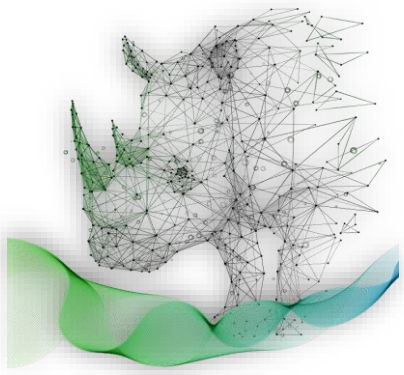
第４回
セミナー・ワークショップ
開催レポート



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９月１０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４回セミナー・ワークショップが開催されました。

第４回セミナーでは、「ISMS の構築と対策基準の策定と実施手順」と題し、情報セキュリティマネジメントシステム（ISMS）のフレームワークを用いたセキュリティ対策基準、実施手順を作成するプロセスについて解説しました。さらに ISO/IEC 27002 における管理策のカテゴリと構成の説明を行ったうえで、４つのカテゴリのひとつである「組織的管理策」に焦点を当て講義を行いました。続いて実施したワークショップではセミナーでインプットした知識を用い、仮想企業の情報資産リスクを低減するための実施内容について、グループごとに活発なディスカッションが行われ様々なアイデアが創出されました。

開催日時と場所

【日時】：令和６年９月１０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 ～ 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 ～ 16:30　ワークショップ（グループワーク）
16:30 ～ 17:20　全体発表・講師からのフィードバック
17:20 ～ 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の情報や具体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網羅的なアプローチ方法である ISMS のフレームワークを用いた対策基準と実施手順の策定方法について説明しました。ISMS の概要紹介に加え、文書体系、取得のプロセス、管理策について解説しました。

第７編　ISMS の構築と対策基準の策定と実施手順

第１３章. ISMS の要求事項と構築

第１３章では、ISMS において PDCA サイクルを回すために重要となる文書化の方法や、実施すべき事項について焦点を当て説明しました。また、ISMS を用いた対策のメリットや留意点、ISO/IEC 27001 の構成について解説を行い、対策基準を策定するために参考とすべき管理策の全体像について紹介しました。

第１４章. ISMS の管理策

第１４章では、ISMS の管理策の分類と構成について解説していきます。2022 年に改訂が行われた ISO/IEC 27002 の主な変更点として、93 ある管理策を「テーマ」と位置づけ、「組織的管理策」「人的管理策」「物理的管理策」「技術的管理策」の 4 カテゴリに管理策が分類されていることを解説しました。さらに、2022 年に導入された属性（attribute）という新しい概念およびテーマと属性の関係について紹介しました。

第１５章. 組織的対策

第１５章では、「組織的管理策」をもとにした対策基準を策定する手順について講じました。そのうえで、策定した対策基準をもとに具体的な実施手順を策定する方法を紹介し、第４回セミナーは終了しました。

※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/

セミナー風景
（プライバシーに配慮し画像を加工しています）

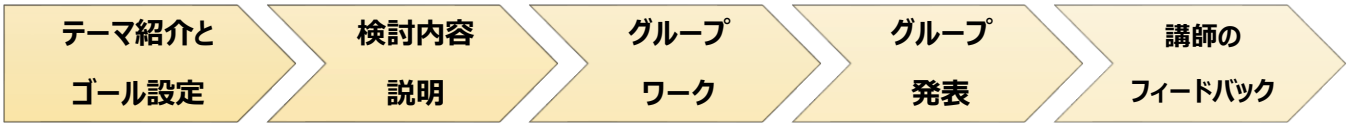
セミナー参加者の声　※参加者アンケートより一部抜粋

- ✓ ISMS の対策基準をもとにしたセキュリティ方針の策定方法を理解することができました。
- ✓ それぞれの管理策について理解が深まり、選定基準や考え方が参考になりました。
- ✓ セミナー受講を契機に自社の実態に即して部分的に導入を検討してみようと考えています。
- ✓ 現在の規程で不足している部分に気づくことができました。
- ✓ 自社のリスク管理の不備を認識し、対策に役立てたいと思いました。
- ✓ ISMS の認証は取得していますが、やり切れていない部分を見つけることができました。
- ✓ ISMS の認証取得について検討しており、セミナーの内容が参考になりました。
- ✓ 定期的な教育や訓練が情報漏えいを防ぐために非常に重要であることを学びました。
- ✓ セミナーで学んだことを社内に展開しメンバーを巻き込みディスカッションすることで、意識向上が期待できそうです。
- ✓ 組織として体系立てて IT プロセスの一環としてセキュリティ対策を構築する必要があると学びました。
- ✓ マネジメントの適用範囲の決定プロセスを再考するきっかけとなりました。

ワークショップ内容

情報資産の洗い出しとリスクアセスメントを実施した後は、組織として必要な対策基準の策定に進みます。第 4 回ワークショップでは、講師が設定した 8 つの社内資産のリスクを低減するため、ISMS の管理策を用い、組織として行うべき実施内容について検討しました。参加企業は 1 チーム 4 ～ 5 名で構成された 8 つのグループに分かれワークに取り組みました。今回はセミナーで学んだ組織的管理策に焦点を当て協議を行いました。37 の組織的管理策の中から適切な管理策を選択し、具体的な実施内容を策定していきます。活発な意見交換を経て各チームで策定された実施内容は、最後に全体に向けて発表され、参加者は多様なアイデアや視点を得る機会を得ました。

【ワークショップの進め方】



テーマ
対策基準の作成
3 つのゴール
① リスクアセスメントの結果をもとに必要な管理策を検討
② 管理策をもとに対策基準および適用宣言書を作成
③ グループでの意見交換、協議、発表

【検討内容】

次の 8 つの社内資産はリスクアセスメントが完了し、リスクがすでにわかっている状態です。このリスクを低減させるための組織的管理策を 3 つ選択し、具体的な実施内容を策定してください。

【8 つの社内資産】

1.顧客データベース

リスク：顧客の個人情報が含まれており、漏えい、改ざん、不正アクセスのリスクが存在します。

2.クラウドサービス利用の契約

リスク：クラウドサービスを利用する際に、データの保存場所や処理の方法が不明確だと、セキュリティのリスクが増大します。

3.事業継続計画（BCP）と関連するドキュメント

リスク：事業継続計画が適切に策定されていないと、災害やサイバー攻撃などの際に迅速な対応ができず、組織全体に影響を及ぼすリスクがあります。

4.従業員の個人情報管理

リスク：従業員の個人情報が漏えいした場合、法的問題や組織の信頼性が損なわれるリスクがあります。

5.製品設計図

リスク：製品設計図が流出した場合、競合他社に技術的優位性を奪われるリスクがあります。

6.内部監査記録

リスク：内部監査記録が漏えいした場合、組織のセキュリティ弱点が外部に露呈し、攻撃のリスクが高まります。

7.マーケティング戦略資料

リスク：マーケティング戦略が競合他社に漏えいすると、市場での競争優位性を失うリスクがあります。

8.ソフトウェア開発プロジェクトの計画書

リスク：ソフトウェア開発の計画が漏えいすると、知的財産権の侵害やプロジェクトの失敗リスクが増加します。

【37 の組織的管理策[1]】

組織的管理策	
5.1 情報セキュリティのための方針群	5.19 供給者関係における情報セキュリティ
5.2 情報セキュリティの役割及び責任	5.20 供給者との合意における情報セキュリティの取扱い
5.3 職務の分離	5.21 ICT サプライチェーンにおける情報セキュリティの管理
5.4 経営陣の責任	5.22 供給者のサービス提供の監視，レビュー及び変更管理
5.5 関係当局との連絡	5.23 クラウドサービスの利用における情報セキュリティ
5.6 専門組織との連絡	5.24 情報セキュリティインシデント管理の計画及び準備
5.7 脅威インテリジェンス	5.25 情報セキュリティ事象の評価及び決定
5.8 プロジェクトマネジメントにおける情報セキュリティ	5.26 情報セキュリティインシデントへの対応
5.9 情報及びその他の関連資産の目録	5.27 情報セキュリティインシデントからの学習
5.10 情報及びその他の関連資産の利用の許容範囲	5.28 証拠の収集
5.11 資産の返却	5.29 事業の中断・阻害時の情報セキュリティ
5.12 情報の分類	5.30 事業継続のための ICT の備え
5.13 情報のラベル付け	5.31 法令，規制及び契約上の要求事項
5.14 情報転送	5.32 知的財産権
5.15 アクセス制御	5.33 記録の保護
5.16 識別情報の管理	5.34 プライバシー及び PII の保護
5.17 認証情報	5.35 情報セキュリティの独立したレビュー
5.18 アクセス権	5.36 情報セキュリティのための方針群，規則及び標準の順守
	5.37 操作手順書

[1] 出典：サイバーセキュリティ社内体制整備事業「第 4 回セミナーテキスト」
https://shanaitaisei.metro.tokyo.lg.jp/assets/pdf/Tokyo_CyberSecurity_HandBook_2024_Text_04.pdf

【発表資料の紹介（抜粋）】

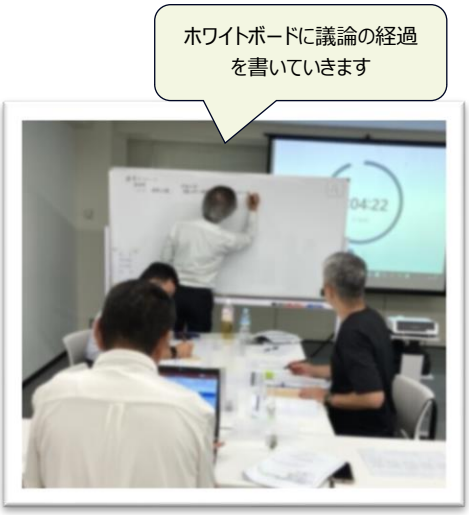
1.顧客データベースについての実施内容

管理策 No	管理策	実施内容
5.12	情報の分類	情報内容を確認し個人情報とそれ以外の分類とする
5.13	情報のラベル付け	5.12 で分類したものを重要度に応じラベル付けする
5.18	アクセス権	情報にアクセスできる人を情報レベルにより限定する。（ログから解析可能な状態にする）

【ワンポイントアドバイス】

5.12「情報の分類」と 5.13「情報のラベル付け」については、順序立てて考えているという点がポイントです。ISMS の考え方として各管理策の「関連性」が重要になってきます。資産を守るうえで、管理策を選定し実施内容を考える際にどの管理策とどの管理策が関連するかといった視点で実施内容を立案してみましょう。

ワークショップ風景



プライバシーに配慮し画像を加工しています

次回のご案内

日時：令和６年９月２４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/