

第5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

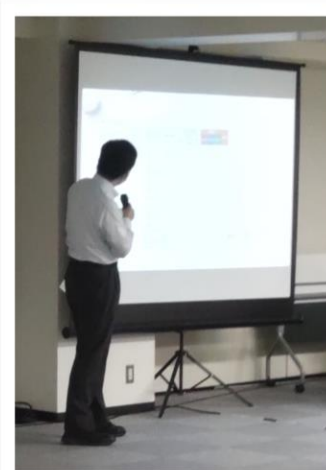
第5回セミナー・ワークショップ概要

令和5年10月10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、組織での情報セキュリティ対策を計画し、実施するために必要な知識とスキルを身につけることを目的に、セキュリティポリシーの概要、サイバーセキュリティ対策のアプローチ方法、ISMSの管理策の概要、リスクマネジメントに関する用語について学びました。



ワークショップでは、情報資産管理台帳の作成方法を理解するため、参加者の皆様は仮想会社の情報資産をリストアップし、それらの評価を行いました。守るべき情報資産について、各グループから様々な意見が出され、討議を通じて情報資産管理についての重要性を実感し、理解が促進されました。



開催日時と場所

【日時】：令和5年10月10日（火） 13時00分～17時30分

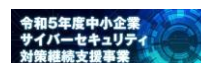
【会場】：東京都新宿区西新宿 1-22-2 新宿サンエービル 7F

【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.adeco.com



第5回セミナー内容

テーマ

組織として策定すべき対策基準及び情報セキュリティの三大要素【対策基準レベル①】

講師：星野 樹昭（ほしの しげあき）氏

【セキュリティ対策基準の策定】（セミナーテキスト 第8章）

セキュリティ対策基準とは、組織の情報資産を保護するための方針やルールです。しかし、一口にセキュリティ対策基準と言っても、その内容や範囲は様々です。そこで、このテーマでは、クイックアプローチ、ベースラインアプローチ、網羅的アプローチという3つのレベルに分けて、それぞれの特徴やメリット・デメリットを解説します。これにより、皆様が自分たちの組織に合った対策基準を選択し、策定できるようになります。

【管理策のテーマと属性】（セミナーテキスト 第9章）

管理策とは、セキュリティ対策基準を実現するための具体的な手段です。管理策は多岐にわたりますが、ここでは国際規格であるISO/IEC 27002を参考にして、組織的、人的、物理的、技術的という4つのテーマに分類して紹介します。また、各テーマには属性という概念があります。属性とは、管理策がどのような目的や効果を持つかを示すものです。属性を理解することで、管理策の意義や重要性を把握することができます。

【脅威、脆弱性、リスクの定義と関係性】（セミナーテキスト 第10章）

脅威とは、情報資産に損害を与える可能性のある事象です。脆弱性とは、情報資産が脅威に対して持つ弱点です。リスクとは、脅威が脆弱性を突いて情報資産に損害を与える可能性とその影響度です。これらの用語は情報セキュリティにおいて重要な概念ですが、しばしば混同されがちです。そこで、このセッションでは、これらの用語の正しい定義と関係性を明確にし、ケーススタディを通して具体的な例を見ていきます。

※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 ※参加者アンケートより一部抜粋

- セミナーでの学びから、対策基準の策定方法や管理策のテーマと属性についての理解が深まりました。最新のISMSの情報も収集できて、非常に有益でした。
- リスク分析シートには以前にも取り組んだ経験がありましたが、考え方やアプローチが明確でなく、行き詰まってしまったことがありました。今回のセミナーでこれらの疑問や不明点が解消され、リスク分析の方法について理解が深まりました。
- セミナーでは、実践的なアプローチや管理策についての知識が得られ、これまでとは異なる視点でセキュリティに関する考え方を身につけました。
- セミナーでの学びを通じて、これまで曖昧だった用語の定義や脅威と脆弱性の関係について理解できました。
- セミナーに参加し、実務的な対策基準の策定方法と具体的なアプローチについて学び、これらがセキュリティ対策においてどれだけ重要かを理解しました。

<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



第5回ワークショップ内容

■ワークショップ “情報資産管理台帳の作成方法を理解する”

第5回ワークショップでは、仮想会社のシナリオに基づいて、組織の情報資産を整理し、情報資産管理台帳の作成に取り組みました。この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の中から、「重要度定義」と「情報資産管理台帳」を利用しました。参加者はそれぞれの情報資産を「情報資産管理台帳」に記入し、各情報資産の機密性、完全性、可用性に関する評価を「重要度定義」を参考にして行い、それに基づいて重要度を付与しました。

【情報資産管理台帳 記入例】

業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類			評価値			
						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
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	有			3	1	1	3
人事	社員名簿	社員基本情報	人事部	人事部	書類	有			3	3	3	3
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部	書類		有		3	3	2	3
経理	給与システムデータ	税務署提出用源泉徴収票	給与計算担当	人事部	事務所PC			有	3	3	2	3

<記入内容についての解説>

- 業務分類** 情報資産と関連する業務や部署を記入します。情報資産が少なければ省いても構いません。
- 情報資産名称** 情報資産の名称や内容を表すものを簡潔に記入します。正式名称がないものは社内通称で構いません。
- 備考** 情報資産名称だけでは個人情報の有無や重要度が判断できない場合に説明を記入してください。
- 利用者範囲** 情報資産を利用してよい部署等を記入してください。アクセスコントロールに利用することができます。
- 管理部署** 情報資産に対して情報セキュリティ上の管理責任がある部署等を記入してください。小規模事業者であれば担当名でも構いません。
- 媒体・保存先** 情報資産の媒体や保存場所をリストから選択してください。書類と電子データの両方を保有している場合は2行に分けて記入してください。
- 個人情報の種類** 個人情報※1、要配慮個人情報※2、特定個人情報が含まれる場合は、該当欄に「有」を記入します。
※1要配慮個人情報も特定個人情報も個人情報ですが、「個人情報の」欄には要配慮個人情報と特定個人情報以外の個人情報に「有」を記入してください。
※2本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実等が含まれる個人情報
- 重要度** 情報資産の機密性、完全性、可用性のそれぞれの評価値（1～3）を選択します。3つの評価値から重要度（3～1）が表示されます。
⑦でいずれかの個人情報が「有」の場合、重要度は自動的に「3」となります。

（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

ワークショップ参加者の声 ※参加者アンケートより一部抜粋

- 情報資産の重要度と取り扱いについて理解を得ました。具体的な情報資産管理台帳の作成プロセスを実際に経験し、データの喪失や漏洩についての新たな視点を持ちました。
- 資産管理台帳の作成方法について学びました。他社の意見を聞き、評価値の決め方に関する洞察を得たことが非常に参考になりました。
- 情報資産としてリストアップする項目の詳細さが重要であることを認識しました。
- ワークショップを通じて、情報資産の洗い出しや目録の作成手順を理解し、情報資産の価値と重要度についての新しい視点を得ました。
- リスクアセスメントは非常に力を必要とする作業であることを学びました。入り口の資産洗い出しは負担がかかりますが、情報資産管理台帳の作成方法が理解でき、セキュリティ対策に役立つと感じています。
- 情報資産の整理の方法や情報資産の重要度の判断基準を学び、今後のセキュリティ対策に活用したいです。

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/>

<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。

運営事務局より編集後記

10月に入り、雲の動きや風のそよぎから季節の移ろいを感じられるようになりました。第5回セミナー・ワークショップにご参加いただきました皆様に、心より感謝申し上げます。

全10回の中間となる今回のセミナーは、より実践的なテーマに基づいて行われ、講師の話に耳を傾けながら、熱心にテキストを読み込む参加者の皆様の姿が印象的でした。ワークショップでは、各グループで慎重に検討が進められ、チームワークの素晴らしさが発揮されました。

中小企業の皆様のサイバーセキュリティ対策が一層向上するために、当事業は引き続きセキュリティ対策に関する情報の普及に努めて参ります。

運営事務局一同



10月の風景『秋風にゆらぐスキ』

次回（第6回） セミナー・ワークショップ のご案内

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
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】

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>

