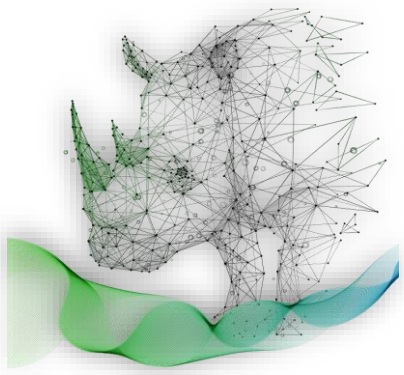
第３回
セミナー・ワークショップ
開催レポート



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８月２０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３回セミナー・ワークショップが開催されました。

第３回セミナーでは、「ISMS などのフレームワークの種類と活用方法の紹介」と題し、ISMS をはじめとしたサイバーセキュリティ対策における代表的なフレームワークの理解を主眼におき、各フレームワークの特徴について取り上げました。さらに、リスクマネジメントの概要と、リスクマネジメントプロセスにおける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解説しました。セミナー後のワークショップではセミナーで得た学びを活かし、仮想企業の情報資産の洗い出しを行い、各資産についてリスクアセスメントを実施しました。活発な意見交換を経て各グループ独自の対策を立案し、最後に全体発表を行いました。この取組により参加企業は自社のアクションプラン構築に資する多様なアイデアやノウハウを獲得しました。

開催日時と場所

【日時】：令和６年８月２０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 ～ 14:55　セミナー（※途中 5 分休憩あり）
14:55 ～ 15:00　質疑応答
15:00 ～ 15:15　休憩
15:15 ～ 16:30　ワークショップ（グループワーク）
16:30 ～ 17:20　全体発表・講師からのフィードバック
17:20 ～ 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の情報や網羅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。３回目となる今回のセミナーでは、サイバーセキュリティ対策においてフレームワークを活用することの意義や重要性について理解することを目的とし、各フレームワークの特徴とリスクマネジメントについて詳しく説明を行いました。

第 6 編　ISMS などのフレームワークの種類と活用法の紹介

第１１章. セキュリティフレームワーク

第１１章では、セキュリティフレームワークの概要説明から講義が始まりました。まずセキュリティフレームワークを使用するメリットを概説し、その後 ISMS、CSF、CPSF、サイバーセキュリティ経営ガイドラインについて詳細な説明が行われました。また、企業がフレームワークを選択するポイントを解説しました。網羅的な対策項目を提示している ISMS をベースとし、必要に応じ業種業態、重点領域によって、その他のフレームワークの内容を補完する活用法を紹介しました。

第１２章. リスクマネジメント

第１２章では、リスクマネジメントの概要と、リスクマネジメントプロセスにおけるリスクアセスメントの手法やリスク対応の全体像を説明しました。はじめに ISO/IEC 27001 におけるリスクマネジメント手順に触れ、状況の確定、リスクアセスメント、リスク対応、監視及びレビューといった手順を踏んだ運用プロセスについて解説しました。さらに各プロセスにおける具体的なアプローチや対応策を検討するうえでの留意点を紹介し、第３回セミナーは終了しました。

※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/

第 3 回セミナー・ワークショップで使用した資料

セミナー参加者の声　※参加者アンケートより一部抜粋

- ✓ 多様なフレームワークを学ぶことができ、自社においても活用できそうな情報が充実したセミナーでした。
- ✓ 代表的なフレームワーク、情報セキュリティの三要素（機密性、完全性、可用性）など、これまで知らなかった考え方や知識を学べました。
- ✓ テキストを見て今回のテーマは難しいと感じていましたが、講師にわかりやすく説明いただき理解が進みました。
- ✓ セキュリティ担当者だけでなく、経営層を巻き込んでセキュリティ対策に取り組むことが重要だと理解しました。
- ✓ 講義で紹介されたサイバーセキュリティ経営ガイドラインは、社内に展開し活用したいと考えています。
- ✓ リスクマネジメントの考え方について理解でき、非常に有意義な講義でした。
- ✓ 情報資産に対するリスク分析や評価が自社で実施できていないことに気づきました。
- ✓ ゼロから規程類を作成するのではなく、フレームワークを活用する有効性を知りました。
- ✓ テキストを参考に社内の資産台帳を確認し、リスク評価を考えてみたいと思います。

＜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

ワークショップ内容

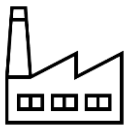
情報資産の洗い出しとリスクアセスメントは、セキュリティ対策の基盤となります。そこで今回のワークショップでは、架空の食品会社のシナリオを用いて資産台帳を作成し、リスクアセスメントを実施しました。１チーム４～５名で構成されたグループ内で各自が自己紹介を行った後、グループワークに取り組みました。IPA が公表している「リスク分析シート」[1] をアレンジした情報資産管理台帳シートを拡大印刷した用紙に、書記担当が議論の過程を記載していきます。一方、発表資料作成担当が議論の結果をエクセルのテンプレートにまとめていきます。各グループで検討した内容は発表担当がプレゼンテーションを行い、その後各グループの発表に対し講師がフィードバックを行いました。

テーマ紹介とゴール設定 → 検討内容説明 → グループワーク → グループ発表 → 講師のフィードバック

テーマ
資産台帳作成およびリスクアセスメント
３つのゴール
① リスクアセスメントの実施に必要となる情報資産の洗い出し
② リスクアセスメントを実施し、リスクレベルを算出
③ 仮想会社を基にグループでの意見交換、協議、発表

【食品会社のシナリオ】

会社概要



業種: 食品

社員数: 50 名

部署は、管理部、生産部、営業部の 3 部門

- ✓ 営業部の従業員にはノート PC が貸与されており、VPN を活用したリモート接続によって、社内環境へアクセス可能です。
- ✓ ノート PC の運用については、ノート PC 内にデータを保存しない運用を実施しています。
- ✓ 情報システム部門はなく、管理部門が兼任しています。

取り扱うシステムと情報

システム・情報の分類	製品管理システム (オンプレミス)	販売管理システム (クラウドベース)	経理管理システム (オンプレミス)	電子メールシステム (クラウドベース)	物理的文書
情報資産の内容	製品の在庫、出荷、品質	顧客情報、販売データ、契約書	売上データ、支出データ、財務報告	内部および外部のコミュニケーション、文書共有	印刷された契約書、社内マニュアル、製品カタログやラベルなどの宣伝資料
取り扱い方法	生産部門と営業部門のみがアクセスできる	暗号化され、営業部門と管理部門のみがアクセスできる	経理部門と管理部門のみがアクセスできる	全従業員がアクセス可能で、重要な文書は暗号化される	鍵付きのキャビネットに保管し、必要な時のみ関係者がアクセスできる

[1] リスク分析シート https://www.ipa.go.jp/security/guide/sme/about.html（付録７参照）

【検討内容】

架空の食品会社では、複数のシステムを活用し業務を遂行しています。これらの情報資産についての**重要度、対応種別、優先順位**を検討します。

【検討手順】

1．前ページに掲げた**取り扱うシステムと情報**の内容から、どのような情報が扱われているかを情報資産管理台帳（表２）に書き出します。経理管理システム、電子メールシステム、物理的文書　の３つについて検討しましょう。

2．書き出した情報に対し、機密性、完全性、可用性の観点からそれぞれ評価値と重要度を記載します。
評価値の記載は、「重要度の定義」（表１）を参照します。

3．リスク値の結果を基に、対応種別を選択します。この時の選定理由もシートに記載してください。
対応種別の選定は、「対応種別の定義」（図１）を参考にしてください。

表１ 重要度の定義

評価値		評価基準	該当する情報の例
機密性 アクセスを許可された者だけが情報にアクセスできる	3	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	●個人情報（個人情報保護法で定義） ●特定個人情報（マイナンバーを含む個人情報）
		守秘義務の対象や限定提供データ[12]として指定されている 漏えいすると取引先や顧客に大きな影響がある	●取引先から秘密として提供された情報 ●取引先の製品・サービスに関わる非公開情報
		自社の営業秘密として管理すべき（不正競争防止法による保護を受けるため） 漏えいすると自社に深刻な影響がある	●自社の独自技術・ノウハウ ●取引先リスト ●特許出願前の発明情報
	2	漏えいすると事業に大きな影響がある	●見積書、仕入価格など顧客（取引先）との商取引に関する情報
	1	漏えいしても事業にほとんど影響はない	●自社製品カタログ ●ホームページ掲載情報
完全性 情報や情報の処理方法が正確で完全である	3	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	●個人情報（個人情報保護法で定義） ●特定個人情報（マイナンバーを含む個人情報）
		改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある	●取引先から処理を委託された会計情報 ●取引先の口座情報 ●顧客から製造を委託された設計図
	2	改ざんされると事業に大きな影響がある	●自社の会計情報 ●受発注・決済・契約情報 ●ホームページ掲載情報
	1	改ざんされても事業にほとんど影響はない	●廃版製品カタログデータ
可用性 許可された者が必要な時に情報資産にアクセスできる	3	利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある	●顧客に提供しているEC サイト ●顧客に提供しているクラウドサービス
	2	利用できなくなると事業に大きな影響がある	●製品の設計図 ●商品・サービスに関するコンテンツ（インターネット向け事業の場合）
	1	利用できなくなっても事業にほとんど影響はない	●廃版製品カタログ

判断基準	重要度
機密性・完全性・可用性評価値のうち最大値が「3」の情報資産	3
機密性・完全性・可用性評価値のうち最大値が「2」の情報資産	2
機密性・完全性・可用性評価値すべてが「1」の情報資産	1

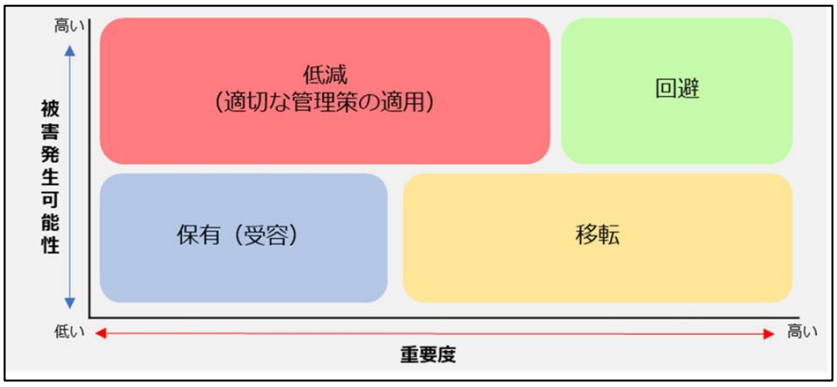


図１　対応種別の定義

表２　発表内容（抜粋）が記載された情報資産管理台帳

	業務分類	情報資産名称	利用者範囲	媒体・保存先	個人情報の有無	評価値 機密性	完全性	可用性	重要度	リスク値		対策方針	対策方針の選定理由
1	製品管理	製品の在庫データ	生産部門、営業部門	社内サーバー		2	2	2	2	2	リスク小	低減	日次バックアップに加えオフラインへデータを保存する
2	製品管理	出荷スケジュール	生産部門、営業部門	社内サーバー		2	2	2	2	2	リスク小	低減	日次バックアップに加えオフラインへデータを保存する
3	製品管理	品質検査結果	生産部門、営業部門	社内サーバー		2	2	2	2	2	リスク小	低減	日次バックアップに加えオフラインへデータを保存する
4	販売管理	顧客情報	生産部門、営業部門	社外サーバー	有	3	3	3	3	6	リスク大	低減	社外サーバーの時点で一定の移転はしている 操作ログ・アクセスログ管理を行うことでよりリスク減
5	販売管理	売上情報	生産部門、営業部門	社外サーバー		3	3	2	3	6	リスク大	低減	内部操作ログを取得する
6	販売管理	仕入れ情報	生産部門、営業部門	社外サーバー		3	3	2	3	6	リスク大	低減	内部操作ログを取得する
7	経理管理	売上データ（個人情報は含まない）	経理部門、管理部門	社内サーバー		2	2	2	2	2	リスク小	低減	日次バックアップに加えオフラインへデータを保存する
8	経理管理	支出データ（個人情報は含まない）	経理部門、管理部門	社内サーバー		2	2	2	2	2	リスク小	低減	日次バックアップに加えオフラインへデータを保存する
9	電子メールシステム	社内メール（業務連絡レベル）	全従業員	社外サーバー	有	3	1	1	3	6	リスク大	低減	（メール情報がなくなった場合への対策として）アーカイブ・バックアップを日次で実施
10	電子メールシステム	社外メール	全従業員	社外サーバー	有	3	3	2	3	6	リスク大	低減	（メール情報がなくなった場合への対策として） アーカイブ・バックアップを日次で実施 ※グループ内に実例あり
11	物理的文書	契約書	必要な時のみ関係者がアクセス	書類	有	3	3	3	3	6	リスク大	低減	監視カメラを導入して管理を強化する 先方都合もあるので回避は断念
12	物理的文書	製品カタログ	必要な時のみ関係者がアクセス	書類		1	1	1	1	2	リスク小	受容	紙のカタログはリスクが低いと判断

発表者のコメント

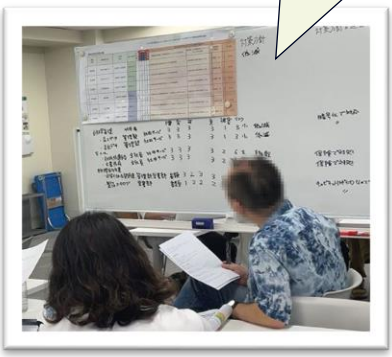
私たちのグループでは情報資産の**社外メール**と**契約書**に焦点を当て検討しました。どちらも個人情報が含まれており、リスク大と評価しました。社外メールについてはメールがなくなった場合の対策としてバックアップを実施すること、契約書については電子契約書への移行についても議論しましたが、先方都合もあることから断念し保管場所に監視カメラを導入することで、どちらの資産についても対策方針（対応種別）を低減としました。

講師のフィードバック

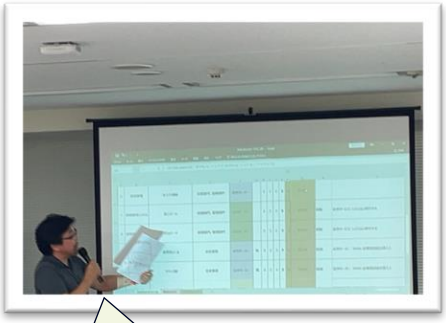
社外サーバー（メールサーバー）の障害を想定したときに、IT-BCP の観点から、メールが全損した場合に備えバックアップを取得するというのは正しい考え方です。なお、バックアップは取得だけでなく、復元する手順を整えておくことがポイントとなります。また契約書の管理ついて、電子契約書は便利な機能ですが全面導入は難しいと思うので、回避策でなく低減策を選択したのは、現実的な対応策といえるでしょう。

ワークショップ風景

パソコンに入力した内容を確認するチームメンバー



ホワイトボードに書かれた検討結果を確認しています



発表内容を投影したスクリーン前でフィードバックを行う星野講師

次回のご案内	**日時**：令和６年９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

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/