第４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４回セミナー・ワークショップ概要

令和５年９月 26 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４回セミナー・ワークショップが開催されました。

セミナーでは、「サイバーセキュリティ対策におけるフレームワークの体系」をテーマに、情報セキュリティマネジメントシステム（ISMS）をはじめとした代表的なフレームワークの概要やその活用価値について講義を展開しました。

ワークショップでは、仮想会社のシナリオをもとに ISMS を使用した管理手順の構築方法を理解することを目指しました。セキュリティ対策は各組織に合ったものが求められます。対策を漏れなくかつ効果的に実施するために、セキュリティフレームワークの高い有用性を参加者に実感いただくためのワークショップを実施しました。

開催日時と場所

【日時】：令和５年９月２６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 ～ 17:30　ワークショップ

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

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４回セミナー内容

テーマ　**サイバーセキュリティ対策におけるフレームワークの体系**

講師：星野 樹昭（ほしの しげあき）氏

【セキュリティフレームワーク】（セミナーテキスト 第７章）

本セミナーではまず、セキュリティフレームワークの基本的な役割と重要性を明示し、ISO/IEC27017、PCI/DSS、PMS などを紹介します。これらのフレームワークは、組織のセキュリティ対策を構築し、評価するための基盤となります。

その後、情報セキュリティマネジメントシステム(ISMS)に焦点を当て、その要求事項、運用プロセス、管理策について詳述します。特に ISO/IEC 27001 及び JIS Q 27001 の規格に基づき、ISMS の構築、実装、認証、そして維持に至るプロセスを説明します。

さらに、NIST サイバーセキュリティフレームワーク(CSF)の概要及び 3 つの構成要素（コア、ティア、プロファイル）についても紹介し、CSF と ISMS の関連性を探ります。ここでは、CSF と ISMS がどのように連携し、組織のセキュリティ対策を強化するかについて詳細に説明します。

最後に、サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要と、経営者及び担当幹部向けのサイバーセキュリティ経営ガイドラインの読解法を提供します。経営の重要 10 項目を通じて、サイバーセキュリティリスクの管理と対応、そして持続的な改善の方法を説明します。

本セミナーを通じて、参加者はサイバーセキュリティの基本的なフレームワークと、それらが組織のセキュリティポリシーとどのように連携するかを理解することができます。そして、最新のセキュリティ対策を効果的に実施し、組織全体のセキュリティを強化するための戦略と実践的知識を得ることができます。

※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

- ISMS と ISO/IEC 27002 について学び、セキュリティ対策の進め方を理解しました。
- セミナーを通じて、セキュリティに関する知識がより明確になり、特に ISMS の重要性を理解しました。セキュリティポリシーの具体的な方向性について有益な情報を得ることができました。
- フレームワークを活用することで、セキュリティ対策を包括的に検討できることを学びました。
- セミナーを通じて、フレームワークの実務への適用方法を明確に理解し、参考になる情報が多かったです。
- ISMS を含む複数のセキュリティ対策の基準と、それらへの適合に向けたプロセスを理解できました。
- サイバーセキュリティガイドラインの内容、経営者と担当者の視点での理解方法が明確になりました。
- 情報セキュリティの方針を一時的に見直していましたが、セミナーを通じて、定期的な PDCA サイクルでの見直しが必要であることを理解しました。
- 適切なフレームワークを選択し、効果的に活用する重要性を実感しました。
- セキュリティ対策はゼロから始めるのは困難であり、対策の指針や基準となるガイドライン、ベストプラクティスなどを活用して進めるべきだというテーマで代表的なフレームワークを体系的に学べました。

第４回ワークショップ内容

第 4 回ワークショップでは、ISMS の管理手順の作成方法を理解することが目的でした。このワークショップを通じて参加者は、ISMS の管理手順を作成するプロセスと、対策例が実際の ISMS 管理策とどのように関連するかを理解しました。

■ワークショップ

“仮想会社のシナリオをもとに、ISMS の管理手順の作り方を理解しよう”

仮想会社のシナリオ

業種と概要	背景
業種：　電子部品製造業 社員数：150 名 オフィス：　本社＋３つの生産工場 IT 環境：社内サーバ、クラウドサービスの利用、 テレワーク環境、機械との連携システム	・仮想会社は、ISMS 認証の更新時期が迫っている。 ・あなたは、この会社に勤務する社員で、ISMS 更新実行委員に選任された。 ・委員会で議論した 10 大脅威のリスクに対して、社内稟議の結果、すべてにおいて対策を実施することが決定した。 ・あなたのチームには、「セキュリティ管理手順」のドキュメント修正が指示された。

検討ポイント

- **作成する手順は、10 大脅威の対策内容を満たす必要がある**
- **対策内容が ISMS 管理策 [1] のどのカテゴリとどの項目に属するかを確認し、管理手順を作成する**

当日のワークショップは以下の流れで進めました。

1. まず、各グループは 10 大脅威の中から講師が指定した 1 組の対策例 [2] を確認し、それぞれの対策例が ISMS 管理策のどの項目に該当するかについて議論しました。 ※1 つの対策が当てはまるのは 1 つの項目とは限りません。
2. その後、議論された項目に該当する管理手順を作成しました。
3. 次に、各チームは 10 大脅威の中から上記 1 以外の任意の 1 組を選択し、選んだ対策例が ISMS 管理策のどの項目に該当するかを議論しました。
4. そして、その項目に該当する管理手順を作成しました。
5. 最後に、各グループは該当する項目と管理手順の内容を発表しました。

【管理手順サンプル】 例：ランサムウェアによる被害の 3 つの対策例の場合

管理策№ / 標題	管理手順
6.3　情報セキュリティの意識向上、教育および訓練	(1)定期的にフィッシング対策の教育プログラムを実施し、従業員がフィッシング攻撃の識別と対処法を理解できるようにする。
	(2)教育プログラムの効果を測定するために、模擬フィッシング攻撃を行い、従業員の理解度を評価する。
8.7　マルウェアに対する保護	(1)最新のセキュリティソフトウェアを導入し、マルウェアからの保護を確保する。
	(2)定期的にセキュリティソフトウェアをアップデートし、新たに出現するマルウェアに対する保護を強化する。
	(3)アップデートの実施を確認するレポートを月次で作成し、管理者に提出する。
8.8　技術的脆弱性の管理	(1)自動パッチ適用システムを導入し、システム管理者がパッチ適用の監視と評価を行う。
	(2)重要なセキュリティパッチは優先して適用し、適用後のシステム安定性を確認する。

1　ISMS 管理策については、第 4 回テキスト第 7 章 – 09、および第 4 回テキスト（別紙）ISO/IEC 27002:2022 管理策と目的 をご参照ください。

2　対策例については、次ページ資料「各脅威に関連する、仮想会社に潜む脆弱性・背景」をご参照ください。

第４回ワークショップ資料：各脅威に関連する、仮想会社に潜む脆弱性・背景

1．ランサムウェアによる被害	対策例
古いセキュリティソフトウェア（ウイルス対策）を使用しており、アップデートがユーザー任せとなっている。	最新のセキュリティソフトウェアを導入し、定期的なアップデートを行う。
OSのセキュリティパッチが定期的に適用されていない。	自動的なセキュリティパッチ適用のシステムを導入する。
従業員がフィッシングメールを認識できない。	従業員向けのフィッシング対策の教育を実施する。
2．サプライチェーンの弱点を悪用した攻撃	**対策例**
外部ベンダーとの認証情報の取り扱いが適切でない。	第三者との認証情報の共有を最小限にし、強固なパスワードポリシーを適用する。
サプライヤから使用を指示されたソフトウェアが、検証せずに使用している。	サプライヤからのソフトウェアを導入前にセキュリティチェックを行う。
サプライヤとの通信チャネルが暗号化されていない。	サプライヤとの通信には強固な暗号化技術を使用する。
3. 標的型攻撃による機密情報の窃取	**対策例**
新製品の設計図が社内サーバに格納され、誰でも容易にアクセスできる場所に保存されている。	機密情報のアクセス権限を見直し、必要な者のみがアクセスできるようにする。
PCにログインするときや、サーバにアクセスする際に使用するパスワードのポリシーが弱い。	強力なパスワードポリシーの導入と、定期的なパスワード変更を推奨する。
利用しているクラウドサービスに2要素認証が導入されていない。	2要素認証をクラウドサービスに導入する。
4. 内部不正による情報漏洩	**対策例**
アクセス権限の管理が適切でない。	アクセス権限の明確化と定期的な見直しを行う。
従業員のセキュリティ教育が不十分。	セキュリティ意識を高めるための継続的な教育を実施する。
社内での情報の共有が過度であり、全員が見られる共有ドライブの使用。	情報の共有を必要最低限にし、アクセスを制限する。
5. テレワーク等のニューノーマルな働き方を狙った攻撃	**対策例**
テレワーク用のデバイスが個人と業務で混在して使用され、それを組織が管理できていない。	業務用と個人用のデバイスを明確に分け、業務用のセキュリティ対策を強化する。
VPNのセキュリティ設定が不十分。	VPNのセキュリティ設定を強化し、定期的に見直す。
テレワーク時の物理的なセキュリティ対策がなされていない。	テレワーク時の物理的なセキュリティ対策のガイドラインを作成し、従業員に周知する。
6. 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	**対策例**
専用の機械制御ソフトウェアが古く、サポートが終了している。	サポート終了のソフトウェアは新しいものにアップデートする。
セキュリティのアップデート情報のモニタリングが不十分。	セキュリティ情報の更新を定期的にモニタリングし、必要なアップデートを迅速に行う。
自社開発ソフトウェアの、開発者のセキュリティ意識が低い。	開発者向けのセキュリティ教育を実施する。
7. ビジネスメール詐欺による金銭被害	**対策例**
請求書の確認プロセスが不十分。	請求書や取引先情報の確認プロセスを強化し、2段階確認制度を導入する。
従業員が偽の取引先からのメールを識別できない。	従業員向けのメールセキュリティ教育を実施する。
メールのセキュリティフィルターが導入されていない。	高度なメールフィルタリングやセキュリティソフトウェアを導入する。
8. 脆弱性対策情報の公開に伴う悪用増加	**対策例**
古く、サポート期限が切れているオペレーティングシステムのままの端末が存在する。	オペレーティングシステムやソフトウェアの最新バージョンへの定期的なアップデートを行う。
セキュリティアラートの対応が遅い。	セキュリティアラートの対応チームを設け、迅速な対応を行う。
社内ネットワークと公開ネットワークの隔離が不十分。	社内ネットワークと公開ネットワークの分離を徹底する。
9. 不注意による情報漏洩等の被害	**対策例**
従業員が外部のUSBメモリを無制限に接続できる。	外部メディアの接続ポリシーを明確にし、不正な接続をブロックする。
不用意に公開Wi-Fiを業務で利用する従業員がいる。	公開Wi-Fiの利用に関するガイドラインを制定し、安全なVPNの利用を推奨する。
プリントした文書の取り扱いが適切でない。	文書の印刷・保管・破棄に関するポリシーを明確にする。
10. 犯罪のビジネス化（アンダーグラウンドサービス）	**対策例**
製造業としてのノウハウの文書化が保護されていない。	重要な業務情報のアクセスを制限し、暗号化技術を導入する。
顧客データベースのアクセス管理が緩い。	顧客データベースのアクセス権限を強化し、定期的なセキュリティチェックを行う。
取引先との情報共有が暗号化されていない。	取引先との情報共有時には強固な暗号化技術を使用する。

セミナー・ワークショップ風景

ワークショップでは、グループごとに書記の方が議論内容をホワイトボードに書き出し、進行役の方が時間管理とメンバーからの発言を引き出す役割を担いました。約 1 時間のグループ作業中、参加者たちは熱心に資料を読み込み、ホワイトボードに考察結果を記入し、講師に対して積極的に質問しました。また、アイデアを共有し合う姿も見受けられ、参加者の皆様がワークショップに意欲的に取り組む姿が印象的でした。

運営事務局より編集後記

秋のお彼岸を過ぎてもまだまだ暑さが残る中、第４回セミナー・ワークショップが開催されました。

今回のセミナーでは、セキュリティ対策の実践編に入り、セキュリティに関するフレームワークの特徴や要点について詳しく学びました。
また、ワークショップでは、代表的なフレームワークである ISMS の管理手順の作成を実際に経験しました。

９月の風景
「雲間に隠れる中秋の名月」

今回のワークショップ運営では、各グループの検討内容がまとめられたホワイトボードをカメラで撮影し、その画像をスクリーンに拡大投影する新たな試みを行いました。
発表内容を視覚的に確認できることで、内容の理解が向上したと皆様からも好評でした。
今後もより良い運営のために工夫し、改善を図って参ります。

最後に、今回のセミナー・ワークショップを通じて、参加者の皆様には自社のセキュリティ課題や目標に合った対策を選択する重要性を一層ご理解いただけましたら幸いです。

運営事務局一同

次回（第５回） セミナー・ワークショップ のご案内	**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 **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】

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