令和４年 10 月 11 日
運営事務局

【開催レポート】東京都 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・ワークショップ開催レポート

～これって攻撃？弱点なんかわかりません？～

開催概要

令和４年 10 月 11 日（火）、東京都主催『東京都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・ワークショップが開催されました。全 10 回を通じてセキュリティの基礎、及び今後必要な対策を学ぶセミナー・ワークショップの５回目となります。今回のテーマは、「これって攻撃？弱点なんかわかりません？」です。サイバーセキュリティは自分たちが事故を起こさないようにするだけでなく、「攻撃」と思われる、外部からの影響を受ける可能性があることを理解し、対策を立てる必要があります。セミナー5 回目では、会社を取り巻く脆弱性や脅威を把握し、会社のリスク（弱点）を考察する方法を学びます。

開催日時と場所

【日時】：令和４年 10 月 11 日（火） 13 時 00 分～17 時 30 分
【会場】：＜新宿会場＞ 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


新宿会場

（次回以降の予定）
第６回、第７回は、天王洲会場にて
第８回、第９回、第 10 回は、新宿会場にて開催予定

当日のタイムスケジュール

13:00 ～ 13:05	開会の挨拶
13:05 ～ 15:15	セミナー（※途中 10 分休憩あり）
15:15 ～ 15:25	休憩
15:25 ～ 17:20	ワークショップ
17:20 ～ 17:30	質疑応答・運営事務局連絡
17:30 ～ 18:00	講師への質問タイム（※希望者のみ）

＜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

セミナー詳細

■**セミナータイトル：**これって攻撃？弱点なんかわかりません？

■**講師：**玉川 博之 氏

<セミナー内容>

第１章「脅威と脆弱性に対応する」では、まず脅威について、自社を脅かす脅威とは何か、どのように分析、アプローチすればよいのか、また、クラウド導入が進む昨今、そこに対してどのようなアプローチがあるのか、などを学びます。次に、脆弱性については、システムの脆弱性と人の脆弱性、また、脆弱性をどのように把握するかや、情報のキャッチアップ方法を学びます。

第２章「リスクを検討する」では、リスクとは何かを学び、セミナー3 回目で紹介した CSF を利用したセキュリティリスクのマネジメントやリスクアセスメントを学びます。最終的には各資産のリスクや、各資産がどのような状況に置かれているかを把握できるようになることを目指します。

登壇した玉川講師

ミニワーク ～振り返ってみよう～

セミナーでは、聞くだけでなく考えることで知識の定着を図るため、毎回ミニワークを行います。セミナー５日目では、以下をテーマに振り返ります。

テーマ１：ATTACK ツリーを埋めてみましょう ・・・・・・・・・・セミナー5 日目テキスト P21 掲載

ATTACK ツリーとは、脅威を実現させうる具体的な攻撃手法を洗い出すことができる、脅威分析手法の一つです。（※詳しくは、セミナー5 日目テキス P6 を参照ください。）

今回は、「鍵付きキャビネットが利用できない」に対し、キャビネットが利用できなくなる要因を２つ考えるところから始めます。

テーマ２：リスクを算出してみましょう （自分たちが持っている資産、リスクを数値で把握できるようになる）

・・・・・・・・・・セミナー5 日目テキスト P25 掲載

個人情報の保有数や一人当たりの資産価値、個人情報が漏えいする可能性などのシチュエーションから、年間予想損失額を算出してみましょう。

※第 5 回セミナーテキストは、以下の事業 HP で公開しています。

【中小企業サイバーセキュリティ対策継続支援事業 HP 】

URL：https://security-keizoku.metro.tokyo.lg.jp/

ワークショップ詳細

■ワークショップ概要：セミナーで得た知識をもとに、グループ（1 グループ 5～6）のメンバー同士で課題や取り組み事例、問題点などを共有します。

■ワークショップ進め方

1．アイスブレイク（自己紹介）
2．まずは自分の考えをワークシートへ書き出してみる（個人ワーク）
3．グループ内で、一人ずつ順番に書き出した内容を発表し、メンバーの意見や考えを共有する（グループワーク）
4．グループ毎に出た意見を発表して全体へ共有する（グループワーク）

グループで出た意見を代表者の方に発表いただきました。

■グループディスカッション（参加者意見抜粋）

テーマ１：自社のネットワーク構成について概要図を書いてみよう

全体を見ている方や部分的に管理されている方など、それぞれの立場から書ける範囲で記載してみましょう。
立場により異なる視点や考え方を共有します。

CHECK!

ネットワーク構成図には、物理構成図と論理構成図があります。クラウド利用がある場合には、外部の情報が盛り込まれる場合もあります。ネットワーク構成がわかると、どこに脅威や脆弱性がありそうか、構成図を見ながら話しができます。構成の全体概要や各ポイントの詳細を理解することで、会社の状況把握や脅威の想定がしやすくなり、脆弱性の考察や分析ができるようになります。

テーマ２：自社にとっての脅威を、働くシチュエーション別に考えてみよう

働くシチュエーション別（オフィス勤務時、在宅勤務時、営業などの外回り、外出先勤務時など）に、自身の業務の中でどのような脅威があるのかを考えます。

外出先勤務時：電話の内容を聞かれる、覗き見防止フィルターをつけていない、Free WiFi など公衆回線に接続する、持ち物の紛失・置き忘れ・盗難リスクなどがある。

在宅勤務時：個人 PC を使用している社員がいるが、セキュリティは個人任せになっている。

オフィス：勤続年数の長い社員が多いが危機意識の薄い部分がある。PC に不慣れな社員は、ID やパスワード情報をポストイットで PC に貼り付けている。

テーマ３：自社にとって脆弱であると思われる部分 Top５を考えてみよう

自社の脆弱と思われる部分をピックアップし、脆弱性について理解を深めていきます。

機器管理やアプリケーション管理、バージョン情報管理などが不十分。未使用のアプリケーションを削除していなかったり、ウイルス検知やアップデートなどの適切な更新ができていなかったりする。

インターネット運用ルールやデータの持ち出しルールが定められておらず、ネットワークの基本ルールも把握できていない。また、規程が不十分なので社員教育にも不足がある。

テーマ４：自社のリスクが高そうな部分 Top３を考えてみよう

自社システムのため災害や事故の際にベンダーでも対応が難しく、セキュリティの相談先がない。

個人判断で無料サービスにアクセスして利用したり、個人契約のサービスに社内情報や業務情報をコピーできたりしてしまう。

セキュリティノウハウがあるのが担当者一人だけ。セキュリティの人材不足、属人化の不安がある。

「人に依存」は、多くの会社でリスクとして挙げられています。しっかりとリスク分析のロジックを整えていく事がポイントです。

※次ページへ当日使用したワークシートを掲載しています。テキストと併せてご活用ください。

東京都セキュリティ継続支援事業 ワークショップ5回目

企業名：

開催日：10月11日(火) 15:15～17:15　　会場：新宿サンエービル　　担当講師予定：玉川

参加者名：

ワークショップ5回目のゴール
リスクの把握する方法を学び、参加者と共有することで気付きづらい脅威について気付きを得る。
外部からの攻撃の可能性についてストーリーやフレームワークを駆使して考えられるようになる。

チームメンバー

★5名～6名でワークショップを実施しました。開始時に自己紹介してメンバー名や業務内容などの記載に活用しましょう。

ワークショップテーマ１　自社のネットワーク構成について概要図を書いてみよう（個人ワーク用）

★全体を見ている方や部分的に管理されている方など、それぞれの立場に合わせてわかる範囲で考え、別紙をご用意いただき、書ける範囲で記載してみましょう。

ワークショップテーマ１　自社のネットワーク構成について概要図を書いてみよう（チームの意見まとめ用）

★グループで共有し、それぞれの立場の方がどのような視点で考えているのかを参考にしてみましょう。

ワークショップテーマ2　自社にとっての脅威を、働くシチュエーション別に考えてみよう（個人ワーク用）

★働くシチュエーションをいくつかのパターンに分け（オフィス勤務時、在宅勤務時、外回り(営業など)、外出先勤務時など）自身の業務の中で考えてみましょう。

ワークショップテーマ2　自社にとっての脅威を、働くシチュエーション別に考えてみよう（チームの意見まとめ用）

★どういった脅威が挙げられたのか、グループで共有してみましょう。

ワークショップテーマ3　自社にとって脆弱であると思われる部分Top５を考えてみよう（個人ワーク用）

★自社の脆弱と思われる部分をピックアップしてみましょう。

ワークショップテーマ3　自社にとって脆弱であると思われる部分Top５を考えてみよう（チームの意見まとめ用）

★上記Top５について、少し説明も加えながらグループに共有しましょう。

ワークショップテーマ4　自社のリスクが高そうな部分Top３を考えてみよう（個人ワーク用）

★セミナーでは、資産価値、脅威、脆弱性、発生可能性を掛け算したものがリスクとしているので、それらを総合的に検討し記載してみましょう。

ワークショップテーマ4　自社のリスクが高そうな部分Top３を考えてみよう（チームの意見まとめ用）

★上記Top3について、説明を加えながら共有してみましょう。

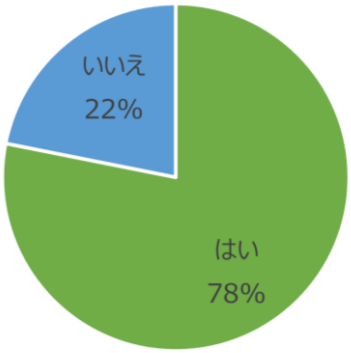
その他

★当日は講師からのフィードバックや気づきのメモに活用しました。

参加者アンケートより

Q. セミナー・ワークショップの内容を受けて、実際に社内で「やってみたこと」はありますか？

右の円グラフは、第 1 回から第 4 回までの結果を集計したものです。
これまで約 8 割の方が、セミナー・ワークショップの内容を受けて、何らか取組をしていると回答されています。



セミナー・ワークショップの内容を、参加者の皆様がどのように自社のセキュリティ対策へつなげていらっしゃるか、第 1 回から第 4 回までの参加者アンケートより、皆様の取組内容の一部をご紹介します。

第1回テーマ：私がセキュリティ担当？サイバーセキュリティって何するの？
セキュリティの仕事や担当として期待されること、セキュリティ推進に欠かせない取組について学びました。

- セミナー資料や動画を使ってセミナー・ワークショップの内容を社内で共有しました。
- 社内へ向けセキュリティに関する注意事項を配信しました。
- セミナーの内容を受けて、セキュリティに関してのルールを見直しました。
- セキュリティ担当の役割を整理し、社内報告体制の確認をするなど、体制作りを始めています。

第2回テーマ：セキュリティとDXは同時進行？一緒にやらないといけないんですか？
世の中を取り巻く変化、デジタル化・DX化の必要性、セキュリティ対策との関わり方について学びました。

- DXについて所属部署役員に説明し、自社におけるDXとは何かを考えてみました。
- セキュリティポリシーの再共有を実施するとともに、夏季休業前に全社員に対してセキュリティに関する注意事項を配信しました。
- セキュリティ会議を開催し、各部門の担当者を選任しました。課題の認識と対応を行っていく予定です。
- 環境構築図の提出をベンダーに求めました。現在疑問点をベンダーにぶつけています。

第3回テーマ：目指せセキュリティ事故ゼロ！防御してれば大丈夫？
事故が起きたことを把握できる仕組み作り、事故が起きた場合の対応方法などを学びました。

- ベンダーとCSFを利用したセキュリティチェックの自己評価結果を共有しました。
- ネットワーク構築図を整備しています。
- 課題の洗い出しと情報収集を始めました。メンバーを決めて、月1回の定期打合せを行うことにしました。
- セキュリティ5カ条を社内配布しました。また、CSIRT責任者と面談しました。

第4回テーマ：守るもの？私は何を守っているのだろう？
守るべきものを洗い出す作業や洗い出し方について学びました。

- 情報資産管理台帳を作り始めました。
- 専門家と共に情報資産を洗い出し、リスク評価を実施しました。
- 社内勉強会を行い、守るべき資産について、テキストを利用して説明しました。
- Microsoft365に多要素認証を設定しました。

＜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

次回セミナー・ワークショップ（第６回）について

【日時】：令和４年 10 月 25 日（火）　13 時 00 分～17 時 30 分

【会場】：：＜天王洲会場＞　東京都品川区東品川 2-2-24 天王洲セントラルタワー 24F

■タイトル：危ない！でも、予算も設備もありません。

■セミナー概要：弱点をそのままにしておくわけにはいきません。では、リスクをなくすためにはどうすれば良いでしょうか？そもそも、「リスクを無くそう」と言って本当にそのリスクを消すことはできますか？必要な設備や予算は確保していますか？セミナー６回目では、リスク対応の考え方を学びます。

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/