずつパソコンを準備しました。書記担当が議論の過程をホワイトボードに記録し、発表資料作成担当が議論の結果をパワーポイントのテンプレートにまとめていきます。各グループで検討した内容は発表担当がスライドを投影してプレゼンテーションを行い、その後各グループの発表に対し講師がフィードバックを行いました。



テーマ
インシデント事例を活用した対策基準の検討
３つのゴール
① 最新のインシデント事例を踏まえた対策基準の検討
② 最新のガイドラインを参考にした対策基準の検討
③ 自社の状況分析を基にグループでの意見交換を実施する

【検討内容】（一部抜粋）

1. 以下のセキュリティインシデント事例は、「5 分でできる！情報セキュリティ自社診断」[1]に記載されている 25 の診断項目が、すべて「実施していない」という結果が出た企業で発生したものです。これらの被害を起こさないようにするために、どのような対策を実施すればよいか、「5 分でできる！情報セキュリティ自社診断」の「解説編」に記載されている対策を選択しましょう。
2. インシデント事例を防ぐための具体的な対策基準を考えましょう。

【インシデント事例 A】クラウドサービスの障害によるデータ損失

ある日、企業が利用していたクラウドサービスが大規模な障害を起こし、サービスが長時間にわたり利用できなくなった。
この結果、重要なデータがアクセス不能となり、一部のデータが永久に失われた。
緊急時の対応手順が整備されていなかったため、従業員は適切な対応ができず、復旧作業に多大な時間と費用がかかってしまった。

【インシデント事例 B】テレワーク中の情報漏えい

テレワーク中に、従業員が個人所有のパソコンを使用して業務を行っていた際、そのパソコンがマルウェアに感染した。
このマルウェアを通じて、社内の重要情報が外部に漏えいしてしまった。さらに、取引先に提供していた情報も流出し、
取引先との信頼関係が破綻した。緊急時の対応手順が整備されていなかったため、迅速な対応ができず、被害が拡大した。

[1] 5 分でできる！情報セキュリティ自社診断 https://www.ipa.go.jp/security/sme/f55m8k0000001waj-att/000055848.pdf

グループ発表（一部抜粋）

【インシデント事例 A】クラウドサービスの障害によるデータ損失

発表者

私たちのグループではデータ損失というインシデントに対し、「**バックアップを励行する**」という対策を選択しました。そして対策基準として重要情報のバックアップを定期的に行うこと、またバックアップ先の装置や媒体は、バックアップの際のみにパソコンと接続するという運用を策定しました。

グループ発表のポイント

定期的なバックアップを手順に記す際は、どの頻度で行うのか、**定量的に表現**（例：月に 1 度フルバックアップを取得する）するとより良い手順になるでしょう。

【インシデント事例 B】テレワーク中の情報漏えい

私たちのグループではテレワーク中の情報漏えいというインシデントに対し、「**OS やソフトウェアは常に最新の状態にする**」という対策を選択しました。テレワークで利用するパソコン等のソフトウェアやファームウェアを最新版にするという基準を設けることにより、一定の対策が取れると考えました。

発表者

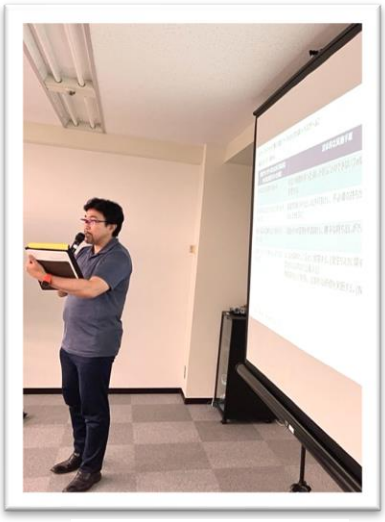
グループ発表のポイント

OS やソフトウェアのアップデートは、若干遅延を持たせて実施することも考慮してみましょう。アップデートをすぐに実施することによって不具合が生じるケースは 0 ではないため、リスクとして捉えることも想定しておきましょう。

セミナー・ワークショップ風景

セミナー風景

グループワークの検討結果を発表する参加者



フィードバックを行う講師

次回のご案内	**日時**：令和６年８月 20 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/