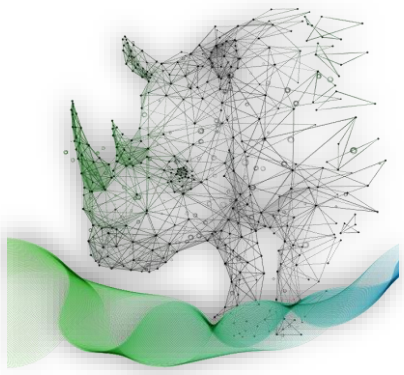
# 第６回
# セミナー・ワークショップ
# 開催レポート



## 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１０月８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、「具体的な構築・運用の実践」と題し、政府向けガイドラインの中から中小企業にも参考になる内容を取り上げて解説しました。さらに、ガイドラインのシステム導入工程に沿ってセキュリティ機能を実装・運用するための方法について紹介しました。セミナーに続いて実施したワークショップでは、情報セキュリティ 10 大脅威への対応について、想定される脅威とその影響、脅威への対応策について検討しました。参加者の皆様は、自社で発生しうる脅威について検討したうえで、参加者同士で意見交換を行い、発展的な協議を行いました。

## 開催日時と場所

【日時】：令和６年１０月８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 5 分休憩あり）
15:00 ～ 15:15　休憩
15:15 ～ 15:40　ワークショップ（内容説明・個人ワーク）
15:40 ～ 16:35　ワークショップ（グループワーク）
16:35 ～ 17:25　全体発表・講師からのフィードバック
17:25 ～ 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.adecco.com

## セミナー内容　　講師：星野 樹昭氏

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、システム導入の際に参考とすべき各種ガイドラインを紹介しました。また、システム導入工程の全体像と実践に当たっての留意点について解説しました。

### 第８編　具体的な構築・運用の実践

**第２０章. セキュリティ機能の実装と運用（IT 環境構築・運用実施手順）**

第２０章では、「デジタル・ガバメント推進標準ガイドライン」などが示すサービスシステム構築と運用の工程を参考に、中小企業においても適用することが有効な工程と、実践に当たっての留意点について解説しました。また、各工程においてセキュリティ機能を実装・運用するためポイントを詳説しました。さらに、近年注目されている「アジャイル開発」の概要と実践ポイントについて紹介し、第６回セミナーは終了しました。

**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の成果**

- ✓ 「システム導入に向けた考え方や方法がよくわかりました」
- ✓ 「セキュリティ機能の運用と実装について理解が深まりました」
- ✓ 「プロジェクトの進め方とその中でのセキュリティの考え方を学べました」
- ✓ 「プロジェクトを進める上での行動のヒントになりました」
- ✓ 「業務で使用するシステムについて、技術的な部分を可視化できました」

**セミナー受講で得た自社の課題・気づき**

- ✓ 「プロジェクトの進め方において社内でばらつきがあり、十分な成果が得られていないことが課題だと感じました」
- ✓ 「協力会社との業務フローを共有し、認識を合わせることが重要だと気づきました」

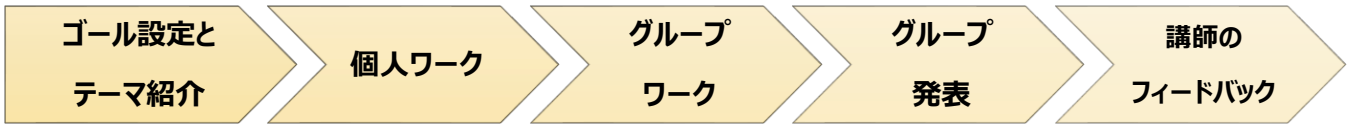
**セミナー受講で得た活用できそうな施策・アイデア**

- ✓ 「各工程でのテスト方法について理解した上で、実施したいと思います」
- ✓ 「システムの外注先と社内を巻き込み、システムの Fit&Gap 分析をしてみようと思いました」
- ✓ 「外部に開発を依頼する際は、自社のセキュリティポリシーを遵守できるかチェックリストを準備し確認を行いたいと考えています」
- ✓ 「三点見積りによる適正予算の算出方法は、活用できそうです」

## ワークショップ内容

第 6 回ワークショップでは、情報セキュリティ 10 大脅威への対応策について検討しました。参加者の皆様は、自社の事業内容や業務内容の特性から想定される脅威を「情報セキュリティ 10 大脅威」から選択し、脅威への影響を考えていきます。そのうえで、脅威に有効な実施手順を検討しました。さらに、実施手順を実装するうえで障壁となる課題を洗い出し、課題解決のための方策を立案しました。個人ワークで自社の状況や問題点を整理し、グループワークで他社の事例を共有することで、自社で取組可能なアイデアやノウハウ、新たな気づきを得る契機となるワークショップになりました。

**【ワークショップの進め方】**




| ゴール |
| --- |
| **グループでの意見交換、協議、発表** |
| **他社が実施している取組について、自社でも取り入れられるか考える** |
| **3 つのテーマ** |
| **①　事業影響の認識**<br><br>**個人ワーク**__「情報セキュリティ 10 大脅威：2024」*1 を参照しそれぞれの脅威が自社事業にどのような影響を与えるか（もしくは可能性があるか）を考えてみましょう。脅威ごとに、事業の内容と影響を記載してください。<br>※「1.ランサムウェアによる被害」は対象外とします。<br>**グループワーク**__事業への脅威に対する影響度は、会社によって異なります。自社だけでなく、他社にとってどのような影響があるのか、グループで認識しましょう。 |
| **②　有効な実施手順の確認**<br><br>**個人ワーク**__脅威に有効と思われる実施手順を、「情報セキュリティ 10 大脅威のリスク低減管理策と実施手順」*2 から選択してください。実施手順は自社にとって最も有効と思われるものを選択し、選択した理由も考えてみましょう。<br>**グループワーク**__各社の事業（業務）内容によって、さまざまな考え方があることを認識し、各社の共通認識となる実施手順について検討しましょう。さらに、実施手順資料に記載のない多様な視点（ユニークな考え方）について、意見交換を実施してください。 |
| **③　現状の課題の洗い出しと解決手段**<br><br>**個人ワーク**__②で選択した実施手順を実際に自社で実施しようとした場合、課題（障壁）となるのはどのようなことでしょうか。また、その課題を解決するための手段の案はどのようなものがありますか。選択した手順ごとに検討してみましょう。<br>**グループワーク**__「課題と解決手段案」を共有し、より具体的な解決手段、もしくは代替手段があるか、という視点で、意見交換を実施してください。 |

## ＊[1]「情報セキュリティ 10 大脅威：2024」

| | |
|---|---|
| 1 ランサムウェアによる被害 | ランサムウェアはコンピュータ内のファイルを暗号化し、使用できなくする攻撃です。復旧には金銭を要求され、データが公開されるリスクもあります。組織の規模に関係なく標的にされます |
| 2 サプライチェーンの弱点を悪用した攻撃 | 取引先やサービス提供者の脆弱性を狙って攻撃を行い、そこからさらに標的の情報やシステムに侵入します。特にソフトウェアのアップデートにウイルスを仕込むなどが行われます |
| 3 内部不正による情報漏えい等の被害 | 組織内の従業員や元従業員が不正に情報を持ち出すことによる被害です。これにより、機密情報が外部に流出し、組織の信用や経済的な損失が発生します |
| 4 標的型攻撃による機密情報の窃取 | メールやウェブサイトを介してウイルスに感染させ、長期間にわたって組織内部に潜入し、機密情報を盗む攻撃です。巧妙に仕組まれ、従業員を油断させる手法が使われます |
| 5 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃） | 脆弱性に対する修正プログラム（パッチ）が公開される前に、その脆弱性を悪用する攻撃です。これにより、サービス停止や大規模なシステム被害が発生します |
| 6 不注意による情報漏えい等の被害 | メールの宛先間違いや端末の紛失など、従業員の不注意によって発生する情報漏えいです。こうしたミスにより、社会的信用の失墜や経済的損失が発生します |
| 7 脆弱性対策情報の公開に伴う悪用増加 | 脆弱性に関する情報が公開された後、それを悪用した攻撃が急増することがあります。公開後に速やかに対策を講じることが求められます |
| 8 ビジネスメール詐欺による金銭被害 | 経営者や取引先を装ってメールを送り、組織を騙して金銭を振り込ませる詐欺です。この詐欺により、組織は多額の損失を被る可能性があります |
| 9 テレワーク等のニューノーマルな働き方を狙った攻撃 | テレワークの普及に伴い、在宅勤務環境やリモートアクセスの脆弱性を狙った攻撃が増えています。自宅のネットワークやリモートシステムのセキュリティ対策が重要です |
| 10 犯罪のビジネス化（アンダーグラウンドサービス） | サイバー犯罪がビジネス化し、犯罪者がサービスとしてサイバー攻撃ツールや技術を提供する「サイバー犯罪ビジネス」が拡大しています。これにより、攻撃のハードルが下がっています |

## ＊[2]「情報セキュリティ 10 大脅威のリスク低減管理策と実施手順」

| No | 管理策種別 | 番号 | 管理策 | 概要 | 実施手順 |
|---|---|---|---|---|---|
| 1 | 組織 | 5.1 | 情報セキュリティのための方針群 | 経営陣が承認し、全社員に周知される情報セキュリティ方針を策定・実施することで、組織全体のセキュリティ意識を統一し、適切な対応を促進する。 | 1-1 経営陣と協力して情報セキュリティ方針を策定し、全社に周知。<br>1-2 方針を定期的にレビューし、最新の脅威に対応。<br>1-3 方針に基づき、全社員向けのセキュリティ研修を実施。 |
| 2 | 組織 | 5.7 | 脅威インテリジェンス | 脅威に関する情報の収集と分析を通じて、ランサムウェアの新たな手口やトレンドを把握し、適切なリスク軽減策を講じる。 | 2-1 セキュリティ情報提供サービスを契約し、脅威インテリジェンスを取得。<br>2-2 取得した情報を分析し、組織のリスクに応じた対応策を策定。<br>2-3 定期的に脅威インテリジェンスを更新し、対応策の改善に活用。 |
| 3 | 組織 | 5.19 | 供給者関係における情報セキュリティ | 供給者との関係において、情報セキュリティリスクを管理し、供給者が提供する製品やサービスに対するセキュリティ対策を強化する。 | 3-1 供給者との契約書にセキュリティ要求事項を明確に記載。<br>3-2 供給者のセキュリティ対策状況を定期的に監査。<br>3-3 サプライチェーン全体のセキュリティリスクを評価し、改善提案を実施。 |
| 4 | 組織 | 5.23 | クラウドサービス利用における情報セキュリティ | クラウドサービスの利用時に、情報の機密性、完全性、可用性を確保するための規則を定め、セキュリティリスクに対応する。 | 4-1 クラウドサービス提供者のセキュリティ基準を確認し、リスク評価を実施。<br>4-2 クラウド利用時のアクセス制御や暗号化設定を適切に実装。<br>4-3 クラウド上のデータバックアップを定期的に行い、リカバリプランを策定。 |
| 5 | 組織 | 5.24 | 情報セキュリティインシデント管理の計画および準備 | ランサムウェア攻撃を含むセキュリティインシデントに対する対応手順を計画し、訓練しておく。 | 5-1 セキュリティインシデント対応手順を文書化し、全社員に周知。<br>5-2 インシデント発生時の責任者を明確にし、迅速な対応を促進。<br>5-3 インシデント対応訓練を定期的に実施し、実効性を確認。 |
| 6 | 人的 | 6.3 | 情報セキュリティの意識向上、教育および訓練 | 要員に対して定期的にランサムウェアに関するセキュリティ教育を実施し、フィッシングメールなどの手口に引っかからないように意識を高める。 | 6-1 全社員向けに、年次セキュリティ研修を開催。<br>6-2 役職に応じたセキュリティ意識向上プログラムを導入。<br>6-3 定期的にフィッシングメール対策訓練を実施し、社員の反応を評価。 |
| 7 | 人的 | 6.7 | リモートワーク | リモートワーク環境でもランサムウェアから情報を保護するための対策（VPNの利用、認証強化など）を行い、遠隔地での作業にも安全な基準を適用する。 | 7-1 リモートアクセスを多要素認証で保護し、不正アクセスを防止。<br>7-2 リモート作業用デバイスにはデータ暗号化を必須化。<br>7-3 リモートワーク環境のセキュリティチェックを定期的に実施。 |
| 8 | 物理 | 7.1 | 物理的セキュリティ境界 | 物理的なセキュリティ境界を設け、情報資産への不正な物理的アクセスや損傷を防止し、情報セキュリティを確保する。 | 8-1 重要な情報資産が保管されている場所（サーバールームやオフィス）の物理的な境界を明確に設定。<br>8-2 不正アクセス防止のため、セキュリティゲートやアクセスカードシステムを導入。<br>8-3 定期的にセキュリティ境界の監査を実施し、脆弱性を特定して改善。 |

| No | 管理策種別 | 番号 | 管理策 | 概要 | 実施手順 |
|---|---|---|---|---|---|
| 9 | 物理 | 7.3 | オフィス、部屋および施設のセキュリティ | 重要な情報資産が保管されているオフィスや施設に対して、適切な物理的セキュリティ対策を施し、不正アクセスを防ぐ。 | 9-1 重要情報が保管されているオフィスや部屋に対して入退室管理を実施し、記録を保管。<br>9-2 セキュリティカメラを設置し、常時監視体制を整える。<br>9-3 オフィスや施設の鍵やアクセスカードの管理プロセスを厳格化し、不正利用を防止。 |
| 10 | 技術的 | 8.2 | 特権的アクセス権 | 特権的なアクセス権の割り当てと管理を適切に行い、システムへの不正アクセスや内部不正を防止する。 | 10-1 特権アクセスを必要最小限に制限し、管理者アカウントを分離。<br>10-2 特権アクセスの使用を監視し、ログを定期的にレビュー。<br>10-3 特権アクセスの利用を自動通知し、異常な使用をリアルタイムで把握。 |
| 11 | 技術的 | 8.7 | マルウェアに対する保護 | マルウェア対策ソフトウェアの導入と適切な管理により、ランサムウェアの侵入を防止する。 | 11-1 全デバイスに最新のマルウェア対策ソフトを導入。<br>11-2 社内ネットワークに入るすべてのファイルをスキャン。<br>11-3 定期的なマルウェア検知テストを実施し、対策の有効性を確認。 |
| 12 | 技術的 | 8.8 | 技術的脆弱性の管理 | システムやアプリケーションの脆弱性を定期的に評価し、適切なパッチを適用することで、ランサムウェアの侵入経路を遮断する。 | 12-1 最新の脆弱性情報を常に取得し、影響を受けるシステムをリスト化。<br>12-2 定期的なパッチ適用スケジュールを策定し、迅速に実施。<br>12-3 自社のシステムに対する脆弱性スキャンを定期的に実施。 |
| 13 | 技術的 | 8.12 | データ漏えいの防止 | データ漏えいを防ぐためのシステムを導入し、機密情報が不正に外部へ流出することを防止する。 | 13-1 機密データに対するアクセス制限を設け、必要最小限の者のみアクセス許可。<br>13-2 データの送受信時に暗号化を適用し、通信内容の漏えいを防止。<br>13-3 DLP（データ漏えい防止）ソリューションを導入し、外部への不正なデータ流出を監視。 |
| 14 | 技術的 | 8.13 | 情報のバックアップ | 定期的にバックアップを取得し、データを安全な場所に保管しておくことで、ランサムウェアによるデータの暗号化に対応できる。 | 14-1 重要データは定期的に自動バックアップを行い、別の場所に保存。<br>14-2 バックアップデータの復旧テストを定期的に実施。<br>14-3 バックアップの暗号化を徹底し、不正アクセスを防止。 |
| 15 | 技術的 | 8.16 | 監視活動 | ネットワークやシステムの異常な動作を監視し、ランサムウェア感染の早期検出と対応を可能にする。 | 15-1 ネットワークおよびシステムのリアルタイム監視を導入。<br>15-2 セキュリティイベントや異常行動の発生を通知するシステムを設定。<br>15-3 監視ログを定期的にレビューし、異常検知の精度を向上。 |
| 16 | 技術的 | 8.20 | ネットワークのセキュリティ | ネットワークのセグメンテーションとセキュリティ管理により、ランサムウェアの拡散を防ぐ。 | 16-1 ファイアウォールや侵入検知システムを導入し、ネットワークトラフィックを監視。<br>16-2 ネットワークに接続するすべてのデバイスを認証し、無断接続を禁止。<br>16-3 ネットワークセグメンテーションを導入し、機密情報へのアクセスを分離。 |
| 17 | 技術的 | 8.21 | ネットワークサービスのセキュリティ | ネットワークサービスにおけるセキュリティを強化し、通信やデータの安全性を確保する。 | 17-1 外部ネットワークサービスとの通信を暗号化し、第三者からの盗聴を防止。<br>17-2 サービス利用状況を定期的に監査し、不正なサービス利用を防ぐ。<br>17-3 サービスプロバイダのセキュリティレベルを評価し、適切な契約を締結。 |
| 18 | 技術的 | 8.22 | ネットワークの分離 | ネットワークを分離して管理することで、攻撃が発生した場合にその影響範囲を限定し、セキュリティを高める。 | 18-1 内部ネットワークを業務別に分離し、各セグメントごとにアクセス制御を実施。<br>18-2 ネットワークトラフィックを監視し、異常な通信を早期に発見。<br>18-3 セキュリティの高いゾーンへのアクセスには多要素認証を導入。 |
| 19 | 技術的 | 8.23 | ウェブ・フィルタリング | 不正なウェブサイトへのアクセスをフィルタリングし、マルウェアやフィッシング詐欺からシステムを保護する。 | 19-1 業務に関係のないウェブサイトへのアクセスを制限。<br>19-2 セキュリティリスクがあるコンテンツやサイトを自動ブロックするフィルタリングを設定。<br>19-3 フィルタリングポリシーを定期的に見直し、新たな脅威に対応。 |
| 20 | 技術的 | 8.24 | 暗号化の使用 | 機密データの暗号化を行い、ランサムウェアによるデータの悪用を防止する。 | 20-1 すべての重要データを暗号化し、無許可のアクセスを防止。<br>20-2 暗号鍵の管理プロセスを導入し、鍵の安全な保管と利用を確保。<br>20-3 暗号化ポリシーの適用範囲を定期的に見直し、新しい技術や要件に適応。 |

**【発表内容（抜粋）】**

**①　事業影響の認識**

発表者

私たちは卸業と製造業で構成されたグループです。
検討した脅威は、３の「内部不正による情報漏えい等の被害」です。

| 事業内容 | 脅威発生時の事業への影響 |
|---|---|
| 卸業<br>製造業 | ・　取引先情報が漏れることで、顧客と仕入れ先が直接取引する可能性が出てくる。<br>・　価格の値下げ交渉が発生する。<br>・　価格や仕様などの機密情報が漏えいすることで案件失注のおそれがある。<br>・　売り上げへの影響が懸念される。 |

**②　有効な実施手順の確認**

| 共通認識と選択した理由 | 多様な視点（ユニークな考え方） |
|---|---|
| （共通認識）<br>6-1　全従業員向けに、年次セキュリティ研修を開催。<br><br>（選択した理由）<br>人的対策が一番有効的であるから。 | ・　人的対策が一番簡単であり、一番難しい課題であるが、根気よくセキュリティの重要度を伝え続けるしかない。<br>・　経営層を味方につけ従業員への意識づけ、ルールを守らない従業員への対応を決めていく。<br>・　就業規則の見直しを行い、従業員に対し罰則を伝え、違反しないように意識づけをしていく。 |

### ③　現状の課題の洗い出しと解決手段

| 課題 | 解決手段 |
|---|---|
| ・　個人の意識の改善が必要。<br>・　従業員を教育できる人材が社内にいない。 | ・　定期的な勉強会を開催する。<br>・　外部研修などを開催し、外部のリソースを活用する。 |
| ・　データの管理権限を設けることで業務の利便性が失われる。 | ・　業務がスムーズに行えるよう社内で検討を重ね、取り扱うデータを精査し重要度別にし、グループの権限分けを行う。 |
| ・　操作履歴を管理するシステム等を導入には、コストがかかる。 | ・　経営層にセキュリティの重要度を伝え、セキュリティ予算を確保し対応する |

課題解決のヒント

経営層にセキュリティ重要度を伝え予算を確保する際は、「セキュリティはコストではなく投資」という考え方を提言していくようにするとよいでしょう。

## ワークショップ風景

個人ワークに取り組む参加者

チーム全員で発表内容を検討中

代表発表を聞く参加者

参加者のプライバシーに配慮し画像を加工しています

## 次回のご案内

**日時**：令和６年１０月２２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
URL：https://shanaitaisei.metro.tokyo.lg.jp/
Facebook: https://www.facebook.com/cys.shanaitaisei/