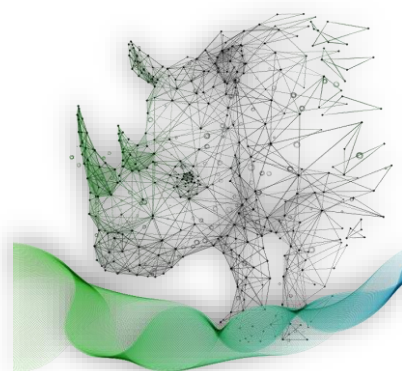


## 第9回

# セミナー・ワークショップ 開催レポート



## 令和6年度 中小企業サイバーセキュリティ社内体制整備事業

### 開催概要

令和6年12月17日(火)、東京都主催「中小企業サイバーセキュリティ社内体制整備事業」第9回セミナー・ワークショップが開催されました。

第9回セミナーでは、「組織として実践するためのスキル・知識と人材育成」と題し、各種人材育成カリキュラムについて解説しました。セキュリティ対策を実践するためには、IT およびデジタル全般のスキルや知識を持つ人材の育成が重要となります。そこで、セミナーでは関係機関が公表しているセキュリティ関連のカリキュラム内容の説明を行いました。また、デジタルスキル習得に関する講座を紹介する「マナビDX」の活用方法についても紹介しました。セミナー後に実施したワークショップでは「教育プログラムの検討」をテーマに据え、新入社員向けの育成カリキュラムの設計に取り組みました。参加者が自社で取組が可能なセキュリティ教育を学ぶための学習方法やツールについて検討を重ね、活発な意見交換を行いました。

### 開催日時と場所

【日時】：令和6年12月17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（※途中10分休憩あり）
- 15:00～15:15 休憩
- 15:15～15:35 ワークショップ（内容説明・個人ワーク）
- 15:35～16:35 ワークショップ（グループワーク）
- 16:35～17:15 全体発表・講師からのコメント
- 17:15～17:30 事務局からの案内

<お問い合わせ先> 中小企業サイバーセキュリティ社内体制整備事業運営事務局 ※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.shanaitaisei@jp.adeco.com



全 10 回開催される本セミナーでは、サイバーセキュリティの最新情報や実践的な対策内容を盛り込んだオリジナルテキストを使用して講義を進めていきます。今回のセミナーでは、セキュリティ対策を実践するために重要となる人材の育成、確保を行うための人材育成カリキュラムの計画および実施方法について解説しました。

## 第 9 編 組織として実践するためのスキル・知識と人材育成

### 第 24 章. 各種人材育成カリキュラム

第 24 章では、知識やスキルを備えた人材の育成・確保に向けて、関係機関が公表しているセキュリティ関連のカリキュラム内容について説明しました。NISC が提供する経営層や担当部署の部課長向けに設計された「プラス・セキュリティ知識補充講座 カリキュラム例」について講じた後、IPA が公開している IT 人材の育成を目的として作成された「IT スキル標準」のなかのレベル 1 向けのモデルカリキュラムについて概観を示しました。また、経済産業省と IPA が運営するデジタル人材育成プラットフォームである「マナビ DX」について活用方法を紹介しました。

### 第 25 章. スキルと知識を持った人材育成・人材確保方法

第 25 章では、前章で紹介したカリキュラムを活用し、リスキングに有効とされるカリキュラムの研修実施計画の作成手順について解説しました。また、リスキングを成功させるために重要な考え方であるチェンジマインド（変革思考）について紹介し、変化の速い IT 分野やセキュリティ領域での継続的な学びの重要性について説明し、第 9 回セミナーは閉講しました。

#### セミナー風景



参加者のプライバシーに配慮し画像を加工しています

※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://shanaitaisei.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

### セミナー受講で得た学び

- ✓ 「現在、策定を進めている社内研修用の教育資料について、作成のヒントを得ることができました」
- ✓ 「経営層や担当部課長、初学者向けなど、対象者のレベルに応じた学習の方法を学びました」
- ✓ 「教育や研修プログラムを設計する際に、そのプロセスと情報収集先がわかりました」

### セミナー受講で得た課題や気づき

- ✓ 「経営者のスキルやチェンジマインドも必要な時代だと認識できましたが、経営者に実行していただくのが課題だと感じています」
- ✓ 「情報セキュリティにおける育成の仕組みが不完全なため、改めて制度として設ける必要性に気づきました」

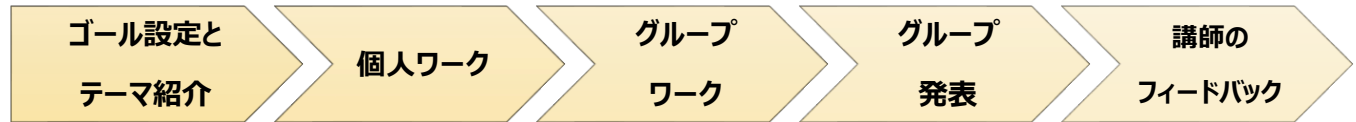
### セミナー受講をきっかけとしたアクション

- ✓ 「自社のセキュリティ教育の一環として、セミナーで紹介いただいたマナビ DX を活用してみたいと思いました」
- ✓ 「研修後の理解度テスト、フォローアップなどは、実施を検討したいと考えています」

## ワークショップ内容

第9回ワークショップでは、新入社員向けのセキュリティ教育カリキュラムの設計に取り組みました。参加者が効果的だと考えるセキュリティ教育について、学習方法やツールを検討します。さらに、優先して取り組むべき重要なトピックについて意見交換をしました。はじめに個人ワークで各自の考えをまとめた後、グループワークでそれぞれの意見やアイデアを展開しました。その後、グループ内で、具体的なセキュリティ教育プログラムについて協議しました。ワークショップの最後は、各グループの代表者が様々なアイデアやプランを全体に向け発表し、実現可能なセキュリティ教育について参加者全員に共有しました。

### 【ワークショップの進め方】



### ゴール

新入社員を対象に、学習ツールを用いてセキュリティ教育プログラム（初級編）を設計してみましょう

### 個人ワークの検討テーマ

1. セキュリティ教育を効果的に学ぶために、どのような学習方法やツールが役に立つと思いますか。また、その理由についても考えましょう。  
(学習ツール例：書籍、学習アプリ、動画教材 など)
2. セキュリティ教育において重要だと思うトピックは何だと思いますか。また、その理由についても考えましょう。  
(重要なトピック例：パスワード管理、フィッシング詐欺の認識、データ保護 など)

### グループワークの検討テーマ

1. 個人ワークの内容を共有しましょう。
2. 個人ワークの内容をもとに、セキュリティ教育プログラム（初級編）を設計しましょう。
  - a. 目標設定をしましょう。また、その理由についても考えましょう。
  - b. 目標を達成するために適した学習ツールや学習内容を考えましょう。また、その理由についても考えましょう。
  - c. どのようなトピックで構成するか考えましょう。また、トピックごとに具体的な実施内容を考えましょう。
  - d. どのような方法で効果測定を実施するか考えましょう。

### 【グループワークの検討・発表内容（抜粋）】

1. 個人ワークの内容の共有をしましょう。



1.役に立つ学習ツールや学習内容は？

マナビ DX の  
動画教材

ゲーム形式の教材

IT 資格取得講座の  
実施

自社で起きた  
インシデントの共有



2.重要だと思うトピックは？

デバイスの管理

内部不正

個人情報の取扱い

利便性と危険性の  
バランス

2\_a. 目標設定をしましょう。また、その理由についても考えましょう。

No	目標	理由
1	・自社のセキュリティポリシーを理解する	・社内リテラシーの維持・向上のため
2	・自社のセキュリティルールを理解する	・インシデント発生時に適切な行動が取れるようにするため
3	・メールやデータなどの社内情報の適切な取扱い方法を理解する	・情報漏えいを防止するため

2\_b. 目標を達成するために適した学習ツールや学習内容を考えましょう。また、その理由についても考えましょう。

No	学習ツール・学習内容	理由
1	・社内講師による面談形式の研修	・教育を受ける従業員の得意不得意に合わせてOJT形式で実施することで、理解度が上がるため
2	・動画教材	・時間を選ばず、自発的な学習ができるため ・制限がなく、反復学習が可能なため
3	・定期的なフォローアップ	・セキュリティ意識の持続が見込めるため
4	・実践演習	・ワークショップなどで実践し、自身で考えてもらう機会をつくるため ・過去に起きた事例をもとに対策を考えてもらうため
5	・eラーニング・学習アプリ	・学習効果をテストなどで把握しやすいため

2\_c. どのようなトピックで構成するか考えましょう。また、トピックごとに具体的な実施内容を考えましょう。

No	トピック	具体的な実施内容
1	・データ保護の必要性の理解 (個人情報保護・機密情報保護)	・保護すべき自社の情報資産の理解を深める
2	・標的型メール(フィッシング)対策	・実際の被害事例を共有する
3	・SNSの取り扱い	・会社の機密情報などを投稿しないといったルールを周知する
4	・インシデント発生時の対応	・報告フローや初動対応の方法を周知する ・インシデント発生時のシュミレーショントレーニングを行う
5	・スマートフォン・ノートPCなどの機器管理	・紛失によるデータ流出の危険について理解する

2\_d. どのような方法で効果測定を実施するか考えましょう。

効果測定の方法
<ul style="list-style-type: none"> <li>・理解度テストを実施する</li> <li>・アンケートを実施しフィードバックを取得する</li> </ul>

## ワークショップ風景

今回は、7つのグループに分かれてワークを実施しました。参加者の皆様は自分の意見を書いた付箋をホワイトボードに貼り付けていきます。その後、グループ全体で付箋の内容を確認しました。参加者同士の積極的な意見交換を経て、グループ全体の意見をまとめていきます。まとめ上げた内容はプレゼンテーション用のスライドとして作成し、最後に完成した成果物を全体に向けて発表しました。



参加者のプライバシーに配慮し画像を加工しています

## 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

- ✓ 「社内教育についてどうすればいいか悩んでいたのですが、他社の取組事例を聞いて大変参考になりました」
- ✓ 「情報セキュリティの新人教育プログラムに、理解度テストを盛り込みたいと思いました」
- ✓ 「新入社員に対しては、自社が守るべき機密情報を具体的に示すことが大切だと理解しました」

## 次回のご案内

**日時**：令和7年1月21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

## 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社内体制整備事業運営事務局

TEL：0120-138-166

受付時間：平日 9:00～17:00（祝日を除く）

メール：[ade.jp.shanaitaisei@jp.adecco.com](mailto:ade.jp.shanaitaisei@jp.adecco.com)

URL：<https://shanaitaisei.metro.tokyo.lg.jp/>

Facebook：<https://www.facebook.com/cys.shanaitaisei/>

<お問い合わせ先> 中小企業サイバーセキュリティ社内体制整備事業運営事務局 ※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.shanaitaisei@jp.adecco.com](mailto:ade.jp.shanaitaisei@jp.adecco.com)

