第３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３回セミナー・ワークショップ概要

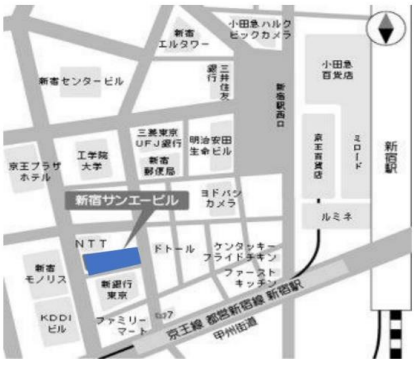
令和５年９月 12 日（火）、東京都が主催する「中小企業サイバーセキュリティ対策継続支援事業」の第３回セミナー・ワークショップが開催されました。

セミナーでは、政府のサイバーセキュリティ方針や最新のサイバー攻撃について説明し、ビジネスにおけるリスクを理解し、適切な対策を検討できるようサポートしました。また、サイバーセキュリティに関連する法律や規制についても分かりやすく解説し、法令遵守の重要性を強調しました。

ワークショップでは、情報セキュリティ 10 大脅威に関する知識を深め、仮想会社に対するセキュリティ対策の見直しを行いました。参加者は、サイバー脅威への対策をグループワークや討論の形式で学び、最適なセキュリティ対策についてのアイデアを共有し、学習を深めました。

開催日時と場所

【日時】：令和５年９月 12 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
17:25 ～ 17:30　運営事務局からの連絡

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

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３回セミナー内容

テーマ　**サイバーセキュリティに関する国の方針・施策およびサイバー脅威の動向**

講師：星野 樹昭（ほしの しげあき）氏

【デジタル社会の方向性と実現に向けた国の方針】（セミナーテキスト 第５章）

現代の経済成長とデジタル変革の密接な関係に焦点を当て、国がどのようにこれらを支えているかを解説します。具体的には、「経済財政運営と改革の基本方針 2023」を中心に、新しい資本主義、グリーントランスフォーメーション（GX）、デジタルトランスフォーメーション（DX）、スタートアップの推進など、ビジネス環境の変化について詳しく説明します。
また、「デジタル社会の実現に向けた重点計画」では、デジタル社会で目指すべき６つの姿と、中小企業のデジタル化を支援する国のアプローチを紹介します。セキュリティの確保にも焦点を当て、国の取組をわかりやすく解説します。
Society5.0 については、情報技術の変革とその社会への影響、生活やビジネスへの影響、さらには新たなセキュリティリスクについても詳しく説明します。

【サイバーセキュリティ戦略及び関連法令】（セミナーテキスト 第６章）

国のサイバーセキュリティ戦略の中核に焦点を当て、経済社会の活性化や国際的な貢献を目指す中で、セキュリティの役割とその実現方法を分かりやすく説明します。DX とサイバーセキュリティの連携、そして実際の企業経営における対策と取組のレベルについても触れます。
法的な側面では、「個人情報保護法」と「GDPR」（EU 一般データ保護規則）の要点に焦点を当て、これらが中小企業にどれほど重要か、留意すべき点についても詳しく解説します。

※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

- サイバーセキュリティに関して、国の方針や施策の動向を学びました。特に、GDPR など、EU の規制について気にかけたことがありませんでしたが、今後気をつけるべきだと感じました。
- セミナーで国の方針や施策を学び、IT 化と DX の加速について理解が深まりました。これに伴い、データ活用とセキュリティ対策の重要性が一段と高まることを実感しました。
- セミナーを通じて、行政のセキュリティに対する方針と中小企業への支援についての知識を得ることができました。
- サイバーセキュリティの国の方針について、わかりやすく説明いただき、理解が深まりました。特に、DX を経営層に説明し推進する際の課題について考える機会となりました。
- 国が提供するデジタルスキル教育の充実度に驚きました。デジタル社会の進化に合わせてセキュリティ対策も必要という学びを得ました。また、GDPR についても学び、対応を検討します。
- 国の基本方針やデジタル社会への施策について学び、DX とセキュリティの同時進行の重要性を再確認しました。DX への意識が高まる中で、セキュリティも常に考える癖を持つことが必要だと感じました。
- 国の方針と関連法令について学ぶ機会を得ました。さらに、マナビ DX のサイトから、DX に関する講座情報が入手できることを知りました。

第 3 回ワークショップ内容

第 3 回ワークショップでは、仮想会社のシナリオを基に、2 つのワークに取り組みました。各グループは自己紹介を行い、メンバーで協力してグループ内の役割（進行役/書記/発表者/オンラインコミュニティ投稿者*）を決定し、その後ワークに入りました。

*当事業では参加者向けのオンラインコミュニティを運営しており、終了後に当日の気づきなどを投稿担当の方が中心となって発信しています。

■ワークショップ 1

“仮想会社のシナリオをもとに、10 大脅威における脆弱性について議論し、対応策を考えよう”

1. まず、10 大脅威の中から、対策を講じる対象となる脅威を選択します。仮想会社のシナリオを通じて、実際に発生しうる脅威を理解します。
2. 次に、選択した脅威に対して、実際に被害が起こった場合の影響を議論します。脅威が会社に及ぼす潜在的な影響を考え、選択した脅威に対する具体的な対応策を検討します。

グループ発表で出た意見（一部抜粋）

選択した 10 大脅威	被害が起こった場合の影響	具体的な対応策
ランサムウェアによる被害	・データが使用不可となる ・情報をダークウェブに公開される可能性がある ・取引先の信頼低下	・OS のバージョン確認およびアップデートの実施 ・ディレクトリサービスの適切な管理 ・モバイルデバイス管理ツールの導入 ・社員教育の実施 ・定期的なスタンドアロン方式でのバックアップの取得
サプライチェーンの弱点を悪用した攻撃	・機密情報が漏えいする可能性がある ・取引先・仕入先に影響が出る ・二次災害の可能性がある	・通信の暗号化 ・データの暗号化 ・ウイルス対策ソフトを利用してスキャンを実施 ・EDR の導入
標的型攻撃による機密情報の窃取	・情報漏えいの可能性が高まる ・製造システムを停止させられる ・業務に支障が出る	・外部ベンダーと認証情報の取扱いルールの策定 ・パスワードの複雑化 ・アクセス権の制限 ・クラウドサービスの管理者パスワードを 2 要素認証にする
不注意による情報漏えい等の被害	・公開 Wi-Fi を使用することで情報窃取の可能性がある	・資産管理ツールを使用し USB をシリアル登録して使用制限をかける ・公開 Wi-Fi 使用時は、ファイアウォールを有効にする ・PDF 印刷設定を許可しない形式でサーバに保管する

■ワークショップ２

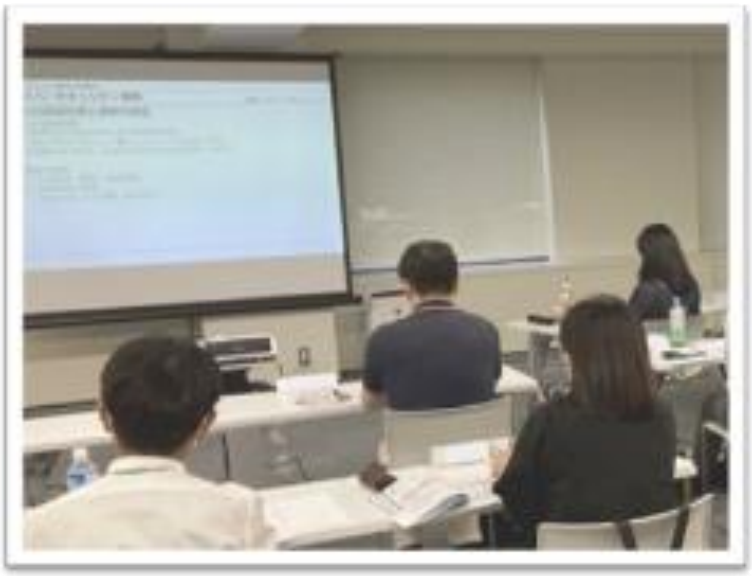
“仮想会社の 10 大脅威に対する対策例を確認しよう”

資料「10 大脅威対策例」（次ページへ掲載）を確認し、その内容とワークショップ１の結果との違い、新たに気づいたこと、また、自社で対応する場合にハードルになりそうなことなどについて議論します。

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

- ワークショップを通じて、サイバーセキュリティの脅威に対する対策方法を学びました。
- 10 大脅威についての議論を通じて、セキュリティの課題を考えることができました。
- 様々な意見を聞きながら、具体的な対策について議論できました。
- 社内で実践できるセキュリティ対策やアプローチについてのヒントを得ることができました。
- セキュリティへの取り組み方、予算の取り方、経営者へのアプローチなど、企業規模に合わせたアプローチを学びました。
- グループメンバーの様々な業界や業種からの意見を聞けたことで、セキュリティ対策の多様性に気づきました。業態に応じたハードルや課題があることを理解しました。
- 対策の優先順位づけや、リスクの発生頻度と影響度の評価について学びました。費用の配分に関する知識も得ました。
- セキュリティ対策において、資本力が重要であることを実感しました。また、社員教育が有効で、費用面でも実施しやすい対策であることに気づきました。

セミナー・ワークショップ風景



参加者の皆様が熱心にセミナーを受講し、新たな知識を獲得中。

登壇中の星野講師

＜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 3 回ワークショップ資料： 10 大脅威対策例

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。

(出典) IPA「情報セキュリティ 10 大脅威」を基に作成

IPA.”情報セキュリティ 10 大脅威 2023”. https://www.ipa.go.jp/security/10threats/ps6vr70000009r2f-att/kaisetsu_2023.pdf , (2023-09-11).

運営事務局より編集後記

9 月に入り、朝夕は秋の風が感じられる季節の中、第 3 回セミナー・ワークショップが開催されました。皆様の熱心な参加と積極的な姿勢に感謝申し上げます。

前回までの学びを活かし、今回のセミナーでも参加者の皆様が講師の話に深く共感し、メモを取る一生懸命さが目立ちました。ワークショップでは、熱心な意見交換が行われ、グループ発表では多彩なアイデアが披露されました。

国が掲げる「自由、公正かつ安全なサイバー空間」 の確保に向け、当事業は引き続き、セキュリティ対策に関する情報の普及に努めて参ります。

運営事務局一同

9 月の風景『都心のキバナコスモス』

次回（第４回）セミナー・ワークショップのご案内

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
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

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