第８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

第８回セミナー・ワークショップ概要

令和５年 11 月 28 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８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、『組織的対策と人的対策【実施手順・実施者マニュアルレベル②】』をテーマに、ISMS の４つの管理策のうち、「組織的管理策の対策基準策定と実施手順策定」および「人的管理策の対策基準策定と実施手順策定」について解説が行われました。その後のワークショップでは、前回のインシデント対応計画策定に続き、インシデントハンドリング演習の第２回目が行われ、セキュリティインシデント発生後の具体的な対応を検討することで、実践的な知識とスキルを身につけました。

開催日時と場所

【日時】：令和５年 11 月 28 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

第８回セミナー内容

テーマ　**組織的対策と人的対策【実施手順・実施者マニュアルレベル②】**

講師：星野 樹昭（ほしの しげあき）氏

【組織的管理策】（セミナーテキスト 第１４章）

第 14 章では、情報セキュリティ方針に基づく組織的な対策基準と実施手順の策定に焦点を当てます。具体的には、情報セキュリティの方針群、役割と責任の明確化、職務の分離、経営陣の責任、関係当局との円滑な連携などについて学びます。さらに、脅威インテリジェンス、プロジェクトマネジメント、情報の分類とラベル付け、情報伝送、アクセス制御などの重要な側面にも触れます。

【人的管理策】（セミナーテキスト 第１５章）

第 15 章は、人的管理策を中心に展開されます。ここでは、人材選考、雇用条件、情報セキュリティの意識向上、教育及び訓練、懲戒手続き、雇用の終了、秘密保持契約、リモートワーク、情報セキュリティ事象への報告などの要素が取り上げられます。

各章では、対策基準を策定する手順と、それらを実施する方法について解説を行います。本セミナーは、情報セキュリティの脅威に対する企業の準備と対応を強化することを目的としており、参加者は組織的および人的管理策の両方において、実践的なスキルと知識を習得することができます。

※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

- 組織的管理策、人的管理策を参考にした対策基準と実施手順について理解を深めました。
- データのアクセス権を見直すよい機会となりました。
- 自社のセキュリティ対策基準の見直すべき箇所に気づきました。
- 対策基準に対する実施手順を具体的に学ぶことができ、実務に役立つ知識を得られました。
- 実用的な対策基準と実施手順の策定例により、作り方の理解が深まりました。
- 紹介された各項目の対策基準と実施手順の例は自社で策定する際の参考になります。
- 自社に合ったドキュメントを作成し、作成したドキュメントを活用するイメージが広がりました。
- 明文化されていなかったルールについて、ドキュメント化する必要性を感じました。テキストに載っていた実施手順例を自社にカスタマイズして、規程作成に役立てます。
- ISMS をフレームワークとして利用し対策基準、実施手順を策定する方法が明確になりました。
- インシデント発生に備えるために必要な人的対策の内容について理解を深めました。
- 対策基準や実施手順の策定には多くの手順が必要であることを理解しました。
- 規程の見直しをしていたところで、ISMS の主旨と手順、セミナーのポイントを確認しながら勉強できました。

第８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①）～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。前回のワークショップでは、「準備」のフェーズとして、インシデント対応計画を策定しました。第 8 回では、実際にインシデントが発生した場合の対応について検討します。

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）

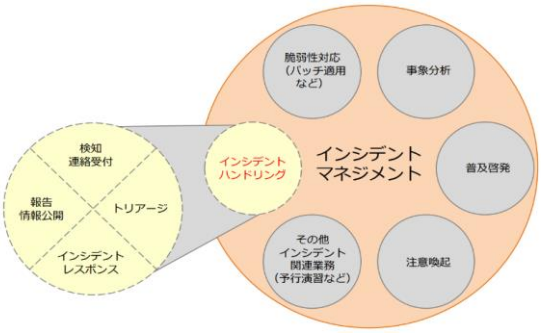

図 1
引用：JPCERT/CC インシデントハンドリングマニュアル

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 8 回では、セキュリティインシデントが発生した際の対応（赤枠内）に焦点を当てます。

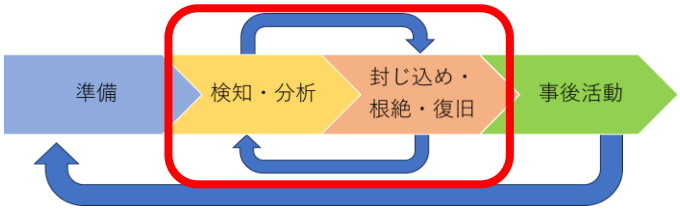

図 2
インシデント対応のライフサイクル（出典：NIST）

■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）

自組織のサーバや従業員が使用しているパソコンがランサムウェアによって暗号化された場合を想定し、「検知」、「分析」、「封じ込め」、「根絶」、「復旧」の各フェーズにおいて、どのような対応をするか検討しました。フェーズごとに、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。

Phase ：「検知」

このフェーズは、従業員が異常な PC の動作を報告し、IT チームが通知を受けるところから始まりました。

検討ポイント	検討ポイントに関する議論の結果
・どのような兆候がランサムウェア感染を示すか？	➢　不審メールに添付されたファイルの拡張子の変化
・初期対応としてどのようなステップを踏むべきか？	➢　ネットワークから切り離す

Phase ：「分析」

このフェーズでは、攻撃の範囲と影響を評価します。

検討ポイント	検討ポイントに関する議論の結果
・攻撃の範囲をどう特定するか？	➢ 社内へ情報共有し同じ事象の発生有無を確認
・感染経路と攻撃者の特定方法は？	➢ 不審メールの送受信元の確認

Phase ：「封じ込め」

このフェーズでは、感染したシステムを隔離し、拡散防止に努めます。

検討ポイント	検討ポイントに関する議論の結果
・どのようにシステムを安全に隔離するか？	➢ ネットワークを感染有無で切り分ける
・通信の制御とデータの保護方法は？	➢ 自動バックアップの停止

Phase ：「根絶」

このフェーズは、ランサムウェアの除去とセキュリティの強化に努めます。

検討ポイント	検討ポイントに関する議論の結果
・マルウェアの根絶方法は？	➢ ネットワーク、システム構成の見直し
・今後の攻撃を防ぐための対策は？	➢ 脆弱性の解消

Phase ：「復旧」

このフェーズは、データとサービスの復旧、事業の正常化に努めます。

検討ポイント	検討ポイントに関する議論の結果
・データ復旧の最善策は？	➢ 有効なバックアップの取得
・復旧後のリスク評価とレビュー方法は？	➢ 発生した事象を事例として教育に活用

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～E の 5 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内容について、着眼点や発想の独自性、改善点に関するフィードバックを提供し、参加者はそれを通じてインシデントレスポンスの理解を深めました。

運営事務局より編集後記

11 月下旬になり、木々の葉が紅や黄色に色づき、秋の深まりを感じる季節となりました。

全 10 回のセミナー・ワークショップの 8 回目を終え、参加者の方からは、「回を重ねるごとに理解が深まっています」「知識がスパイラルしていって定期的なカリキュラムの効果を実感しています」などのお声をいただいております。

残り 2 回となりましたセミナー・ワークショップも、参加者の皆様にとって有意義なものとなるよう改善しながら運営をしてまいります。

今回のセミナーでは具体的な規則としての「対策基準」、方法としての「実施手順」について学びました。また、ワークショップでは、セキュリティインシデントの事後対応の演習を行い、組織として必要な対応について議論を重ねました。

当事業では、セミナー・ワークショップの開催やセミナー資料の Web サイト公開などを通して、引き続きセキュリティ対策に関する情報の普及・発信に努めて参ります。

運営事務局一同

１１月の風景 『深紅に色づくイロハモミジ』

次回（第９回）セミナー・ワークショップのご案内

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
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】

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