

当事業について



支援内容



募集概要



よくある質問



お問い合わせ



自社のセキュリティ環境の実態を把握

基本方針の策定から機器導入まで、
セキュリティの専門家がフルサポート

サイト
訪問者数 **16,000** 人突破!

集計期間: 令和6年5月30日~現在



ABOUT

当事業について

中小企業サイバーセキュリティ基本対策事業

中小企業サイバーセキュリティ基本対策事業では、ウイルス対策ソフトやファイアウォールなどでは対応しきれない、不正アクセス・侵入に対する防御に有効なセキュリティ機器(UTM)やセキュリティソフトウェア(EDR)の導入に向けて、その機能が無償で3か月間程度体験できる機会を提供します。SECURITY ACTION二つ星宣言を目指し、サイバーセキュリティに関する基本方針や社内規定の策定のサポートを実施します。

また、企業のセキュリティ環境を調査し、今後の対策に向けて指導・助言する情報セキュリティマネジメント指導支援も提供します。

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

2024.05.30

お知らせ

本年度参加企業の事例を公開しました。

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

【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

【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

「第2部 東京都中小企業サイバーセキュリティ基本対策事業について」の事業説明会動画を公開しました。

2024.07.26

【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...
10 フォロワー

セキュリティ情報ポータルサイトをフォロー
ページをフォロー

中小企業向け
サイバーセキュリティ
対策の極意

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
約5ヶ月前

【東京都セキュリティ事業参加企業向けセミナー・懇親会に追加で30名様をご招待!!】
この度東京都が主催する、サイバーセキュリティ対策に取り組む企業向けの特別イベントに抽選で30名様をご招待するキャンペーンを開催いたします！

■キャンペーン実施期間
令和6年10月29日(火)～11月7日(木) ...
もっと見る

「いいね！」 コメントする シェアする

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社内体制整備事業」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特別支援事業」参加企業の募集を開始
2024.05.23

SERVICE

支援内容

支援① UTM機器設置

UTM(統合脅威管理)とは、複数の異なるセキュリティ機能をひとつのハードウェアに統合した機器のことです。企業の皆様の社内ネットワークの出入口に設置することで、包括的に社内ネットワークを保護する機能を持ち、出入口対策として、不正な通信を検知・ブロックすることが可能です。

ポイント

UTM機器を最大3か月間無料体験でき、期間中はサポートデスクによる支援を実施

支援② EDR導入

EDRは社内ネットワークを保護するためのファイアウォールやUTM、アンチウイルスソフトで検知・ブロック出来なかった悪意のある外部からの攻撃やマルウェアといった不正プログラムの動きを検知・対策します。

本事業のEDRはクラウドの技術を使い、ファイアウォールやUTMなどに守られていないテレワーク環境の端末でも検知・対策が可能となっています。

ポイント

EDRを最大3か月間無料体験でき、期間中はサポートデスクによる支援を実施

支援①+支援② UTM機器とEDR導入のイメージ

専門家による事前診断で、現状のセキュリティ環境をチェック!



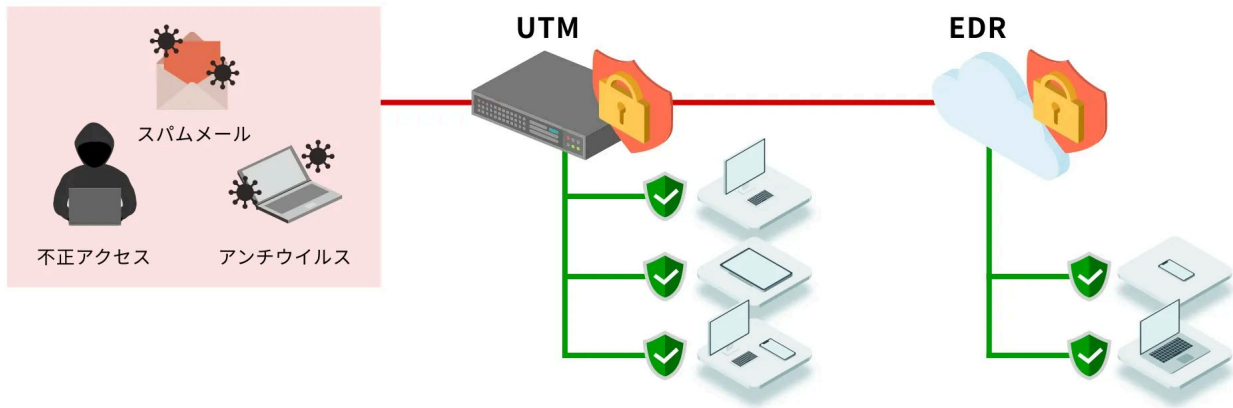
UTM機器

無料で最大3か月間、UTMを設置して各種サイバー攻撃の状況を確認、出入口対策の効果を実感

EDR

無料で最大3か月間、EDRを導入し、エンドポイントに侵入したサイバー攻撃を検知し、迅速な対応を図る

- 1 様々な脅威（ウイルス、不正アクセス、スパムメール）が侵入
- 2 UTM（セキュリティ機器）を設置してネットワークを防御
基本的にはここで防御できる
- 3 UTMで防ぎきれなかった脅威に対して、EDRによって各デバイスを防御

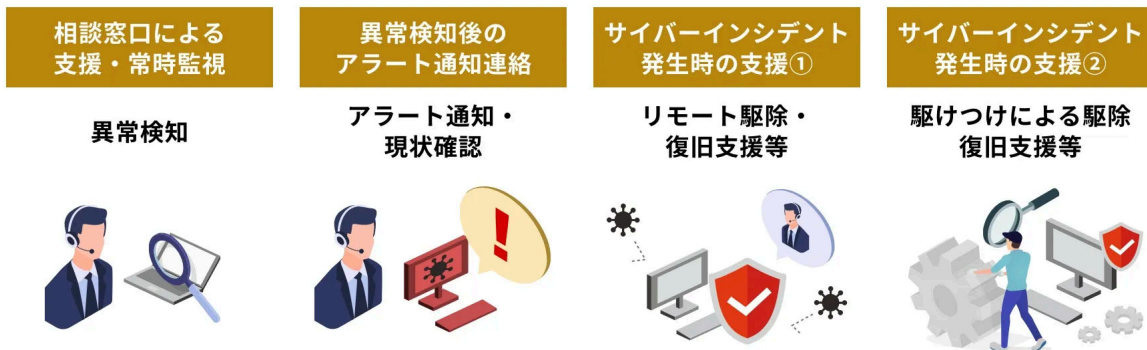


UTMとEDRによるインシデント対応(3か月程度)

支援期間中はUTM、EDRサービス利用者向けのサポートデスクの機能も無料で体験可能!

サイバー攻撃を受けた際、インシデント診断・遠隔除去を実施

[対応期間:無料体験の期間中、24時間対応(休日も含む)]



UTM機器設置/EDR導入の流れ


STEP 01

STEP 02

STEP 03

STEP 04



お申し込み	現在のセキュリティ状況の確認	<p>支援①:UTM機器設置 (50社)</p> <ul style="list-style-type: none"> ・UTM機器設置工事 ・UTM機器によるインシデント対応 (最大3か月) <p>支援②:EDR導入 (50社)</p> <ul style="list-style-type: none"> ・EDRクラウドシステムのインストール ・EDR導入によるインシデント対応 (最大3か月) 	<p>事後サポート</p> <p>本事業実施後のアンケートによる振り返りや、事業時のQ&Aなどを通じて、セキュリティ環境の見直しやセキュリティ対策のサポートを実施</p> 
-------	----------------	--	--

支援③情報セキュリティマネジメント指導

知識レベル・対応品質・事務作業の品質に優れた専門家を派遣して、最大4回の支援を実施。セキュリティに関する基本方針や規定等の策定を通じて「SECURITY ACTION二つ星宣言」を目指します。

STEP 01 お申し込み	STEP 02 現在のセキュリティ状況の確認	STEP 03 <p>支援③:情報セキュリティマネジメント指導 (100社)</p> <ul style="list-style-type: none"> ・専門家とともにセキュリティ診断・ポリシー作成など、個社ごとに実施(最大4回) ・SECURITY ACTION二つ星宣言を目指すようサポート 	STEP 04 <p>事後サポート</p> <p>本事業実施後のアンケートによる振り返りや、事業時のQ&Aなどを通じて、セキュリティ環境の見直しやセキュリティ対策のサポートを実施</p>
------------------	---------------------------	---	---

専門家派遣のイメージ			
1回目	2回目	3回目	4回目
<p>情報資産管理状況の確認 リスク洗い出し</p> <p>専門家によるセキュリティリスクの分析・コンサルティングを通じて、社内セキュリティ対策の構築をサポート</p>	<p>対策の決定 基本方針の策定見直し</p> <p>整理された情報をもとに具体的な対策と運用に向けた情報セキュリティ基本方針の策定・見直しができる状態にする</p>	<p>関連規定の策定 見直しに向けた検討</p> <p>新たな情報セキュリティ基本方針案が決まり、SECURITY ACTION二つ星宣言が実施できる状態にする</p>	<p>関連規定 実施計画書のレビュー</p> <p>情報セキュリティ基本方針ならびに実施計画書を作成し、本支援後に実施すべきセキュリティ対策を明らかにする</p>

SECURITY ACTION 二つ星宣言について

経済産業省のIT政策実施機関であるIPA(独立行政法人情報処理推進機構)が定めるSECURITY ACTION 二つ星宣言は、中小企業自らが情報セキュリティ対策に取り組むことを宣言する制度です。

社内で事前にセキュリティ基本方針や規程を準備し、それに沿った行動方針について予め定めておくことで、実際に攻撃を受けた際に適切な対応を取ることができます。

二つ星宣言をしておくことで、情報セキュリティへの自社の取組を取引先等にアピールすることもでき、信頼の獲得にもつながります。



機密資料以外にも技術情報を含む加工データの保護対策に繋がる

自社の「セキュリティ対策の取り組み」をアピールできる

IT関連の補助金を受けられるようになる

募集概要

申込受付期間

【支援①UTM機器設置コース】

お申し込みは終了しました。

令和6年5月30日(木)から

令和6年11月29日(金)まで

【支援②EDR導入コース】

お申し込みは終了しました。

令和6年5月30日(木)から

令和6年11月29日(金)まで

【支援③セキュリティマネジメント指導コース】

お申し込みは終了しました。

令和6年5月30日(木)から

令和6年11月29日(金)まで

参加対象企業

東京都内に主たる事業所を有し、サイバーセキュリティ対策への意欲を持つ中小企業

受講対象

①UTM機器設置(50社)

お申し込みは終了しました。

②EDR導入(50社)

お申し込みは終了しました。

③情報セキュリティマネジメント指導(100社)

お申し込みは終了しました。

※事業申込企業のセキュリティ状況に応じて支援①または支援②、支援③を実施します。

※定員になり次第、締め切らせていただきます。

※1つの支援でも、①～③全ての支援でも受けることが可能です。

支援期間

3か月

参加費用

無料

募集要項 [PDF0.463MB]



事業説明会について

本事業の特徴や支援内容の概要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 東京都中小企業サイバーセキュリティ基本対策事業について」の内容となります。

中小企業サイバーセキュリティ基本対策事業 事業説明



開催方法 会場とオンライン (Zoom) によるハイブリッド型

定員 各回 会場30名 オンライン100名

参加費 無料

**申し込み
受付期間** お申し込みは終了しました

事業説明会資料 [PDF1.85MB]

第1回

日時

令和6年6月27日(木) 13:30～15:00(90分)

場所

東京都新宿区西新宿1-10-1

ヨドバシ新宿西口駅前ビル TKP新宿西口カンファレンスセンター カンファレンスルーム9階

※オンライン (Zoom) でもご参加いただけます。

プログラム

【第1部】 中小企業のための効果的なセキュリティ対策とリスク管理セミナー

【第2部】 中小企業サイバーセキュリティ基本対策事業説明



講師



株式会社ワールドスカイ

取締役 星野樹昭 氏

中小企業が直面する最新の脅威とセキュリティの重要性についてお話いただきます。効果的なセキュリティ対策とリスク管理を実施するための具体的な手法を解説するとともに、進化する脅威に対応するための情報を提供します。

第一回、第二回目、第三回目の説明会の募集は終了しました。

第2回

日時

令和6年7月10日(水) 13:30～15:00 (90分)

場所

東京都中央区八重洲1-8-16

新槇町ビル TKP東京駅カンファレンスセンター

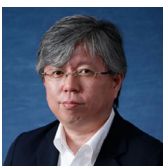
※オンライン(Zoom)でもご参加いただけます。

プログラム

【第1部】 新たな攻撃の予防とセキュリティガバナンス

【第2部】 中小企業サイバーセキュリティ基本対策事業説明

講師



日本マイクロソフト株式会社 パートナー事業本部

AI & Security/BizApps アーキテクト本部

シニア パートナー ソリューション アーキテクト 田住 一茂 氏

サイバーセキュリティ事故を正しく恐れることができるようになるためには、事故が発生する仕組みを正しく理解することが重要です。セキュリティ対策の基本から、これからの攻撃への対策までを解説いたします。

第一回、第二回目、第三回目の説明会の募集は終了しました。

第3回

日時

令和6年7月25日(木) 13:30～15:00 (90分)

場所

東京都立川市曙町2-10-1 ふどうやビル 10階

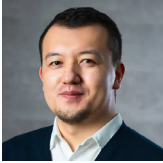
※オンライン(Zoom)でもご参加いただけます。

プログラム

【第1部】 ホワイトハッカーが語る、巧妙化するサイバー攻撃の脅威と企業が行うべきセキュリティ対策セミナー

【第2部】 中小企業サイバーセキュリティ基本対策事業説明

講師



株式会社レオンテクノロジー セキュリティサービス本部

調査・監視部 部長 北川慎人 氏



ホワイトハッカーの視点から、巧妙化するサイバー攻撃の脅威と企業が行うべきセキュリティ対策についてお話しいただきます。最新のサイバー攻撃の動向について、具体的な事例を通じて、その手法や被害の実態を明らかにします。

第一回、第二回目、第三回目の説明会の募集は終了しました。

サイバーセキュリティ対策事業の一覧

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、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

本事業参加企業の事例



事例① UTMでアクセスを「見える化」～気付かなかった脅威を知る～

企業情報

業種: 製造業
従業員数: 6名～20名
支援コース: 支援①UTM機器設置

他企業へ向けたメッセージ

まずは説明会に参加し、自社のセキュリティ対策に必要な支援か判断してみてもいいでしょうか? セキュリティ対策は予防接種のようなものです。“セキュリティワクチン”を打っておきましょう!

事例② コツコツ進めることが、セキュリティ対策の第一歩

企業情報

業種: 製造業
従業員数: 21名～50名
支援コース: 支援②EDR導入、
支援③情報セキュリティマネジメント指導

他企業へ向けたメッセージ

一気にすべて対応することは難しいと思います。自社のレベルにあった内容をコツコツ進めていく必要がある中で、専門家がアドバイスしてくれる今回のような事業を利用することをお勧めします。

事例③ 経営層の意識を変え、攻めのセキュリティ対策で企業価値を高める

企業情報

業種: 出版・マスコミ
従業員数: 101名～300名
支援コース: 支援③情報セキュリティマネジメント指導

他企業へ向けたメッセージ

セキュリティ対策をすることで企業価値が上がっていく時代です。セキュリティ担当者としての成長にもつながったので、経営層も巻き込み、攻めのセキュリティ対策をしていきましょう!

事例④ 専門家との相談で自社に合ったセキュリティ対策を実現

企業情報

業種: サービス業(保険代理店業)
従業員数: 6名～20名
支援コース: 支援③情報セキュリティマネジメント指導

他企業へ向けたメッセージ

自社の情報は自社で守るしかありません。何から始めれば良いかわからない状態から脱却し、自社に合った対策の道標として東京都のサイバーセキュリティ事業を活用してみてもいいでしょうか。

事例⑤ 3つの支援で基本的な対策を整備

企業情報

業種:建設業
従業員数:51名~100名
支援コース:支援①UTM機器設置、支援②EDR導入、
支援③情報セキュリティマネジメント指導

他企業へ向けたメッセージ

わかりにくい「セキュリティ」を専門家が丁寧に
ます。東京都の支援事業を受けることにプラスはあれどマ
イナスは無いと思います。セキュリティ対策を継続してい
きましょう!



Q&A

よくある質問

Q 支援①UTM機器設置コースと支援②EDR導入コース、支援③情報セキュリティマネジメント指導コースの選定基準はありますか？

A UTM機器の設置、EDRの導入状況が選定基準となります。
未設置、未導入の企業様は支援①、もしくは②を、既に設置、導入している企業様は支援③をご案内いたします。
※セキュリティ環境や機器設置箇所の状況により、必ずしも上記のとおりになるとは限りません。
お申し込み後に送付する質問票や、ヒアリングにより最終的には支援コースを決定いたします。

Q 支援① UTM機器設置コースで、UTM機器の設置は工事が必要ですか？

A 大規模な工事は不要ですが、UTM機器はルーター等に設置するため、配線の入れ替えや接続等の簡単な作業を行います。
作業については、専門員が訪問しご説明の上、実施します。

Q SECURITY ACTION二つ星宣言に向けたサポートはありますか？

A 支援③の情報セキュリティマネジメント指導の中でサポートいたします。
SECURITY ACTION二つ星宣言は、自社の情報セキュリティの状況を把握したうえで、情報セキュリティポリシー（基本方針・社内規定）を定め、外部に公開することで、宣言できます。
支援③では情報セキュリティポリシー（基本方針・社内規定）のサンプルの提供や、二つ星宣言に向けた流れをアドバイスするなどSECURITY ACTION二つ星宣言に向けて可能な限りサポートいたします。

Q 情報セキュリティマネジメントコース（支援③）のみでの参加は可能でしょうか？

A はい、支援③のみのご参加も可能でございます。
支援①②③を組み合わせるとのご参加でも、いずれかひとつの支援コースのご参加でもお申込みいただけます。

**Q 小規模（4~5名）ほどで業務を行っています。
業務はサブスクリプションのアプリケーションを使用し、データはMicrosoft365で共有しています。
このような小規模でもUTM機器などの導入を検討した方がいいのでしょうか？**

A 事業規模に関係なく、インターネットをご利用いただいているのであれば、UTMやEDRを入れていただくことでセキュリティのレベルを上げることが可能です。この事業をご利用いただき、ご検討ください。

Q 支援③のみでも参加OKとのことですが、UTM、EDRを導入していなくても問題ないでしょうか？



A UTM、EDR未導入でも支援③は参加可能です。

例えば、セキュリティマネジメント1回目を受けてみたうえで、UTMやEDRを試してみたいとのことであれば、追加でご参加も可能です。

Q 事前相談の上、参加するか決めてもよいのでしょうか？

A 支援①と②につきましては、事前診断がございますので、その際にご相談ください。また、支援③のセキュリティマネジメントにつきましては、事前診断はございません。

東京都「中小企業サイバーセキュリティ基本対策事業」運営事務局

TEL:050-4560-3824 (受付時間 平日 9:00~17:00)

メール: ade.jp.kihontaisaku@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

050-4560-3824

受付時間 9:00~17:00 (平日のみ)



[参加同意書](#)

[サイトポリシー](#)

[プライバシーポリシー](#)

[アクセシビリティ方針](#)