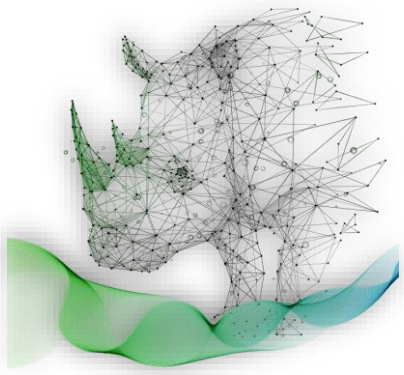
第５回
セミナー・ワークショップ
開催レポート



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２４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５回セミナー・ワークショップが開催されました。

第５回セミナーでは、前回に続き「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４つのカテゴリから「人的管理策」「物理的管理策」「技術的管理策」を取り上げ、講義を行いました。セミナーに続いて実施したワークショップでは、ランサムウェアを防ぐ対策について、上掲の管理策に加え、「組織的管理策」を含め、自社で取組が可能な管理策について選択し、各管理策に基づいた実施内容について検討を行いました。参加者の皆様はセミナーで得た知識や情報を存分に活用し、積極的にディスカッションを行いました。

開催日時と場所

【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
【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 ～ 15:35　ワークショップ（内容説明・個人ワーク）
15:35 ～ 16:30　ワークショップ（グループワーク）
16:30 ～ 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「人的管理策」「物理的管理策」「技術的管理策」のカテゴリ別に説明しました。また、対策を施した後の有効性評価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１６章. 人的対策

第１６章では、「人的管理策」に基づいた対策基準を策定する手順について講じました。「人的管理策」に属する管理策は全 8 項目あり、各管理策の対策基準と実施手順を例示しながら、解説を行いました。

第１７章. 物理的対策

第１７章では、「物理的管理策」に基づいた対策基準を策定する手順について講じました。「物理的管理策」に属する管理策は全 14 項目あり、各管理策の対策基準と実施手順を例示しながら、解説を行いました。さらに本章では、BYOD（個人所有の端末を業務に利用すること）の概念や導入に向けたポイントについて、中小企業の現状を踏まえて説明を行いました。

第１８章. 技術的対策

第１８章では、「技術的管理策」に基づいた対策基準を策定する手順について講じました。「技術的管理策」に属する管理策は全 34 項目あり、各管理策の対策基準と実施手順を例示しながら、解説を行いました。また、実施手順を適用するうえで重要となる「Security by Design」および「ゼロトラスト」の概念について紹介しました。続けて本章では、セキュリティインシデント発生時の対応について説明を行いました。

第１９章. セキュリティ対策状況の有効性評価

第１９章では、セキュリティ対策を実施した結果、効果があったか、目標に近づいているかを判断するための取組である監査について解説しました。

※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/

セミナー参加者の声　※参加者アンケートより一部抜粋

- ✓ 自社で不足している部分の対策について再確認できました。
- ✓ 各管理策の実施手順は、今後の改善に有効だと感じました。
- ✓ セキュリティガイドブックを作成するにあたり、今回の講義は参考になりました。
- ✓ これまでのテーマに比べ人的対策という身近な部分が多く、理解しやすい内容でした。
- ✓ 経営層への人的対策のアプローチとして活用できる内容だと思いました。
- ✓ コストをかけずに実施できる対策や技術的対策とそれ以外の対策とのバランスなど、自社に役立つ話を聞くことができました。

ワークショップ内容

近年、ランサムウェアの被害が後を絶ちません。そこで、今回のワークショップではランサムウェアに対抗する手段について検討を行いました。講師が作成した「実施手順（簡易版）」（次ページ参照）を用いた資料を用い、参加者は提示された３つのテーマについて個人ワークを行った後、グループワークを行いました。活発な意見交換を経て議論を深め、他社事例に触れることで多種多様なノウハウやナレッジを参加者全体が共有するワークショップとなりました。

【ワークショップの進め方】

ゴール設定とテーマ紹介 → 個人ワーク → グループワーク → グループ発表 → 講師のフィードバック

ゴール
グループでの意見交換、協議、発表
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
３つのテーマ
①　実施優先度について 実施手順資料の３つの管理策しか導入できないとしたらどれを選びますか。またその理由も考えてみましょう。どの対策が最も実現可能性が高いか、というのは、事業内容や予算的なものなど、会社によって異なります。自分の会社の場合だったら…という視点で意見交換してみてください。 ※発表時は３つに絞る必要はありません。
②　教育・トレーニングの効果について ランサムウェアから全社員を守るために、どのようなトレーニングや意識向上活動が効果的だと思いますか。メールに対する取り組み方や、リモートワーク環境でのセキュリティについて、皆さんの会社で実施している取組やアイデアを共有しましょう。
③　技術的・非技術的対策のバランスについて ランサムウェア攻撃を防ぐために、技術的な対策が実装できないとき、それに代わる非技術的対策（組織的・物理的・人的）にはどのようなものがあるでしょうか。もしくは、それに代わる会社の取組について考えてみましょう。技術的な対策は一定のコストがかかります。組織的対策や人的対策を組み合わせ、技術的対策をどのように補完し合うかについて意見交換してみましょう。

ワークショップ風景

個人ワークに取り組む参加者

チームで意見交換をしています

検討結果を全体に向けて発表中

プライバシーに配慮し画像を加工しています

＜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

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

【実施手順（簡易版）】

ランサムウェアに対抗するための管理策と実施手順

管理策種別	番号	管理策	概要	実施手順
組織的	5.7	脅威インテリジェンス	脅威に関する情報の収集と分析を通じて、ランサムウェアの新たな手口やトレンドを把握し、適切なリスク軽減策を講じる。	・脅威インテリジェンスの専門家を社員から選任する。 ・外部の脅威インテリジェンスサービスと契約する。 ・月1回の定期的な脅威レポートを受け取り、分析する。 ・新たな脅威が発見された場合、対策を迅速に適用する。
組織的	5.24	情報セキュリティインシデント管理の計画および準備	ランサムウェア攻撃を含むセキュリティインシデントに対する対応手順を計画し、訓練しておく。	・インシデント対応チームを編成し、役割と責任を明確化する。 ・インシデント対応マニュアルを作成し、全社員に配布する。 ・年に1回、シミュレーション演習を実施し、実際の対応力を強化する。 ・発生したインシデントの記録と教訓を共有し、対策を改善する。
組織的	5.29	事業の中断・阻害時の情報セキュリティ	事業継続計画（BCP）にランサムウェア対応を組み込み、攻撃後の業務再開をスムーズに行えるようにする(ISO27002)。	・事業継続計画（BCP）を策定し、ランサムウェア攻撃を含むインシデントに備える。 ・重要な業務プロセスを特定し、継続に必要なITリソースをリストアップする。 ・年に1回、BCPのテストを実施し、必要に応じて改善する。 ・復旧時の優先順位を明確にし、リソースの再配分を計画する。
人的	6.3	情報セキュリティの意識向上、教育および訓練	要員に対して定期的にランサムウェアに関するセキュリティ教育を実施し、フィッシングメールなどの手口に引っかからないように意識を高める。	・半年に1回、社員に対してセキュリティトレーニングを実施する。 ・フィッシングメールの訓練やシミュレーションを行い、社員の対応力を高める。 ・セキュリティに関するポリシー変更があれば即座に全員に通知し、教育を実施する。 ・全社員がセキュリティインシデントに気づいた際に報告できる体制を整備する。
人的	6.7	リモートワーク	リモートワーク環境でもランサムウェアから情報を保護するための対策（VPNの利用、認証強化など）を行い、遠隔地での作業にも安全な基準を適用する。	・リモートワーク用のセキュリティガイドラインを作成し、全員に周知する。 ・VPNや多要素認証の使用を義務付ける。 ・リモート作業環境でのデータ暗号化やアクセス制御の徹底する。 ・3ヵ月に1回、リモートワーク環境のセキュリティ評価を実施し、必要に応じて改善する。
技術的	8.7	マルウェアに対する保護	マルウェア対策ソフトウェアの導入と適切な管理により、ランサムウェアの侵入を防止する。	・全社員が利用するPCに、EDRを導入する。 ・ソフトウェアの自動更新を設定し、常に最新バージョンを維持する。 ・毎日1回、ウイルススキャンをスケジュールする。 ・マルウェア発見時の対処手順を定義し、全社員に周知する。
技術的	8.8	技術的脆弱性の管理	システムやアプリケーションの脆弱性を定期的に評価し、適切なパッチを適用することで、ランサムウェアの侵入経路を遮断する。	・脆弱性スキャンツールを導入し、週に1回、全システムをスキャンする。 ・脆弱性レポートを受け取り、リスクの高いものから優先的に修正を実施する。 ・セキュリティパッチを迅速に適用する体制を構築する。 ・未修正の脆弱性についてはリスク緩和策を実施（アクセス制限など）する。
技術的	8.13	情報のバックアップ	定期的にバックアップを取得し、データを安全な場所に保管しておくことで、ランサムウェアによるデータの暗号化に対応できる。	・データのバックアップポリシーを策定する。 ・重要なデータを毎日バックアップし、リモートサーバーに保存する。 ・バックアップの整合性を月に1回テストし、復元可能か確認する。 ・データ復元手順を確立し、災害時にスムーズに復元できるようにする。
技術的	8.16	監視活動	ネットワークやシステムの異常な動作を監視し、ランサムウェア感染の早期検出と対応を可能にする。	・ネットワークやシステム監視ツールを導入する。 ・不正なアクセスや異常な通信をリアルタイムで監視する。 ・アラートが発生した際の対応手順を定義する。 ・月に1回、監視ログをレビューし、潜在的な脅威を特定する。
技術的	8.20	ネットワークのセキュリティ	ネットワークのセグメンテーションとセキュリティ管理により、ランサムウェアの拡散を防ぐ。	・ネットワークセグメンテーションを実施し、重要なシステムを論理的に分離する。 ・ファイアウォールや侵入防止システム（IPS）の設定を強化する。 ・定期的にネットワーク脆弱性スキャンを実施する。 ・セキュリティポリシーに基づいて、アクセス制御リストを設定する。
技術的	8.24	暗号化の使用	機密データの暗号化を行い、ランサムウェアによるデータの悪用を防止する。	・データの分類に基づいて暗号化ポリシーを策定する。 ・重要なデータの保存、送信時に強力な暗号化アルゴリズムを使用する。 ・暗号鍵の管理体制を整備し、鍵の定期的な更新を実施する。 ・暗号化の適用状況を監査し、適切に運用されているか確認する。

【発表内容（抜粋）と講師コメント】

①　実施優先度について

※多くのチームで選択された管理策について列挙しています。

管理策 No	管理策	選択した理由
5.24	情報セキュリティインシデント管理の計画および準備（組織的）	・インシデントに対応できるようにマニュアル化し、役割の明確化を行うことが重要なため
5.29	事業の中断・阻害時の情報セキュリティ（組織的）	・BCP を明確化することによって、インシデント時の対応をブラッシュアップできるため
6.3	情報セキュリティの意識向上、教育および訓練（人的）	・コストをかけず社内の意識向上につながるため

8.7	マルウェアに対する保護（技術的）	・個人使用端末の業務利用（BYOD）への対応は必須のため
8.13	情報のバックアップ（技術的）	・データ復元は最重要のため ・コストをかけず実施できるため
8.24	暗号化の使用（技術的）	・情報を盗まれた時に備えるため

講師コメント

インシデント発生に備えマニュアルの作成、役割の明確化を行うというのはよい着眼点ですね。マニュアル化する際に情報の流れと連絡先を明記したフロー図を作成し社内に展開することで、誰がどこへ何をするのかを図示することで、従業員が理解しやすいマニュアルとなるでしょう。

② 教育・トレーニングの効果について

取組やアイデアについて
・ 標的型メール訓練の実施と開封率の確認をする ・ 怪しいメールは開かない ・ 月 1 回情報ペーパーを社内に配布する ・ 「会社のためにやらされている」ではなく「自分自身を守る」という意識を持ってもらう ・ インシデント情報を共有する ・ 社外で端末を使用する場合は、許可制とし専用端末を使用する（ VPN の利用 ）

講師コメント

メール訓練についてはそれほどコストがかからずにできるサービスがあるので活用を検討するのもよいでしょう。また、開封率や開封者を確認できるサービスもあります。開封した従業員に対し注意喚起を行っていきましょう。

③ 技術的・非技術的対策のバランスについて

技術的対策が実装できないとき、それを補完する非技術的対策について
【組織的】 • 脅威に関する情報の収集と分析を通じて、ランサムウェアの新たな手口やトレンドを把握し、適切なリスク軽減策を講じる（社員を専任して意識の向上を図る） • ランサムウェア攻撃を受けた時のシミュレーションを実施し、その後の対応力を高める 【人的】 • 基本は技術的対策を実施しエビデンスを残すが、前提としてその技術を社員に理解してもらい不正を働かないように教育する • セキュリティトレーニングの強化の取組を実施する • リモート時のフリーWi-Fi の使用を禁止する 【物理的】 • PC の持ち出しを禁止する

講師コメント

脅威に対抗する方策として情報の収集や分析を行うのは重要です。その際、専任者は社内で毎年変えるようにしましょう。担当変更することにより、新任者にとっては学習の契機となるでしょう。

セミナー・ワークショップ参加後の社内での取組

令和６年７月からスタートした全 10 回のセミナー・ワークショップは、第５回まで実施されました。参加者の皆様には、各回終了後にアンケートへのご協力をお願いしております。中間地点となる今回の開催レポートでは、これまでいただいた貴重なご意見の中から「セミナー・ワークショップの学びを受けて行った社内での取組」についてご紹介します。

- ✓ **セミナー資料や IPA が公開する情報の社内共有**
  「セキュリティ意識を高めるために、セミナーテキストやワークショップで使用した資料を社内に展開しています」
  「セミナーで教示いただいた情報セキュリティ白書 2024 をダウンロードし、社内に共有しました」
- ✓ **社内教育や研修**
  「教育の一環として、インシデント対応訓練の実施が決定しました」
  「セミナーテキストを使って、セキュリティ研修を行いました」
  「標的型メール訓練を実施しました」
- ✓ **情報資産の洗い出しとリスクアセスメント**
  「資産管理台帳の作成に着手しました。台帳完成後、リスク分析を実施する予定です」
  「講義で学んだ内容を活かし、リスクアセスメントの見直しを行いました」
- ✓ **ポリシーの改訂**
  「パスワードポリシーを改訂しました」
  「セキュリティ規程の見直しを実施し、SECURITY ACTION　二つ星の宣言を目指します」
- ✓ **経営層への提言**
  「経営層にセキュリティ対策の重要性について、また、今後実施を検討している施策について提案しました」
  「経営者と今後のセキュリティ対策の社内展開について、話し合う機会を持ちました」
- ✓ **セキュリティ製品の検討および導入**
  「資産管理ツールについて検討を始めました」
  「パソコンの遠隔操作システムを導入し、各パソコンのアップデート状況を確認できる環境が整備されました」

次回のご案内	**日時**：令和６年１０月８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/