

当事業について



支援内容



参加の流れ



よくある質問



お問い合わせ



サイバー攻撃に備えよう!

## 全6回の専門家派遣で、 セキュリティ事故への対応を強化する

サイト訪問者数 **27,000** 人突破!

集計期間: 令和6年5月23日~現在



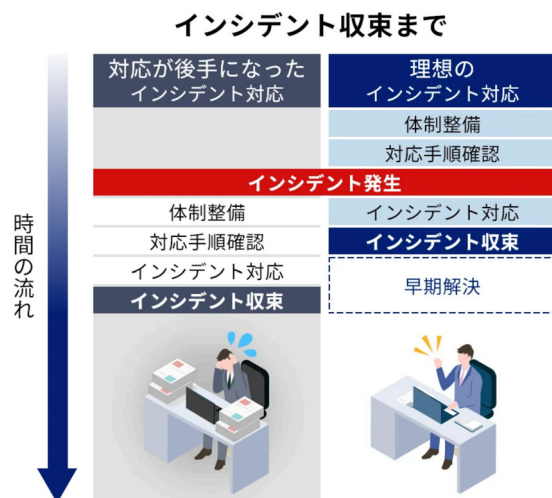
## サイバー攻撃が迫る! 差をつけるのはインシデント対応!

対応が不足していると  
予期せぬコストがかかる!



中小企業においても数千万円単位、  
場合によっては億単位のお金がかかります。

事前のセキュリティ対策が  
インシデント収束までの  
明暗を分ける!



サイバー攻撃の発生をゼロにはできません。  
対策しておくことで早期の収束が可能です。

インシデントとは・・・セキュリティの事故・出来事のこと。たとえば、情報の漏えいや改ざん、破壊・消失、情報システムの機能停止またはこれらにつながる可能性のある事象等がインシデントに該当。



## 中小企業サイバーセキュリティ特別支援事業では 対応から復旧まで考慮したセキュリティ対策をサポートします。

### ABOUT

## 中小企業サイバーセキュリティ特別支援事業について

本事業では、一定のセキュリティ対策を構築し、サイバーセキュリティ対策の継続や自走化に向けた取組を実施している中小企業の皆様へ向けたプラスアルファの支援として、サプライチェーンの安全を確保するための支援を提供します。

現在では、インシデントが起こらないと考えることは現実的ではなく、中小企業が事業を安定的に運営するためには、対応（事故に対する対策を用意する）、復旧（システムを正常な状態に戻すための必要なタスクを明確にする）まで考慮したセキュリティ対策が求められています。そのため、インシデント対応フローを事前に準備しておくことが重要です。

本事業では、攻撃が発生した際に迅速に検知し、的確な対応を行うことで、サプライチェーンの影響を最小限に抑えるためのセキュリティインシデント対応力の強化をサポートします。

## 支援内容

### 選べる2つの支援コース

企業の状況に応じて、CSIRT構築コースとIT-BCP策定コースからお選びいただけます。  
支援コースは、参加企業のご希望と専門家によるヒアリングを踏まえて、適したコースを決定いたします。

#### CSIRT構築コース

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。

こんな企業に・・・

CSIRT（インシデント対応する組織）を持っていない。

インシデント発生時の対応方法が不明。

インシデント対応に関する規程・ルールがない。

インシデント対応に関する規程・ルールはあるが、演習が不十分。

## 支援実施の流れ

### 1回目 ヒアリング



専門家がヒアリングを行い、参加企業のニーズに合ったコースを決定します。組織の置かれている現状や課題を理解し、CSIRT構築に必要な情報を整理します。

### 2回目～4回目 インシデント対応体制整備



CSIRTの方向性を明確にし、達成する目的を定めます。また、CSIRT運用に必要な規程・要領・インシデント対応基本フロー等を整備します。

### 5回目～6回目 インシデント対応机上演習



実際のインシデントに備え、構築した手順の適正を確認し、問題点を洗い出し、改善に向けた具体的なアクションを講じます。



## 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。

こんな企業に・・・

IT-BCP (ITシステムの事業継続計画) を持っていない。

BCP (事業継続計画) に関する規程・ルールはあるが、サイバー攻撃に対する予防策、復旧プランがない。

IT-BCPに関する規程・ルールはあるが、演習が不十分。

## 支援実施の流れ

### 1回目 ヒアリング



専門家がヒアリングを行い、参加企業のニーズに合ったコースを決定します。組織の弱点や課題を理解し、IT-BCP整備計画の方向性を明確にします。

### 2回目～4回目 インシデント対応体制整備



インシデントに備えた対応方針を確立し、迅速かつ効果的な対策を講じる準備を整えます。また、IT-BCP計画を策定し、対象システムの復旧手順を明確にします。

### 5回目～6回目 インシデント対応机上演習



実際のインシデントに備え、構築した手順の適正を確認し、問題点を洗い出し、改善に向けた具体的なアクションを講じます。

## 募集概要

### 申込期間

お申し込みは終了しました。

令和6年5月23日 (木) ～令和6年7月3日 (水)

#### 対象企業

以下の要件をすべて満たす中小企業であること。

- ・東京都内に主たる事業所を有する中小企業
- ・UTMやEDR等の一定程度のセキュリティ対策機器・ソフトウェアを導入し、社内セキュリティポリシー（IPAの「中小企業向けセキュリティ対策の極意」のSECURITY ACTION 二つ星宣言企業レベル）を策定した後、サイバーセキュリティ対策の継続や取組を実施している中小企業



※本事業は、サイバー攻撃を受けて事故が発生した際の事後対応に特化した体制整備支援であるため、一定水準のセキュリティ対策を構築している企業を対象とします。

#### 募集企業

40社（CSIRT構築コース 20社 / IT-BCP策定コース 20社）

※各コースの定員は応募状況により変動します。

※40社を超える申し込みがあった場合は、締切後に抽選を実施して参加企業を決定します。

#### 派遣回数

1社あたり全6回

#### 派遣期間

令和6年7月中旬から令和7年1月下旬の間に、1社あたり3～4か月

[募集要項 \[PDF753KB\]](#)

## 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】 事業説明 中小企業サイバーセキュリティ特別支援事業について」の内容となります。

中小企業サイバーセキュリティ特別支援事業説明会 第2部 事業説明



#### 日程

全日程終了しました。

- ① 令和6年6月11日（火）13:00～14:30（90分）
- ② 令和6年6月19日（水）12:00～13:30（90分）
- ③ 令和6年6月26日（水）10:30～12:00（90分）

開催方式 オンライン開催 (Zoom)

プログラム 【第1部】 セキュリティセミナー『インシデント被害を最小化! 中小企業向けインシデント対応力の  
【第2部】 事業説明 中小企業サイバーセキュリティ特別支援事業について



定員 各回先着100名

申込方法 お申し込みは終了しました。

事業説明会資料 [PDF2.3MB]

## FLOW

# 参加の流れ

令和6年7月3日(水) 応募締切 お申し込みは終了しました。

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ありませんが、事業内容を十分に理解した上でお申し込みいただくことをお勧めします。

### 事業申し込みフォームへの入力と送信

### 受信後、運営事務局よりご連絡

※申し込みフォームで提供いただいた内容の確認と、参加に際しての遵守事項をご案内いたします。その内容についてご了解をいただいた後に、お申し込み完了となります。

※お申し込み内容により、ご希望に添えない場合がございます。予めご了承ください。

### 抽選の実施

※40社を超える申し込みがあった場合は、締切後に抽選を実施して参加企業を決定します。

### 参加同意書の提出

参加確定



## 本事業参加企業の事例

### IT-BCP策定支援事例① 実体験から学ぶインシデント対応、IT-BCP運用の第一歩

#### 企業情報

- ・業種:建設業
- ・従業員数:101~300名

#### 他企業へ向けたメッセージ

サイバーセキュリティ対策は、企業にとって必要不可欠なものです。本事業を活用することで、無料でインシデント対応体制の基盤を構築することが可能です。

### IT-BCP策定支援事例② クラウド環境におけるBCP計画の進展とセキュリティ対策の課題

#### 企業情報

- ・業種:不動産業
- ・従業員数:21~50名

#### 他企業へ向けたメッセージ

サイバー攻撃は、もはや他人事ではありません。特に中小企業の方々にとって、この事業に参加することは、インシデント対応の基盤を構築するための有効な第一歩となります。

### IT-BCP策定支援事例③ 机上演習で実感、課題認識が企業を成長させる

#### 企業情報

- ・業種:運輸業
- ・従業員数:101~300名

#### 他企業へ向けたメッセージ

課題の整理と実践的な机上演習を通じ、初動対応や復旧体制の重要性を学びました。IT-BCP策定は自社対応力の向上に大きく貢献します。

### IT-BCP策定支援事例④ 閉域網と外付けHDD活用で、安価に実現するセキュリティ強化

#### 企業情報

- ・業種:エネルギー供給業
- ・従業員数:6~20名

#### 他企業へ向けたメッセージ

中小企業でも実施可能なバックアップ体制を構築し、具体的な対応策を明確化しました。専門家による丁寧な支援を受けたことで、成果を実感することができました。

## CSIRT構築支援事例① 他部署との連携で挑む、CSIRT体制作りの実践例



### 企業情報

- ・業種:製造業
- ・従業員数:101~300名

### 他企業へ向けたメッセージ

支援中に専門家へネットワーク構成図などの情報を開示する機会がありました。今後も顧客などから情報開示を求められることがあると思いますので、普段から情報を整理しておくの良いと感じました。

## CSIRT構築支援事例② 既存の仕組みを進化させ、現場ですぐに活用できる対応フローを整備したインシデント対策

### 企業情報

- ・業種:農業、農地活用、採用支援
- ・従業員数:101~300名

### 他企業へ向けたメッセージ

机上演習でインシデント対応フローを整備し、初動対応や役割分担を明確化しました。さらに、SaaS障害時の個人情報流出を想定した協議を通じ、コストを抑えた実践的な対応策を具体化しました。

## CSIRT構築支援事例③ 取引先のNIST対応要件を踏まえたインシデント対応力向上への挑戦

### 企業情報

- ・業種:情報通信業
- ・従業員数:51~100名

### 他企業へ向けたメッセージ

NIST対応やインシデント対応力の強化が進みました。役員を巻き込んだ取り組みが成果につながりました。

## Q&A

### よくあるご質問

**Q** 参加費用は無料ですか？

**A** はい、本事業の支援は無料です。ただし、通信費などは参加企業の自己負担となります。

**Q** 全6回の専門家派遣にかかる期間はどのくらいですか？

**A** 専門家派遣の期間は1社につき全6回で、約3~4か月です。

**Q** 専門家派遣は土日祝も対応可能ですか？

A 支援実施は平日のみです。

Q CSIRT構築コースとIT-BCP策定コース、どちらのコースを選べばよいかわかりません。



A 顧客データの漏洩やサーバーへの攻撃など、インシデント対応機能を重視する場合はCSIRT構築コースをお勧めします。一方、事業継続性を重視し、サイバー攻撃に備えて事業を継続する必要がある場合はIT-BCP策定コースをお勧めします。支援コースは第1回支援時に専門家が企業の状況を詳しくヒアリングした上で、最適なコースを提案させていただきます。

Q CSIRT構築コースとIT-BCP策定コースを両方申し込むことは可能ですか？

A 申し込みはどちらか一方のコースのみとなります。

Q 担当する専門家はどのような人ですか？

A 中小企業に対するセキュリティコンサルティングやCSIRT構築支援、およびIT-BCP策定の実務経験があり、情報セキュリティ関連の資格を有する専門家が支援いたします。

## セキュリティ情報

『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

2024.05.23

【IPA】情報セキュリティ10大脅威2024について

2024.06.18

## 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

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

本年度参加企業の事例を公開しました。

2025.02.14

【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



【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特別支援事業」説明会全日程が終了。

第2部動画公開中。

2024.06.26

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

## 東京都「中小企業サイバーセキュリティ特別支援事業」運営事務局

TEL:050-4560-7553(電話受付 平日 9:00～17:00)

メール:ade.jp.tokubetsu@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

**050-4560-7553**

受付時間 9:00～17:00(平日のみ)



[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](#)

