第９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

ワークショップにて：参加企業の皆様がプレゼンテーションを行う様子

第９回セミナー・ワークショップ概要

令和５年 12 月 19 日（火）、東京都が主催する「中小企業サイバーセキュリティ対策継続支援事業」の第９回セミナー・ワークショップが開催されました。
セミナーでは、『技術的対策と物理的対策およびセキュリティ対策状況の有効性評価【実施手順・実施者マニュアルレベル③】』をテーマに、ISMS の４つの管理策のうち、「物理的管理策の対策基準策定と実施手順策定」および「技術的管理策の対策基準策定と実施手順策定」に焦点を当て、さらに「セキュリティ対策状況の有効性評価」についても解説が行われました。
ワークショップでは、第７回から続くインシデントハンドリング演習の最終回となりました。前回に引き続き、セキュリティインシデント発生後の対応に焦点を当て、実践的なシナリオを基に、参加者同士で活発な議論が交わされました。

開催日時と場所

【日時】：令和５年 12 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
【アクセス】：JR・私鉄各線 「新宿駅」 西口・南口より 徒歩 5～8 分

＜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９回セミナー内容

テーマ　**技術的対策と物理的対策およびセキュリティ対策状況の有効性評価**
【実施手順・実施者マニュアルレベル③】

講師：星野 樹昭（ほしの しげあき）氏

【物理的管理策】（セミナーテキスト第 16 章）

第 16 章では、物理的管理策の対策基準策定と実施手順策定について学びます。ここでは、物理的なセキュリティ境界、入退場管理、オフィスや施設のセキュリティ、監視、脅威からの保護、セキュリティ領域での作業、クリアデスクポリシー、装置の設置と保護など、実際の対策基準の策定と実施手順策定についての理解を深めます。

【技術的管理策】（セミナーテキスト第 17 章）

次に第 17 章では、エンドポイント機器、アクセス権、情報へのアクセス制限、認証、マルウェア保護、脆弱性の管理、データ保護、バックアップ、ネットワークとアプリケーションのセキュリティなど、技術的な側面に焦点を当て、対策基準の策定から実施手順の策定までをカバーします。また、Security by Design や、ゼロトラスト環境の導入に向けた実施手順の具体例なども紹介し、解説します。

【セキュリティ対策状況の有効性評価】（セミナーテキスト第 18 章）

最後に、第 18 章では、内部監査と外部監査の重要性を理解し、セキュリティ対策の成果と効果を評価する方法を学びます。

このセミナーを通じて、参加者は物理的および技術的セキュリティ対策の基本を学び、自社のセキュリティ環境を強化するための具体的な手順と戦略を身に付けることができます。また、セキュリティ対策の効果を評価し、継続的な改善を図るための方法も学びます。これらの知識とスキルは、現代のデジタル経済において非常に重要であり、参加者が自社のセキュリティポリシーを強化し、リスクを管理するのに役立ちます。

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

セミナー参加者の声

- 物理的、技術的管理策の対策基準を策定したうえでオフィス環境を設計する重要性を理解しました。
- クリアデスク・クリアスクリーンは社内でルール化し導入を進めていきたいと思います。
- 物理的管理策の対策基準は可視化して評価できる内容のため、すぐに着手したいと考えています。
- 物理的管理策の実施手順については、実際に自社オフィスの環境と照らし合わせることでイメージをつかめました。
- ゼロトラストなどの概念や導入することによる有効性を理解できました。
- ゼロトラストを実装するための技術的なツールとして、CASB について知識を得ることができました。
- 社員各人のセキュリティリテラシーに依存しない体制づくりの重要性を理解しました。

第９回ワークショップ内容

テーマ　インシデントハンドリング（事後対応②）～インシデント対応について理解する～

セキュリティ対策において、セキュリティインシデントへの対応が重要です。第 7 回のワークショップでは、事前準備の重要性に焦点を当て、第 8 回では実際のインシデント発生時の適切な対応策を検討しました。第 9 回ワークショップでは、これまでの経験を踏まえ、インシデントが発生した場合の事後対応について掘り下げます。

インシデントハンドリングとは？

インシデントマネジメントの要素の一つにインシデントハンドリングがあります。インシデントハンドリングは、検知/連絡受付、トリアージ、インシデントレスポンス、報告/情報公開の要素で構成されています。（図 1）

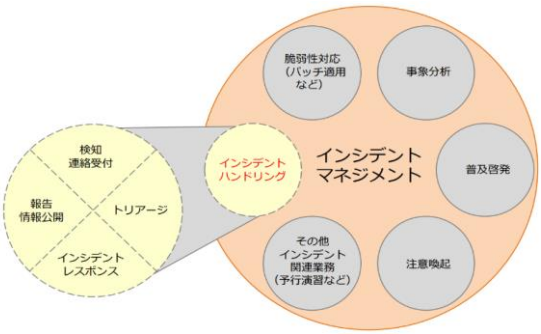

図 1
引用：JPCERT/CC インシデントハンドリングマニュアル

インシデントレスポンス（インシデント対応）とは？

インシデントレスポンスは、①準備　②検知・分析　③封じ込め・根絶・復旧　④事後活動のサイクルが循環しています。（図 2）第９回では、セキュリティインシデントが発生した際の事後活動（赤枠内）に焦点を当てます。

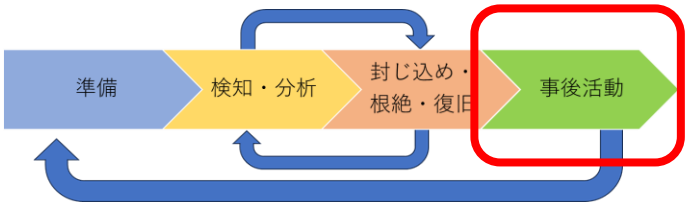

図 2
インシデント対応のライフサイクル（出典：NIST）

■ワークショップの流れ：

1.　講師より本日のワークショップについて説明（５分）

2.　グループディスカッション（90 分）

仮想会社の従業員の PC がランサムウェアに感染した場合のインシデント対応（「検知」「分析」「封じ込め」「根絶」「復旧」）シナリオをもとに、「事後活動」の各フェーズについて議論しました。次のページでは、検討ポイントと参加者の議論の結果の一部をご紹介します。

本議論では、事後処理を通じて組織がインシデントから学び、将来のリスクに対してより良く備えることを目的としています。具体的な改善策とアクションプランを立案することが重要です。

＜事後活動のフェーズ＞

①インシデントレポートの作成 → ②教訓の抽出と共有 → ③セキュリティ対策の見直し → ④従業員トレーニングと意識向上 → ⑤コミュニケーションプランの改善 → ⑥リスク管理プロセスの見直し → ⑦バックアップとデータ復旧戦略の再評価

＜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

① インシデントレポートの作成

検討ポイント	検討ポイントに関する議論の結果
・どのようなレポート内容にするべきか	➢ 被害内容の詳細（種類・日時・被害額等）を記載

② 教訓の抽出と共有

検討ポイント	検討ポイントに関する議論の結果
・インシデントから学んだ主要な教訓 ・改善が必要だった対応内容とその理由 ・今後の対応策の改善にどのように教訓を活用できるか	➢ 社員教育の不足 ➢ 検知システムの不備 ➢ 不審メールに対する社員教育

③ セキュリティ対策の見直し

検討ポイント	検討ポイントに関する議論の結果
・インシデントが露呈したセキュリティの弱点 ・EDR ソフトウェアの導入の効果とその統合方法 ・今後のセキュリティ強化のための追加措置	➢ セキュリティ対策ツールに検知されない攻撃への脆弱性 ➢ EDR とエンドポイントの連携 ➢ OS やソフトウェアのアップデート

④ 従業員トレーニングと意識向上

検討ポイント	検討ポイントに関する議論の結果
・フィッシング対策とセキュリティ意識向上トレーニングの必要性 ・トレーニングプログラムの内容とその実施方法 ・従業員のセキュリティ意識向上のための継続的な取組	➢ 事前予告なしの標的型メール訓練の実施 ➢ インシデント実例を用いたトレーニング ➢ 定期的な社内訓練の実施

⑤ コミュニケーションプランの改善

検討ポイント	検討ポイントに関する議論の結果
・インシデント発生時の内外部コミュニケーションの効果 ・コミュニケーション戦略の弱点と改善策 ・今後の危機管理時のコミュニケーションプランの改善	➢ 取引先への連絡手段の確立 ➢ インシデント用社内緊急連絡網の整備 ➢ セキュリティ担当者不在時の手順書作成

⑥ リスク管理プロセスの見直し

検討ポイント	検討ポイントに関する議論の結果
・リスク評価方法と管理プロセスの有効性 ・インシデント後のリスク管理戦略の更新 ・長期的なリスク管理のための新たな取組	➢ 情報資産管理台帳の見直し ➢ 年に 1 回の内部監査の実施 ➢ サイバー保険加入の検討

⑦ バックアップとデータ復旧戦略の再評価

検討ポイント	検討ポイントに関する議論の結果
・バックアップ戦略の効果と改善点 ・データ復旧プロセスの効率と整合性チェックの方法 ・今後のデータ保護と復旧計画の強化策	➢ 定期的なバックアップの実施 ➢ バックアップ媒体の分散 ➢ ネットワークの分離および復元テストの実施

3. グループ発表と講師からのフィードバック（40 分）

ワークショップは A～F の 6 チームで実施され、各グループは検討の過程や結果をスクリーンへ投影しながら発表しました。講師は各グループの発表に対して具体的なフィードバックを提供し、第 7 回以降の振り返りとして、「事前準備の重要性」、「コミュニケーションプランの改善」、「インシデントを活かした振り返りと見直しの必要性」に言及しました。これにより、参加者はインシデントレスポンスについての理解を一段と深めました。

ワークショップ参加者の声

第 7 回から全 3 回にわたって、インシデント対応の一連の流れを体験した参加者の皆様から寄せられた声をご紹介します。

- 事前準備でインシデント対応計画の策定を体験し、インシデントが発生する前に、ポリシーや計画を策定する必要を理解しました。インシデント発生後の対応手順を検討した際は、メンバー全員の知識を結集しアイデアを出しました。事後対応のフェーズでは、実際に発生したインシデントを教訓にして対応策を検討する方法を学びました。
- インシデントレスポンスの全体像を学んで感じたことは、事前準備の大切さでした。いざという時に慌てないためにも、計画策定に取り組み、社内に展開していきたいと思います。
- 実際にインシデントが発生した後の対応が曖昧でしたが、ワークを通じて検知から復旧まで段階ごとに行う対策が理解できました。また事後対応についてはこれまで検討したことがなかったので、今回のワークショップがよい経験となりました。
- インシデント対応の次の準備へつなげるために、インシデントの事後活動として、レポート作成の重要性を理解しました。

運営事務局より編集後記

年末の訪れとともに、都心の街はイルミネーションで輝く季節となりました。街路に敷き詰められた落ち葉が冬の到来を感じさせます。

全 10 回のセミナー・ワークショップの 9 回目が終了し、残すはあと 1 回となりました。これまで継続してご参加いただいている皆様に心より感謝申し上げます。

サイバー攻撃の手法やサイバーセキュリティにおける脅威は日々進化しています。中小企業のセキュリティリスクを軽減し、セキュリティ体制を強化するため、当事業では引き続きセミナー・ワークショップの開催、セミナー資料の Web サイト公開などを通して、セキュリティ対策に関する情報を広く普及・発信していきます。

12 月の風景『街路樹にきらめくイルミネーション』

運営事務局一同

次回（第 10 回）セミナー・ワークショップのご案内

日時：令和 6 年 1 月 23 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：全体総括～これまでのセミナー・ワークショップの振り返り～

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