# 第 10 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 10 回セミナー・ワークショップ概要

令和 6 年 1 月 23 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 10 回セミナー・ワークショップが開催されました。この事業は、基本的なセキュリティ対策を実施した中小企業に対し、次のステップに進むためのサポートを行うことで、中小企業のセキュリティ人材の育成と体制強化を目指しています。今回は、昨年 7 月から開始したプログラムの最終回となり、「全体総括」として、第 1 回から第 9 回までの内容を振り返りました。

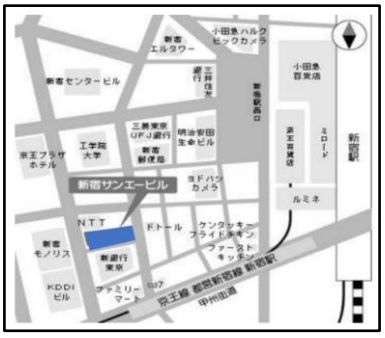
セミナーでは、各回で学んだポイントをピックアップして解説し、重要な知識を定着させ、さらに今後継続して実施すべきアクションについて解説しました。

ワークショップで発表される参加者の方

ワークショップでは、第 9 回までのワークの内容をグループで振り返り、参加企業同士の情報交換や他社の成功事例から知見を共有し、サイバーセキュリティ対策の自走に向けたディスカッションが行われました。

## 開催日時と場所

【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
【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**
15:00 ～ 15:15 ： 休憩
**15:15 ～ 17:25 ： ワークショップ**
17:25 ～ 17:30 ： 運営事務局からのご挨拶

＜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 10 回セミナー内容

## 全体総括

講師：星野 樹昭（ほしの しげあき）氏

**【総括編】（セミナーテキスト第 19 章）**

第 10 回のセミナーでは、「全体総括」として、第 1 回から第 9 回までのセミナー内容を振り返り、重要な知識の定着と今後のセキュリティ活動の推進に向け、必要な考え方を理解することを目的としています。各章のポイントを振り返り、テキストの活用方法について解説します。各章の重要なポイントを再確認することで、その概要を理解することができます。また、本テキストに記載された実施手順を活用し、自組織でセキュリティ対策を実践するために必要な考え方や参考文献を把握することができます。情報セキュリティ担当者、情報システム管理者、経営者など、それぞれの立場で本テキストをどのように活用すべきか説明します。

テーマは、「テキスト活用のポイント」と「これまでの振り返り」に分かれており、テキストの活用ポイントでは、「DX の理解から対策の実践まで」の重要性を再認識し、経営者と情報共有、経営者のリーダーシップで社内体制を整え、具体的なアクションにより実践していくことを解説します。
「これまでの振り返り」では、テキストの第 1 章から第 18 章までの内容を取り上げ、デジタル時代の社会と IT 情勢、重大なインシデントから学ぶ事例、サイバーセキュリティの基礎知識、企業経営と IT 投資、デジタル社会の方向性、サイバーセキュリティ戦略、セキュリティフレームワーク、リスクマネジメントなど、広範囲なトピックにわたる内容を振り返ります。各章では、主なキーワード、全体概要、訴求ポイントを明確にし、章を通じての気づきや学び、実施概要の認識を深める説明をします。

このセミナーを通じて、参加者は情報セキュリティの全体像を把握し、自組織でのセキュリティ対策の実践に向けた準備を整えることができます。今後のセキュリティ活動において自走するための基礎となるこの機会を、ぜひ有効活用してください。

**※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/**

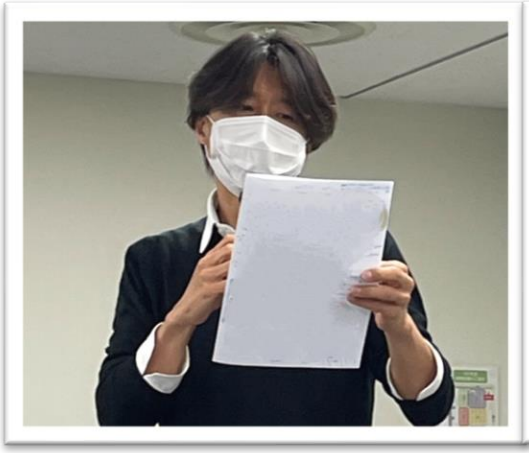
# 第 10 回ワークショップ内容

## 今後の改善点やワークショップ内でのメリット・デメリットを共有し、今後の情報セキュリティ対策に活かそう

これまでのワークショップを振り返り、次の 3 つの観点で意見交換しました。

1. ワークショップの回ごとに、得られた点や組織のセキュリティ活動に役立つと思われる点について。
2. どのテーマの回が、最も皆さんの組織の直近のセキュリティ活動で役に立っているか。
3. どのテーマの回が、最も皆さんの組織の今後のセキュリティ活動に役立ちそうか。

## 全ワークショップの内容と参加者のフィードバック



参加者の皆様は、特に印象に残った回やテーマ、そしてセミナー・ワークショップで得た知識やスキルを活かし、社内で取組んだ成果や今後実施予定の対策について共有しました。

**第１回**

**・自社で活用している IT 及び実施できているセキュリティ対策とセキュリティ課題について整理し、今後取組み可能なセキュリティ対策について検討する。**

**自社のセキュリティ対策の実情について他社と情報交換できたことが役立ちました。**

**第２回**

**・仮想会社の攻めと守りの IT 活用シナリオを基に、IT 活用のチャレンジやリスク、セキュリティ対策やプライバシー対策について検討する。**
**・仮想会社のデジタル化の現状と課題を基にデジタル戦略、セキュリティ対策、実行計画の作成について検討する。**

**第３回**

**・仮想会社の脆弱性について、10 大脅威ごとにまとめられた脆弱性を基に、対策を講じる対象となる脅威を選択し、その影響と対応策を検討する。**

**10 大脅威とその対策例は、具体的な脆弱性を理解するうえで役立ちました。**

**第４回**

**・第３回で用いた 10 大脅威対策例の中から、選択した対策例を確認し、それぞれの対策例がどの管理策に当てはまるかを議論し、その項目に当てはまる管理手順を記載する。**

**フレームワークの活用方法が参考になりました。**

**第５回**

**・仮想会社のシナリオを基に、情報資産管理台帳作成に取組み、評価値と重要度を検討する。**

**情報資産の洗い出しと重要度の見極めのワークで新しい知識を獲得できました。自社の情報資産管理台帳の作成に役立てたいと思います。**

**第６回**

**・仮想会社の情報資産管理台帳に対し、対策方針を選択し、方針に沿った具体的な対策内容を検討する。**

**４つの対策方針「回避」「低減」「移転」「受容」があることを学びました。中でも「移転」の対策が実業務で役立ちました。情報資産に対し、リスクアセスメントを行い、優先順位をつけることで、高いものから対策をしていこうと思っています。**

**第７回**

**・インシデントレスポンスポリシーのサンプルを基に、インシデントレスポンス計画を策定する。**

**第８回**

**・仮想会社がランサムウェアに感染したという想定に基づき、インシデントレスポンスの各フェーズについて対応策を検討する。**

**第９回**

**・インシデント発生後の「事後対応」の各フェーズについて検討する。**

**第 7 回から第 9 回で演習したインシデントレスポンスは、ランサムウェア攻撃を受けた際の具体的なイメージがつかめ、インシデントに対して心の準備ができました。ワークで得た知識を活かしてインシデント対応計画をブラッシュアップしていきます。**

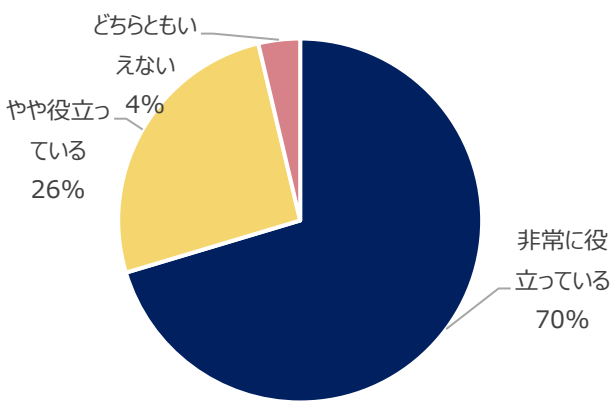
**講師より**

全 9 回のワークを通じて、自社のセキュリティ状況や対策への理解が深まったかと思います。また優先順位の付け方や実践的な対策に触れることで、セキュリティの脅威に対して全て対策するのではなく、自社の環境や事業内容に沿った現実的な対応策を取ることが重要であることを示しました。セキュリティ対策を実施するうえで重要なことは「セキュリティに対する経営層の理解」「セキュリティ担当者一人でなくチームでの取組」「PDCA サイクルの運用」です。「リスクは生もの」であるという認識を常に持って、継続的な取組を実施し、今後のセキュリティリスクに備えていきましょう。

## セミナー・ワークショップ参加者の声

セミナー・ワークショップ終了後、参加者の皆様にご協力いただいたアンケートより、ご意見の一部をご紹介します。

### Q.セミナー・ワークショップを通じて得た知識やスキルは、現在の業務にどれだけ役立っていますか？




**「非常に役立っている」と回答した方のご意見**

- セミナーを通じて、情報セキュリティにおける課題や対策方法が明確になりました。
- インシデント発生時の事後対応について学び、今後のセキュリティ強化計画を立てることができました。
- セキュリティ意識が向上し、自社で必要な対策を見極める力が身につきました。
- 専門用語の理解や社内規程の整備、情報資産の管理方法など、具体的なスキルが向上しました。
- 学んだ知識を積極的に活用し、情報セキュリティを強化していく意欲が高まりました。

＜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

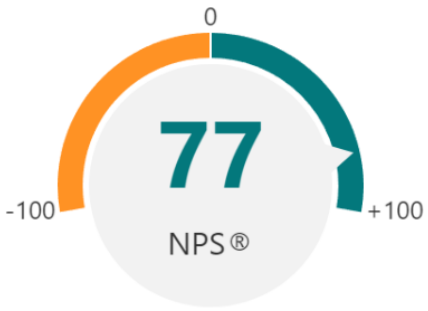
**「やや役立っている」と回答した方のご意見**

- 具体的なセキュリティ対策として、資産管理ソフトの導入などを行い、対策の強化を実現しています。
- 他社の EDR や資産管理ソフトの導入事例を参考にし、自社でも EDR の導入を進めています。
- システム選定時にセキュリティ要件を考慮することやログの取得など、セキュリティに対する感度が向上しました。

**「どちらともいえない」と回答した方のご意見**

- 現在はまだ活用機会が限られますが、今後セキュリティに力を入れていく中で、学んだ知識を活かしたいです。

## Q.本セミナー・ワークショップを、本事業へ参加していない他社などへ、どのくらいおすすめしたいと思われますか？




NPS（Net Promoter Score）：質問に対し、0 から 10 点の 11 段階で回答を求め、その得点に基づいて、回答者を「批評者（0 から 6 点）」「中立者（7 から 8 点）」「推奨者（9 から 10 点）」の 3 つのカテゴリーに分類します。「推奨者」の割合から「批判者」の割合を引いた値が、NPS として示されます。

参加者ご意見より

- 体系的な学びと他社の意見を聞けることで、大変勉強になりました。セキュリティ対策に関する知見を得て、モチベーションも向上しました。
- セミナーだけでなく、フォローアップも手厚いと感じます。中小企業ではセキュリティの重要性は認識されていますが、実行に移すことが難しい場合もあります。このセミナーを通じて、自走できる知識を得ることができました。
- 最初は自分だけが知識不足だと思っていましたが、周囲も同じようで安心しました。
- 私は社長であり、情報システム担当者もいないため、ICT 対応者としても参加しました。両立場から見て、このセミナーは会社の情報セキュリティ対策に役立つと感じました。情報システム担当者だけでなく、社長も参加すべきだと思います。

## 運営事務局より編集後記

令和 6 年、新しい年が幕を開けました。寒さが続く中で冬の花は澄み渡る空に向かい、凛として花を咲かせています。

全 10 回のセミナー・ワークショップは、今回をもちまして終了いたしました。これまで長きにわたり、ご参加いただきました皆様に心より御礼申し上げます。また、運営にご協力いただいた全ての方に感謝申し上げます。

Society5.0 に向け、社会のデジタル化が進展するなか、ビジネスにおけるサイバー攻撃のリスクは日々増しています。IT の世界は日進月歩であり、絶えず社会情勢は変化していきます。そこで、セキュリティ対策もアップデートが必要です。適切な PDCA サイクルの運用が、対応力の向上や社内体制の強化につながります。

1 月の風景『厳寒に咲くロウバイ』

今後も当事業では、中小企業のセキュリティリスクの軽減やセキュリティ対策の自走に向け、情報の普及・発信に努めて参ります。

## 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