

中小企業も狙われる今、
サイバー攻撃にどう対応する？

中小企業

サイバーセキュリティ対策事業

サイバーセキュリティ対策はもうお済みですか？

東京都では、セキュリティ対策をまだ実施していない企業から、
一定程度のセキュリティ機器・ソフトウェアを導入し、
情報セキュリティポリシーを整備済みである企業まで、
貴社の状況に合わせて**5つの事業**で包括的にサポートを実施いたします。

貴社はどのレベル？

サイバーセキュリティ 対策成熟度診断

START

サイバー
セキュリティ
対策は必要だ

サイバー攻撃を
身近に感じる

設備・ソフト等の
導入を検討して
いるところだ

セキュリティへの意識がなく、
対策等も考えていない

そんな方には 啓発事業

セキュリティ対策をしたいが、
何から始めたらよいかわからない

そんな方には 基本対策事業

設備・ソフトを
導入しており
規定・ルールも
定めている

設備・ソフトを
導入しているが
規定・ルールは
まだない

基本的な対策はしているが、
次に何をしたらよいかわからない

そんな方には 社内体制整備事業

今の規定・
ルールで大丈夫か
確認したい

専門家にアドバイスをもらい
ながら、インシデント対応力を
強化したい

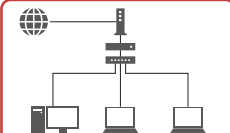
そんな方には 特別支援事業

フォローアップ事業



東京都産業労働局

5つの事業でサイバー攻撃への対応をサポートいたします!!

ベーシックなサポート		事業の内容やスキーム		期待できる効果		
レベル 1	サイバーセキュリティ啓発事業 ■ セキュリティ対策をこれから検討する中小企業へ、意識醸成を促し、セキュリティ対策の実践を後押しします。 	①サイバー攻撃対応演習セミナー 経営層向け - サイバー攻撃被害時の損失額のシュミュレーション - セキュリティインシデント発生時の対応 ②標的型攻撃メール訓練 従業員向け - 標的型攻撃メールを疑似体験する訓練を実施 - 訓練結果の分析とフィードバック ③ネットワーク調査・構成図作成(専門家派遣) セキュリティ担当者向け - 環境を調査し、ネットワーク構成図を作成・提供する - リスクを洗い出し、専門家から指導・助言  ☒ 現状の把握 ☒ リスクの洗い出し	セキュリティ対策を「経営課題」として認識し、予算化する 従業員全体のセキュリティ意識向上(意識醸成) セキュリティ機器の必要性を理解し、導入を検討する			
レベル 2	サイバーセキュリティ基本対策事業 ■ 機器・ソフトウェア等の導入支援や社内ルールの策定を専門的にサポートします。 3か月間無償体験 	①セキュリティ機器(UTM)の試行導入 - UTM(統合脅威管理)とは複数のセキュリティ機能を1つの機器で管理する手法や製品のこと  基本的にはここで防御できる ②セキュリティソフトウェア(EDR)の試行導入 - EDRとはUTMで防ぎきれなかった脅威に対して早期検知・保護するためのツールやサービス 	自社がどれくらいサイバー攻撃を受けているかを確認し、セキュリティ機器の導入や運用ノウハウの提供によって、基本的な対策を構築する SECURITY ACTION 二つ星宣言を達成できる			
レベル 3	サイバーセキュリティ社内体制整備事業 ■ セミナーやワークショップを通じて、人材を育成し、継続的なサイバーセキュリティ対策の自走化を実現します。 	①サイバー人材育成支援セミナー - 自社でセキュリティ対策を計画的に実行できる知識・ノウハウが身に付くセミナー ②課題解決型実践ワークショップ - セミナーで得た知識を基に、グループメンバーで課題や取組事例、問題点を共有し、ディスカッション ③自社の課題を解決する専門家の派遣 - セミナーやワークショップで洗い出した課題解決に向けて専門家が現地に赴き、サポート 	セキュリティ対策ができる人材を育成し、自社内での体制を強化する			
プラスαのサポート		① 専門家を派遣して貴社の実情に応じて「CSIRT構築」や「IT-BCP策定」を支援		体制構築や演習を通じて、自社の実践的なインシデント対応力を強化する		
レベル 3~		サイバーセキュリティ特別支援事業 ■ インシデント発生時の円滑な対応・復旧、被害軽減に向けて、実践的な対応力を強化します。 		インシデント対応機能を重視する企業には CSIRT構築コース セキュリティインシデントが発生した場合に備えて、準備から初動対応までの一連の対応を行う組織(機能)を構築します。 ②構築した体制等を踏まえ、インシデント対応机上演習を実施	企業継続性を重視する企業には IT-BCP策定コース サイバー攻撃などのセキュリティ被害を受けた際に、IT-BCPを発動し、業務再開からITシステムが復旧するまでの計画を策定します。	実際にインシデントが発生した際には、サイバー攻撃等による被害の低減や企業活動の早期復旧を実現する

全レベル共通

サイバーセキュリティフォローアップ事業

■ 専門家派遣によるセキュリティ対策の見直しやレベルに合わせたコンテンツを提供することでセキュリティ対策の継続を支援します。



① セキュリティ対策点検

1回コース

メンテナンスのために点検をご希望の企業様向けです。セキュリティ状況を確認し、調査結果を専門家に分析。ご訪問時に必要なサポートを実施します。

3回コース

セキュリティ対策に対する課題を解決したい企業様向けです。セキュリティ状況を確認し、1回目のご訪問時に詳細をヒアリング。全3回の訪問を通じて課題解決に向けたサポートを実施します。

■ サポートの流れ

Webからお申し込み

セキュリティ状況の確認

1回コース

3回コース

② 情報発信・提供

各機関から情報収集・情報コンテンツの作成

ポータルサイト発信

メルマガ配信

セミナー開催

詳しくは、裏表紙「ポータルサイト」東京都の取組のページをご覧ください。

「中小企業向けサイバーセキュリティ対策の極意」ポータルサイト

東京都では、中小企業のセキュリティ対策に役立つコンテンツ等を提供したり、各種支援事業を実施しています。また、都内の中小企業者等を対象としてサイバーセキュリティに関する無料相談窓口を開設していますので、お気軽にご相談ください。

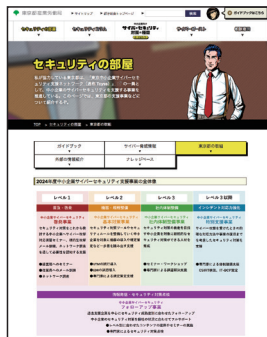


下記、電話・窓口以外にWebサイト専用フォームでのご相談もできます！



セキュリティの部屋

中小企業が緊急に対応すべきサイバーセキュリティ情報や、必ず押さえておくべき情報を提供します。



東京都の取組

東京都が実施しているサイバーセキュリティ対策支援事業などについて紹介しています。



TOPページ

TOPページはこちら



サイバー脅威

サイバー攻撃の種類や特徴を紹介するページです。



相談窓口

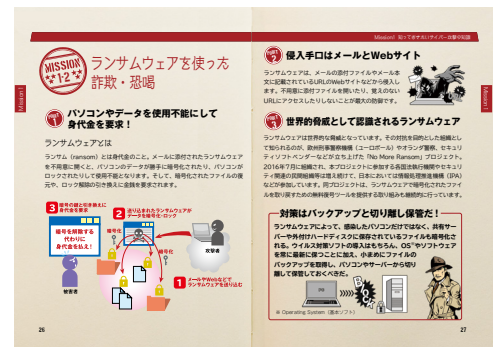
情報セキュリティ対策の強化や、情報流出等に関するご相談を受け付けています。

お役立ち資料の提供

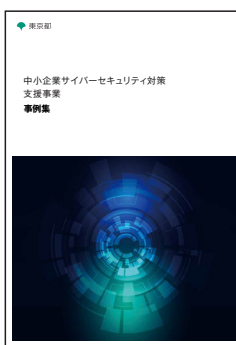
下記資料以外にも右下のQRコードよりPDF版をダウンロードできます



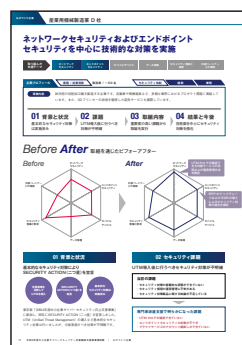
「中小企業向け サイバーセキュリティ対策の極意」
中小企業がサイバー攻撃について必ず行うべき対策や事故が発生した場合の初期対応などを分かりやすく解説したサイバーセキュリティ対策ガイドブックの決定版。



「中小企業向け サイバーセキュリティ 実践ハンドブック」
組織内におけるシステム管理者等(システム管理などの実務に責任を持つ方々)向けに自組織の状況に応じて必要な対策を選択して実践するための参考書。ぜひ、ご活用ください。



「中小企業向け サイバーセキュリティ対策 支援事業 事例集」
サイバーセキュリティ対策支援事業の参加企業における具体的な支援・取組などについて紹介。様々な事例からヒントを見つけて、貴社でのセキュリティ対策の実践にお役立ていただけます。



東京都産業労働局

東京都産業労働局商工部 相談窓口
東京都新宿区西新宿2-8-1 都庁第一本庁舎20階北側

TEL 03-5320-4773

電話・窓口
受付時間

都庁開庁日 9:00～12:00 / 13:00～17:00

Webサイト専用フォームでのご相談はこちら

WEB

<https://www.cybersecurity.metro.tokyo.lg.jp/>



R250
古紙パルプ配合率50%再生紙を使用

リサイクル適性(A)
この印刷物は、印刷用の紙へリサイクルできます。

登録番号 (6)78