第６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６回セミナー・ワークショップ概要

令和５年 10 月 24 日（火）、東京都主催の「中小企業サイバーセキュリティ対策継続支援事業」の第６回セミナー・ワークショップが開催されました。

第６回セミナーでは、リスクマネジメントに焦点を当て、その概要やリスクマネジメントプロセスにおける重要な要素について学びました。参加者はリスクアセスメントの手法やリスク対応の考え方について理解を深め、サイバーセキュリティの現状に対処するための戦略を習得しました。

さらに、ワークショップでは理論を実践に移す機会が提供されました。参加者は仮想会社のシナリオを通じて、実際の情報資産に対するリスクの特定と評価を行い、特定したリスクに対する優先度づけやリスク対応策の検討を行いました。この実践的なアプローチは、参加者にとって抽象的な概念を具体的な行動に結びつけ、セキュリティ対策の実施に向けたスキル向上を促進しました。

開催日時と場所

【日時】：令和５年 10 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：　第６回セミナー**　※途中５分間休憩あり
  （　休憩　）
- **15:15 ～ 17:25：　第６回ワークショップ**
  - 15:15 ～ 16:40：　グループディスカッション
  - 16:40 ～ 17:25：　グループ発表と講師からのフィードバック
- **17:25 ～ 17:30：　運営事務局からの連絡**

＜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６回セミナー内容

テーマ **セキュリティリスク評価及び対策基準に記載されるべき管理策【対策基準レベル②】**

講師：星野 樹昭（ほしの しげあき）氏

【リスクマネジメント】（セミナーテキスト 第 11 章）

第６回セミナーでは、リスクマネジメントの概要を学び、組織が取るべき具体的なステップを理解することを目的としています。この過程において、リスクアセスメントの手法やそれに続くリスク対応の適切な考え方が含まれます。参加者がこのプロセスを通じてリスクマネジメントの意義を深く理解し、組織全体でセキュリティを強化することがゴールです。

まず最初に、「リスクマネジメント」とその重要な３要素について解説します。また、国際標準である ISO/IEC 27005 に基づく情報セキュリティリスクマネジメントの枠組みについて、その手順と基準の確立方法を学びます。

特に重要なのは、リスク特定のアプローチです。このセクションでは、異なる手法の特徴や、それぞれのメリット・デメリット、そしてリスク所有者の特定方法について説明します。実際の情報資産の洗い出し例をもとに、資産目録を効率的に作成する方法についても触れます。

さらに、機密性、完全性、可用性が損なわれた場合の具体的な影響度の評価方法を解説し、これに基づいたリスクの重要度の判断方法を学びます。リスク分析の実例を通じて、被害の発生可能性やその影響の評価、そして最終的なリスク評価についても詳細に見ていきます。

最後に、リスク対応プロセスに焦点を当てます。リスクに対する様々な対応選択肢と、それらをどのように選定し、実行するかについての具体的なステップを学びます。残留リスクについても触れ、組織がこれをどのように理解し、受け入れるかの基準についても話します。

※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/

第６回ワークショップ内容

テーマ **リスクの特定・評価について理解し対策案を立てられるようになる**

第５回ワークショップでは、情報処理推進機構（IPA）が提供するリスク分析シート[1]を使用して、情報資産管理台帳を作成しました。第６回ワークショップでは次のステップとして、作成した台帳を基に守るべき情報資産に対するリスク対策を考えます。

[1] IPA「中小企業の情報セキュリティ対策ガイドライン」付録７： リスク分析シート https://www.ipa.go.jp/security/keihatsu/sme/guideline/

情報資産管理台帳（サンプル）

業務分類	情報資産名称	利用者範囲	管理部署	媒体・保存先	個人情報の種類			評価値			重要度
					個人情報	要配慮個人情報	特定個人情報	機密性	完全性	可用性	
法務	契約書	法務部	法務部	書類				3	2	1	**3**
法務	法的通知	担当者	法務部	事務所PC				2	3	1	**3**
製造	製品設計図	設計部	設計部	社内サーバー				3	3	3	**3**
製造	原材料在庫データ	製造部	製造部	社内サーバー				1	3	2	**3**
製造	工場の安全手順書	担当者	安全管理部	書類				1	3	3	**3**
製造	製造機器メンテナンスログ	製造部	製造部	書類				1	3	2	**3**
製造	生産スケジュール	製造部	製造部	社内サーバー				1	3	3	**3**
製造	廃止された製品のカタログ	営業部	製造部	書類				1	1	1	**1**
人事	従業員名簿	人事部	人事部	社外サーバー	有	有	有	3	3	2	**3**
人事	社内ポリシー	従業員	人事部	書類				1	1	2	**2**

（出典）IPA「中小企業の情報セキュリティ対策ガイドライン」付録 7 リスク分析シートを基に作成

■ワークショップの流れ：

1. グループディスカッション（85 分）

※当日使用したドキュメントは、別添「資料 1　情報資産管理台帳（サンプル）」を参照ください。

検討手順

① リスク対策を実施する資産に対し、優先順位をつける

② 優先順位の高い順から、対策の方針（「回避」、「提言」、「移転」、「受容」から選択）を決める
※詳細は、セミナーテキスト第 11 章-15、16 ページを参照ください。
・対策方針は一つとは限りません。様々な視点から考えることが重要です。

③ 選択した方針に合った具体的な対策内容を考える
・会社や組織の特性や業務に合わせて、最適な対策方針と具体的な対策内容を立案しましょう。
・リスクが高い情報資産だけでなく、実際の業務に応じて検討を行い、取捨選択を行いましょう。

2. グループ発表と講師からのフィードバック（45 分）

ワークショップは 5 名ずつに分かれて A～F の合計 6 チームで実施しました。各グループは独自のアプローチでリスク対策の検討に取り組み、その成果をグループ発表で共有しました。発表では、各グループの発表担当者が検討の過程や結果をスクリーンへ投影しながら、全体へ具体的な提案を伝えました。

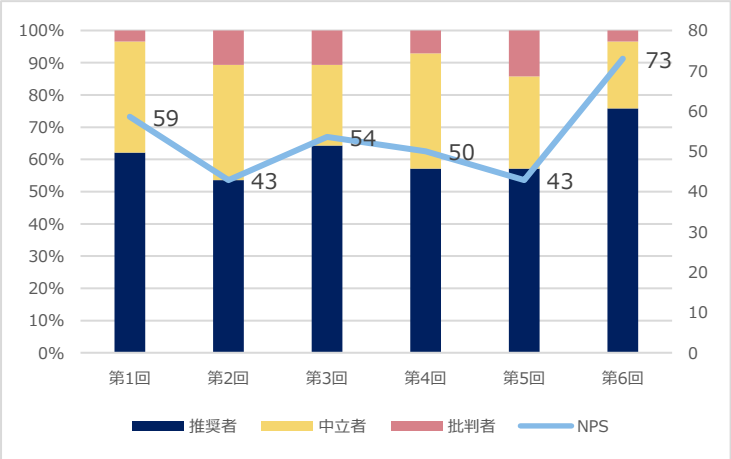
また、各グループに対して講師からフィードバックがあり、提案の妥当性や実現可能性について、参加者は理解を深めることができました。

グループ発表の様子

参加者の声

令和 5 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、すでに第 6 回までが実施されました。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。折り返しとなる第 6 回の開催レポートでは、これまで頂いた貴重なご意見の一部をアンケート結果よりご紹介いたします。

■NPS の推移



NPS（Net Promoter Score）は、特定のサービスや商品に対する顧客のロイヤルティを測るための指標です。このスコアは、推奨者の割合から批判者の割合を差し引いたものであり、プラスのスコアは推奨者が優勢であり、サービスが高く評価されていることを示しています。

（参加者の声）

- **具体的なサイバーセキュリティ対策を進められそう**
  セミナーでは理論だけでなく、具体的な手順や実践的な方法が示され、実際の業務に取り組む手助けになりました。
- **多くの企業にとって確実にプラスになる**
  セキュリティ対策は企業規模や業界に関係なく、確実にプラスの影響をもたらすことを実感しています。
- **回を追うごとに理解が深まり、分からないことが少しずつ分かるようになってきた**
  繰り返しのセミナーで学びを深め、漠然とした不安感が確実に少なくなりました。
- **セキュリティを何からやったらいいかわからない、という人には手掛かりがつかめていいと思う**
  セミナーは初心者にもわかりやすく、具体的な手がかりが提供され、取り組みやすくなりました。
- **他社の状況を聞くことにより、自社の取組を客観的に見ることができた**
  他社の経験や課題から学ぶことで、自社のセキュリティ対策の立ち位置を確認し、改善の方針を見出せました。

■セミナー・ワークショップの内容を受けて社内でやってみたこと

- **経営層へのリスク説明と方針決定：**
  「セミナー参加を通じて、社内で進まないセキュリティ対策について、取締役にリスク説明をし、トップダウンでの進め方を増やしていくことに成功しました。」
- **セキュリティ教育とパスワード強化の実施:**
  「セキュリティ教育を通じて得た知識を活かし、社員に向けてパスワードの複雑化や変更に関する指導を行いました。」
- **セキュリティ教育とスキルアップの同時進行:**
  「セキュリティ教育を受講する一方で、自身のスキルアップを目指して IPA や NISC の教育プログラムを受講し、情報セキュリティマネジメント試験の合格を目指しています。
- **業務プロセスの改善と電子化の検討:**
  「DX 化の一環として、業務プロセスを洗い出し、請求書の電子化を検討しテスト中です。」
- **セキュリティ対策の見直しと ISO/IEC27002:2022 の活用:**
  「セキュリティ対策の見直しにおいて、ISO/IEC27002:2022 を参考にして、必要な管理策や目的を検討しています。」

- **セキュリティインシデントの一元管理表の導入:**
  「セミナーで学んだことを活かし、セキュリティインシデントやヒヤリハットの一元管理表を作成し、社内での情報共有を始めました。」
- **VPN 設定見直しとセキュリティ脆弱性のチェック:**
  「VPN の設定を見直し、セキュリティ脆弱性のチェックと対応を行い、自社ホームページのセキュリティ向上に取り組みました。」
- **セキュリティポリシー策定とベンダー管理の確認:**
  「セキュリティポリシーの策定やベンダーとの責任所在の確認を進め、セミナーの主旨を社内で共有しました。」

運営事務局より編集後記

10 月も半ばが過ぎ、新宿の街路樹が少しずつ色づきはじめました。本格的な秋の訪れを感じる中、第 6 回セミナー・ワークショップが開催されました。

本セミナー・ワークショップは全 10 回の連続したプログラムとなっております。今回の開催レポートでは、これまで参加者の方からアンケートで寄せられた声を紹介しています。
これまでのセッションで得られた洞察や参加者のフィードバックは、今後のセミナー・ワークショップの展開において非常に貴重な情報となっております。
皆様方のご協力に心より感謝申し上げます。

セミナー・ワークショップは残すところ 4 回となりましたが、参加者の皆様にとって有意義なものとなりますよう、引き続き創意工夫を重ねて運営してまいります。

また、事業 Web サイトでのセミナー資料の公開やサイバーセキュリティ情報の発信を通して、中小企業のセキュリティ強化に向け、今後も取り組んでまいります。

運営事務局一同

10 月の風景 『水鏡に映る木々』

次回（第 7 回） セミナー・ワークショップのご案内	**日時**：令和 5 年 11 月 14 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**：組織として実施すべき具体的な対策事項・手順 【実施手順・実施者マニュアル レベル①】

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

資料１　情報資産管理台帳（サンプル）

（出典）IPA「中小企業の情報セキュリティ対策ガイドライン」付録7リスク分析シートを基に作成

業務分類	情報資産名称	利用者範囲	管理部署	媒体・保存先	個人情報の種類			評価値				現状から想定されるリスク（入力不要・自動表示）						手順①	手順②
					個人情報	要配慮個人情報	特定個人情報	機密性	完全性	可用性	重要度	脅威の発生頻度 ※「脅威の状況」シートに入力すると表示	脆弱性 ※「対策状況チェック」シートに入力すると表示	被害発生可能性		リスク値		優先順位	対策方針
法務	契約書	法務部	法務部	書類				3	2	1	**3**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大		
法務	法的通知	担当者	法務部	事務所PC				2	3	1	**3**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大		
総務	社内行事の写真集	従業員	総務部	社外サーバー				1	1	1	**1**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	2	リスク小		
製造	製品設計図	設計部	設計部	社内サーバー				3	3	3	**3**	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	3	リスク小		
製造	原材料在庫データ	製造部	製造部	社内サーバー				1	3	2	**3**	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	3	リスク小		
製造	工場の安全手順書	担当者	安全管理部	書類				1	3	3	**3**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大		
製造	製造機器メンテナンスログ	製造部	製造部	書類				1	3	2	**3**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大		
製造	生産スケジュール	製造部	製造部	社内サーバー				1	3	3	**3**	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	3	リスク小		
製造	廃止された製品のカタログ	営業部	製造部	書類				1	1	1	**1**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	2	リスク小		
人事	従業員名簿	人事部	人事部	社外サーバー	有	有	有	3	3	2	**3**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大		
人事	社内ポリシー	従業員	人事部	書類				1	1	2	**2**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4	リスク小		
人事	従業員の出勤簿	人事部	人事部	書類				1	2	2	**2**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4	リスク小		
人事	社員の趣味リスト	人事部	人事部	書類				1	1	1	**1**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	2	リスク小		
購買	仕入れリスト	購買部	購買部	書類				1	2	1	**2**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4	リスク小		
研究開発	製品開発計画書	開発部	開発部	書類				2	2	1	**2**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4	リスク小		
経理	会計レポート	経理部	経理部	社内サーバー				3	3	1	**3**	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	3	リスク小		
経理	領収書	経理部	経理部	書類				1	2	1	**2**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4	リスク小		
経理	経費報告書	経理部	経理部	書類				1	2	1	**2**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4	リスク小		
経理	財務監査報告書	経理部	経理部	書類				3	3	1	**3**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大		
経理	古い経費報告のコピー	経理部	経理部	書類				1	1	1	**1**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	2	リスク小		
開発	ソフトウェアコード	開発部	開発部	社外サーバー				3	3	2	**3**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大		
開発	テスト結果	品質保証部	品質保証部	社内サーバー				1	3	1	**3**	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	3	リスク小		
営業	顧客データベース	営業部	営業部	社外サーバー	有			3	2	2	**3**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大		
営業	営業戦略資料	営業部	営業部	社内サーバー				2	2	1	**2**	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	2	リスク小		
営業	営業会議の議事録	営業部	営業部	社内サーバー				1	2	1	**2**	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	2	リスク小		
マーケティング	市場調査報告	マーケティング部	マーケティング部	社外サーバー				1	2	1	**2**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4	リスク小		
マーケティング	古い広告草案	マーケティング部	マーケティング部	書類				1	1	1	**1**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	2	リスク小		
カスタマーサービス	サービス履歴	サービス部	サービス部	社外サーバー	有			3	3	3	**3**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大		
カスタマーサービス	顧客対応履歴	サービス部	サービス部	社内サーバー	有			3	3	3	**3**	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	3	リスク小		
IT	システムバックアップ	IT部	IT部	可搬電子媒体				3	3	3	**3**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大		
IT	アクセスログ	IT部	IT部	社内サーバー				2	3	1	**3**	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	3	リスク小		
IT	ソフトウェアライセンス	IT部	IT部	書類				2	2	1	**2**	3:通常の状況で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4	リスク小		