サイバーセキュリティの課題を
解決できる人材の育成をサポート

人材育成と実践的課題解決で中小企業のセキュリティ対策を継続的に強化！

サイト訪問者数 25,000 人突破！

集計期間：令和6年5月23日～現在

事業イメージ動画をチェック

中小企業サイバーセキュリティ社内体制整備事業について

ABOUT

当事業について

参加メリット

自社でセキュリティ強化や
課題解決ができるようになる

他の参加企業の状況や
事例を知ることができる

次に追加導入すべき
機器やソフトの選び方が分かる

セキュリティ対策を継続する体制がで
取引先からの信頼獲得につなが

セキュリティ情報

【IPA】情報セキュリティ10大脅威2025について
2025.02.04

『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
https://www.cybersecurity.metro.tokyo.lg.jp/
2024.05.23

【IPA】情報セキュリティ10大脅威2024について
2024.06.19

お知らせ

令和6年度「中小企業サイバーセキュリティ基本対策事業」に本年度参加された企業の事例を公開。
2025.02.27

令和6年度「中小企業サイバーセキュリティ特別支援事業」に本年度参加された企業の事例を公開。
2025.02.20

令和6年度「中小企業サイバーセキュリティ特別支援事業」に本年度参加された企業の事例を公開。
2025.02.20

令和6年度「中小企業サイバーセキュリティフォローアップ事業」に本年度参加された企業の声を紹介。
2025.02.20

毎年2月1日～3月１８日は【サイバーセキュリティ月間】です。
期間中には、セキュリティ対策に関する『中小企業向けセミナー』が開催されます。
2025.02.19

令和6年度「中小企業サイバーセキュリティ社内体制事業」第10回セミナー資料を掲載しました。
2025.01.21

令和6年度「中小企業サイバーセキュリティ社内体制事業」第9回セミナー資料を掲載しました。
2024.12.17

【年末年始休業のお知らせ】誠に勝手ながら、下記の期間は運営事務局の年末年始休業とさせていただきます。

■年末年始休業期間　2024年12月30日(月)～2025年1月3日(金)

2024.12.02

令和6年度「中小企業サイバーセキュリティ社内体制事業」第8回セミナー資料を掲載しました。

2024.11.19

令和6年度「中小企業サイバーセキュリティ社内体制事業」第7回セミナー資料を掲載しました。

2024.10.22

【IPA】夏休みにおける情報セキュリティに関する注意喚起について

2024.08.09

・【 夏季休業のお知らせ】誠に勝手ながら、下記の期間は運営事務局の夏季休業とさせていただきます。
■夏季休業期間　2024年8月13日(火)～15日(木)の3日間

2024.07.23

・令和６年度「中小企業サイバーセキュリティ特別支援事業」参加企業の募集締め切り

2024.07.03

・令和６年度「中小企業サイバーセキュリティフォローアップ事業」参加企業の募集を開始

2024.07.01

・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」参加企業の募集締め切り

2024.06.28

・令和６年度「中小企業サイバーセキュリティ基本対策事業」参加企業の募集を開始

2024.05.30

・令和６年度「中小企業サイバーセキュリティ啓発事業」参加企業の募集を開始

2024.05.30

・令和６年度「中小企業サイバーセキュリティ特別支援事業」参加企業の募集を開始

2024.05.23

・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」参加企業の募集を開始

2024.05.23

中小企業サイバーセキュリティ社内体制整備事業について

本事業では、基本的なセキュリティ機器を備え、セキュリティに関する方針、ルール、対策を決めるところまでは実施したものの、その先どうしたらいいのか分からない、自社だけでは対策ができないという中小企業を対象に、セキュリティ対策の基本を再確認し、課題解決などの手法を学ぶことで継続的なセキュリティ対策ができる人材を育成します。

また、支援実施過程で使用するテキストや事例集など、本事業の取組を広く社会へ公開し、中小企業の皆様が自社でセキュリティ対策を実行する際、困った時に使うことができるツールとして活用していただくことで、中小企業全体の体制強化を目指

当事業の対象

社内にてセキュリティ対策を継続的に実施することを想定した実践的な講座内容であることから、既にUTMやEDRなど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中小企業を対象とします。

レベル1

普及・啓発

中小企業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サイバー攻撃対応演習セミナー、標的型攻撃メール訓練、ネットワーク調査を通して必要性を認知する支援を行います。

啓発事業

レベル2

機器・規程整備

中小企業サイバーセキュリティ

基本対策事業

セキュリティ対策をこれから始める中小企業に対し、機器の導入や規定策定など一歩目を踏み出す支援を行います。

基本対策事業

レベル3

社内体制整備

中小企業サイバーセキュリティ

社内体制整備事業

セキュリティ対策の自走を目指す中小企業を対象に、継続的なセキュリティ対策ができる人材を育成します。

社内体制整備事業

レベル3以降

インシデント対応力強化

中小企業サイバーセキュリティ

特別支援事業

サイバー攻撃を受けたときの的確な対応方法や事業の復旧までを考慮した、セキュリティ対策を支援します。

特別支援事業

情報発信

中小企業サイバーセキュリティ

フォローアップ事業

中小企業のセキュリティ対策を個社の状況に合わせてフルサポート。
段階的なさまざまな取組で中小企業全体のセキュリティ対策強化を目指します。

フォローアップ事業

当事業の特徴

４つの取組みでセキュリティ対策の継続をサポート！
次にどうしたらいいか分からない状態を解消します！

01 セキュリティ業務経験が豊富な講師によるセミナー

導入済のセキュリティ機器の日常的な運用方法や業務内容に沿ったセキュリティルールの策定方法など、中小企業の皆様が自主的にセキュリティ対策業務を運営する上で生じる疑問点の解決に直接役立つ、実践的な知識・ノウハウを講義形式でお伝えします。

02 参加企業間のディスカッションで知見を広げられるワークショップ

中小企業の皆様が直面しているセキュリティ対策上の困難について、参加企業の皆様同士で、それぞれの課題に一緒に取り組み、解決策を考えるワークショップを実施します。自社の問題だけでなく、他社の事例に触れることで、様々な課題の解決に向けた引き出しとなる知識を得られます。

04 参加者同士のネットワーク形成をサポート

セミナーやワークショップを通じた参加者間のコミュニケーションの活性化に向けたサポートに加え、オンラインコミュニティで学習成果やプロセスなど、タイムリーに情報をシェアし、参加者同士で知識やノウハウを高め合える環境を提供します。

03 課題解決の支援を行う 専門家を派遣

参加企業へ専門家を派遣し、ワークショップで洗い出した課題を中心に、企業が直面しているセキュリティ上の問題点解決や、社内体制構築へ向けた支援を行います。

募集概要

申込締切	お申し込みは終了しました。
支援対象	・東京都内に主たる事業所を有する中小企業者（会社及び個人事業者） ※中小企業基本法で定める中小企業者

・既にUTMやEDRなど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

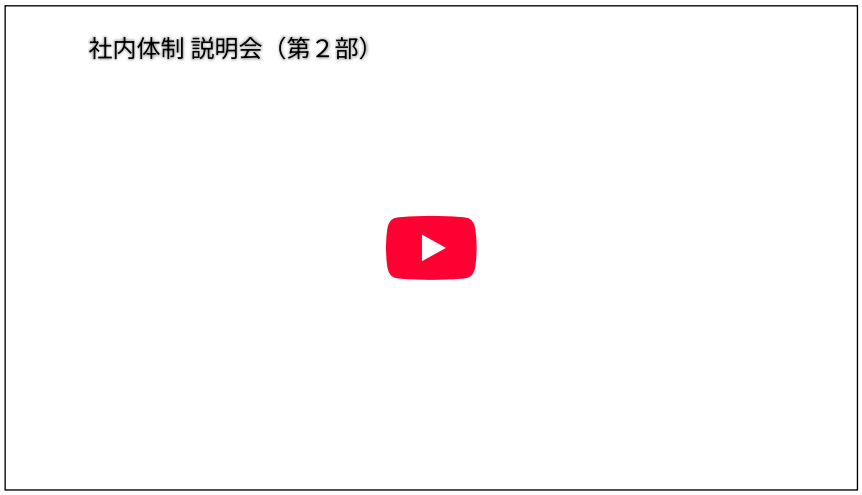
である中小企業者

受講対象	・本事業における取組に意欲的に参加できる経営者、セキュリティ担当者等 ・事業への参加者ご自身と、所属企業のご同意をいただける方 ※参加人数は1社につき1名とさせていただきます。 ※原則、受講者の途中変更や代理出席はできないこととしますが、やむを得ない事情がある場合、運営事務局までご相談ください
募集企業	40社（小売・卸売枠：10社程度、建設・製造枠：10社程度、サービス・その他枠：20社程度） ※業種ごとの募集枠を設定します。なお、各枠の社数は目安となりますので、応募状況により変動することがあります。
支援期間	約7か月間（セミナー・ワークショップ・専門家派遣）
参加費用	無料
会場	東京都新宿区西新宿1-22-2 新宿サンエービル内ビジョンセンター西新宿会議室

募集要項[PDF1.78MB]

事業説明会について

本事業の特徴や支援内容の概要、メリットなどを伝える説明会を実施しました。
当日の様子を動画にてご覧ください
※「【第2部】　事業説明　中小企業サイバーセキュリティ社内体制整備事業について」の内容となります。



日程	全日程終了しました。 ①令和6年6月6日（木）14:00～15:30（90分） ②令和6年6月12日（水）14:00～15:30（90分） ③令和6年6月18日（火）14:00～15:30（90分）
開催方式	オンライン開催（Zoom）
参加費	無料
プログラム	【第1部】　ミニセミナー「DXのセキュリティ対策実現に向けて　～中小企業向け体制整備のポイント～」 ＜内容＞ ・中小企業のDX推進における必要性、およびその際に必要なセキュリティ概念をご説明します ・セキュリティ機器設置等の整備だけでなく、社内の体制整備に必要な知識、ノウハウ等の情報を具体的な事例を交えて解説します。 【第2部】　中小企業サイバーセキュリティ社内体制整備事業について ＜内容＞ ・事業概要や参加要件などを解説します。
定員	各回100名程度
申込方法	お申し込みは終了しました。

事業説明会資料［PDF1.82MB］

SUPPORT

支援内容

本事業では、セミナーやワークショップの取組を通じて、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だけでなく、参加企業同士のディスカッションを通じたセキュリティ課題の洗い出しや、専門家派遣による課題解決へのサポートを通じ、セキュリティ機器の運用や業務に直結した社内規程の整備に取り組む際に、次に何をしたらいいか分からない状態を解消し、本事業の参加後には、自力でセキュリティ対策計画が立てられるようになることを目指します。また、DX推進に必要なセキュリティの考え方・サプライチェーン対策などの最新のトレンド情報も学ぶことができます。

セミナー・ワークショップ　全10回　令和6年7月～令和7年1月

セミナーでは、セキュリティ対策の知識だけでなく、役割の違いやDXの推進といった、今後の中小企業のセキュリティを担う中心人物を育成します。ワークショップでは、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、他社の事例に

対して全員で対策を検討・議論します。多様なセキュリティ課題を疑似体験することで、未知の課題にも対応できるようになります。また、インシデント等を題材とした事例に基づく演習により今後発生しうる課題への対応力や実践力を強化します。

1回目	2回目	3回目	4回目	
7月23日（火）	8月6日（火）	8月20日（火）	9月10日（火）	9[illegible]
セミナー資料を見る	セミナー資料を見る	セミナー資料を見る	セミナー資料を見る	[illegible]

6回目	7回目	8回目	9回目	10回目
10月8日（火）	10月22日（火）	11月19日（火）	12月17日（火）	1月21日（火）
セミナー資料を見る	セミナー資料を見る	セミナー資料を見る	セミナー資料を見る	セミナー資料を見る

全10回のセミナーで学べるテーマ・内容

テーマ	概要
サイバーセキュリティを取り巻く背景	クラウドワークロードが複雑化し、サプライチェーンの脆弱性が狙われ、生成AI・IoT・DXなどの新しいテクノロジーへのセキュリティ対策が求められている現状を解説します。Society5.0等で示されている社会の方向性と実現に向けた基本概念を理解するとともに、その環境下で中小企業に求められるセキュリティ対策の考え方を理解することを目的とします。
中小企業に求められるデジタル化の推進とサイバーセキュリティ対策	重大なインシデント発生から課題解決までを事例で理解するとともに、IT活用、サイバーセキュリティ対策の必要性を解説します。
これからの企業経営に必要なIT活用とサイバーセキュリティ対策	企業経営に必要なIT活用、サイバーセキュリティ対策について、フレームワーク等を参考に、組織の現状と目標に応じた対策手段を解説します。
セキュリティ事象に対応して組織として策定すべき対策基準と具体的な実施	インシデント事例に対応したレベル別の具体的な対策方法と対策手順の作成について解説します。
各種ガイドラインを参考にした対策の実施	関係機関から提示されている各種サンプル、ひな形をベースとした具体的な対策方法を解説します。
ISMS等のフレームワークの種類と活用法の紹介	組織全体にわたるセキュリティの向上を図るために、各フレームワークの概要と活用法について解説し、損失となりうるサイバーセキュリティのリスクへの効率的な対策を施すために必要なリスクマネジメントの方法を解説します。

ISMSの構築と対策基準の策定と実施手順	ISMSに準拠して、自社に必要な管理策を選 策基準を策定し、策定した対策基準の実施手 で解説します。中小企業の規模・立ち位置、リ ト結果等に応じて、必須・選択式の事項と判 対策（組織、人、物理、技術）の実施手順を学 キュリティ対策を実施した結果の評価方法を
ISMSの具体的な構築・運用の実践	作成した実施手順に沿った具体的な対策（実装・運用）を、国内外の中小企業向けのガイドラインの中から、優先的に実施すべき内容を選び解説します。対策（組織、人、物理、技術）の実施手順に沿った具体的な手順のポイントや、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を学びます。
中小企業が組織として実践するための スキル・知識と人材育成	サイバーセキュリティ対策を実践するためのスキル・知識の理解を目的とします。ITおよびデジタル人材に必要なスキル（ITSS+、Di-Lite（デジタルリテラシー領域）、プラス・セキュリティ等）と知識を持った人材育成・人材確保について解説します。また、チェンジマインド、リスクキリングを含めた実施計画および教育・研修の実施内容について、ITおよびデジタル人材のスキル、知識の認定制度と活用方法を学びます。
全体総括	これまでの内容を振り返り、重要な知識を定着させることを目的とします。また、受講者が今後のセキュリティ活動において、自走できるために必要な考え方、経営者等に説明するための組織として実施すべき事項と概要について解説します。

ワークショップ内容

テーマ紹介と目標設定 | **グループ討議** | **個別発表と質疑応答** | **講師のコメントとフィードバッグ** | **意見交換とアクションプラン**

テーマ	概要
第1回：自社のIT活用とセキュリティ事情の検討	・自社のIT活用状況と、 生成AIなど近年のトレンドを踏まえた今後の課題を検討 ・自社のセキュリティ状況と、 セキュリティの知識向上に向けた今後の課題を検討 ・自社の状況分析を基にグループでの意見交換、協議、発表
第2回：インシデント事例を活用した対策基準の検討	・最新のインシデント事例を踏まえた対策基準の検討 ・最新のガイドラインを参考にした対策基準の検討

	・インシデント事例、ガイドラインを基に グループでの意見交換、協議、発表
第3回：資産台帳作成およびリスクアセスメント（机上演習）	・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 ・リスクアセスメントを実施し、リスクレベル ・仮想会社を基にグループでの意見交換、協
第4回：対策基準の作成（机上演習）	・リスクアセスメントの結果をもとに必要な管理策を検討 ・管理策をもとに対策基準および適用宣言書を作成 ・仮想会社を基にグループでの意見交換、協議、発表
第5回：実施手順の策定（机上演習）	・対策基準を参考に実施手順を作成 ・仮想会社を基にグループでの意見交換、協議、発表
第6回・第7回：実施手順に沿った具体的な対策の検討（机上演習）	・実施手順を実践するため、情報セキュリティリスク対応計画書を作成 ・仮想会社を基にグループでの意見交換、協議、発表
第8回・第9回：人材確保の検討	・求める人材・スキルの設定 ・実施計画書の作成 ・教育・研修の実施内容検討 ・自社の状況分析を基にグループでの意見交換、協議、発表
第10回：振り返りおよび経営者に対する説明事項の検討	・セミナーやワークショップを振り返り、 組織として実践すべき事項の検討 ・経営者に対して実践すべき事項を説明するために 必要な事項の検討 ・自社の状況分析を基にグループでの意見交換、協議、発表

講師紹介

星野 樹昭（ほしの しげあき）氏

専門分野　ITインフラ設計・構築・テスト、移行設計、セキュリティ製品導入支援、ISMS導入支援

業務経験　25年（セキュリティ経験 ：20年）

保有資格　CISSP、情報処理安全確保支援士（登録番号 第002047号）、MCP

官公庁や金融機関などの大規模環境から、中小企業規模まで、オンプレ/クラウド問わず様々な環境のITインフラ環境導入・移行の経験あり。セキュリティ製品の導入支援では、DB暗号化ソフトウェアやWeb Application Firewall、クライアントPCのセキュリティ対応など、実績豊富。現在はISMSコンサルも実施しており、活動は多岐にわたる。

専門家派遣　全4回　令和6年7月～令和7年1月

参加企業の皆様が、ワークショップを通じて洗い出した課題の解決に向け、多様な得意分野を持つ専門家が、皆様の
現場の状況に対応したサポートを実施します。セミナー・ワークショップで得た気づきや知識を活かし、参加企業の皆
立案できるようアドバイスを行います。1回あたりの支援時間は2時間程度、全4回の支援を予定しています。

専門家派遣支援イメージ

1回目	2回目	3回目	4回目
参加企業の状況をヒアリングします。解決すべき問題を決めて、課題の洗い出しと解決までの道筋を検討します。	課題解決に向け、実施することを明確にします。また、スケジュールを共有し、解決へ向けたスタートを切れるようにします。	セミナー・ワークショップで得た知識を活かし、中小企業の皆様が自ら考え行動できるようにフィードバック、フォローします。	中小企業の皆様が考えた次年度以降のスケジュールやリスク検討をフィードバックして、不明点・不安点が残らないようにします。
支援時期：参加決定直後～セミナー・ワークショップ開始後	支援時期：セミナー・ワークショップ開始後	支援時期：セミナー・ワークショップ中盤～終盤	支援時期：セミナー・ワークショップ終了後

FLOW

参加の流れ

お申し込みは終了しました。

事業説明会へ参加

※説明会への参加は必須ではございませんが、先ずは説明会で事業内容をよくご確認された上でお申し込みをいただくことをお勧めします。

事業参加申込フォームに必要事項を入力し送信

受信後、事務局よりご連絡

※セキュリティレベルが本事業の対象であることを確認させていただきます。また、参加にあたっての想定や遵守事項をご説明した上で申込完了となります。

令和6年6月28日（金）応募締切

お申し込みは終了しました。

参加同意書・機密保持の同意書提出

※参加同意・機密保持の同意書の提出をもって参加確定となります。

参加確定

Q&A

よくある質問

Q 本事業への参加要件を教えてください。

A 参加要件は、都内に主たる事業所を有する中小企業であり、一定のセキュリティレベルを有することです。詳細については募集要項をご確認ください。

Q 本事業で求められるセキュリティレベルとはどのようなものですか？

A 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ことを要件としています。
①セキュリティ機器・ソフトウェアのレベルとしてUTMやEDRがあります。

・UTMとは、ファイアウォールやアンチウィルスなど、複数のセキュリティ対策機能を統合し、社内ネットワークを経由する通信を1台で多層防御できるセキュリティ製品です。

・EDRとは、パソコンやサーバなどのエンドポイントを監視し、ウィルスが侵入した際に素早く検知、対応を行うことで被害を防ぐセキュリティ製品です。

②情報セキュリティポリシー（社内セキュリティ規程）のレベルとして、IPAのSECURITY ACTION二つ星宣言があります。
「SECURITY ACTION」は中小企業自らが、情報セキュリティ対策に取組むことを自己宣言する制度です。

・SECURITY ACTION二つ星宣言とは、IPAの「5分でできる！情報セキュリティ自社診断シート」に基づきセキュリティポリシーを策定し、外部に公開したことを宣言することです。詳細は、こちらをご覧ください。

Q 参加要件を満たしていれば必ず参加できるのでしょうか？

A 申込企業が多数の場合は、抽選となります

Q セミナー・ワークショップは、すべての回に参加が必要ですか？

A はい。全10回のご参加をお願いしております。

Q セミナー・ワークショップはオンラインで参加可能ですか？

A 原則として会場参加となりますが、やむを得ない事情が発生した場合は運営事務局までご相談ください。

Q セミナー・ワークショップについて、複数名での参加は可能ですか？

A 1社1名様でのご参加をお願いしております。

Q 参加費用はかかりますか？

A 参加費用はかかりません。
ただし、交通費・通信費等は参加企業の自己負担となります。

Q 事例集に掲載される情報に社名は掲載されますか？

A 企業名や担当者の個人名は掲載せず、内容に関して参加企業が特定できないようにいたします。

東京都「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（電話受付 平日 9:00～17:00）
メール：ade.jp.shanaitaisei@jp.adecco.com
主催：東京都　※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。

お電話でもご相談いただけます
0120-138-166
受付時間 9:00～17:00（平日のみ）

東京都　東京都産業労働局