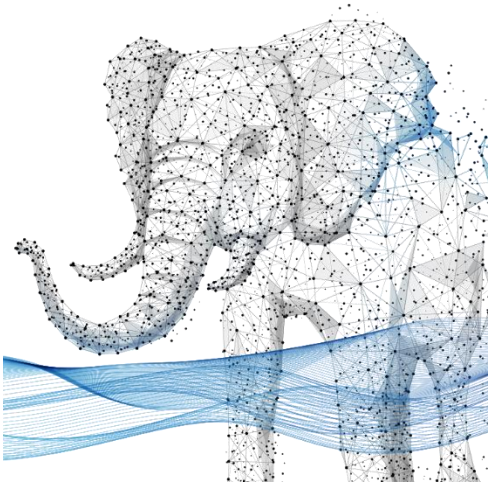
～セキュリティ事故発生に備えた体制整備を支援します～

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
（専門家派遣）

募　集　要　項



東京都 産業労働局 商工部 経営支援課

事務局委託運営：アデコ株式会社

１　事業の概要

【　事業の目的　】

近年、サプライチェーンを狙うサイバー攻撃等が発生しており、脆弱な中小企業が足掛かりとなり、サプライチェーン全体が脅威に晒され、生産活動の一時停止、サービス障害、金銭被害、個人情報・機密情報窃取等、経済社会活動、ひいては国家安全保障に大きな影響が生じ得る状況となっています。こうした状況を踏まえ、東京都では、サイバー攻撃被害（以下、インシデント）が発生した際の「検知」「対応」「復旧」といった事後対応に向けた体制整備を支援することにより、中小企業のインシデント対応力を向上させ、サプライチェーンへの被害拡大の防止を図ります。

【　支援の概要　】

都内に主たる事業所を置く中小企業で、「中小企業サイバーセキュリティ対策継続支援事業」のサイバーセキュリティ人材育成・社内体制整備等の支援後、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企業、または同水準にある企業に対し、プラスアルファの支援として、インシデント発生後に特化した体制整備支援を行っていきます。

本事業では、企業の状況によって、２つのコース（CSIRT 構築コース、IT-BCP 策定コース）を用意しています。令和６年度は CSIRT 構築コースと IT-BCP 策定コース合わせて、計 40 社の募集となります。

支援コース	達成目標	支援内容	
		インシデント対応体制整備	インシデント対応机上演習
CSIRT 構築コース	インシデント発生時に備えて、準備から初動対応までの一連の対応を行う組織（機能）を構築することを目指す	●組織のニーズに沿った CSIRT の役割を定義し、関連部署を含んだ CSIRT 体制の構築を支援	●インシデントシナリオにおける対応手順の確認 ●演習実施、手順・フローのレビュー、問題点の協議、改善に向けた指導・助言
IT-BCP 策定コース	インシデント発生時に、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することを目指す	●関連部署を含んだ IT-BCP 体制を構築し、策定された計画・文書類は緊急時に参照できる等、運用面を踏まえた計画策定を支援	

２　申込の要件

本事業へ参加申込できる事業者は、以下の要件をすべて満たす中小企業※１とします。

(1) 東京都内に主たる事業所を有する中小企業（会社及び個人事業者）。
(2) 次の（ア）または（イ）に該当する社内セキュリティ体制を有していること。
（ア）「中小企業サイバーセキュリティ対策継続支援事業」のサイバーセキュリティ人材育成・社内体制整備等の支援を受けた後、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
（イ）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 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自走化に向けた取組を実施している中小企業

(3) 支援期間中［令和６年７月中旬～令和７年１月下旬（予定）］、１社につき全６回の専門家派遣（３～４か月で実施）を受け入れ可能であること。
(4) インシデント対応体制整備及びインシデント対応力向上に強い意欲を有していること。
(5) 支援期間中は、運営事務局からの電話連絡やメールに迅速かつ適切に対応し、専門家（支援者）からの支援や助言を積極的に活用すること。また、本事業で実施するコミュニティイベントに原則参加すること。
(6) 支援期間中及び支援期間終了後に運営事務局が実施するアンケートやヒアリング調査に協力すること。
(7) 次のア～キの全てに該当すること
（ア）都税、消費税及び地方消費税の額に滞納がないこと
（イ）法令等もしくは公序良俗に反し、またはその恐れがないこと
（ウ）東京都に対する賃料・使用料等の債務が存する場合、その支払いが滞っていないこと
（エ）民事再生法、会社更生法、破産法に基づく申立手続中（再生計画等認可後は除く）、又は私的整理手続中など 、事業の継続性について不確実な状況が存在していないこと
（オ）「東京都暴力団排除条例」に規定する暴力団関係者又は「風俗営業等の規制及び業務の適正化等に関する法律」第２条に規定する風俗関連業、ギャンブル業、賭博等、支援の対象として社会通念上適切でないと判断される業態を営むものではないこと
（カ）その他、連鎖販売取引、ネガティブ・オプション（送り付け商法）、催眠商法、霊感商法など公的資金の助成先として適切でないと判断する業態を営むものではないこと
（キ）宗教活動や政治活動を主たる目的とする団体等でないこと

(8) 本事業への参加にあたっては、本項に記載された申込要件を全て満たし、かつ、本事業への申込を行う個人および所属企業が募集要項の記載内容を理解し、了承すること。

※１　本事業における中小企業とは、中小企業基本法第２条第１項に規定に基づく下表に該当するものをいう。

業種	下記のいずれかを満たす	
	資本金の額又は出資の総額	従業員数（常勤）
製造業、建設業、運輸業	3 億円以下	300 人以下
卸売業	1 億円以下	100 人以下
サービス業	5,000 万円以下	100 人以下
小売業	5,000 万円以下	50 人以下
ゴム製品製造業（自動車又は航空機用タイヤ及びチューブ製造業並びに工業用ベルト製造業を除く）	3 億円以下	900 人以下
ソフトウェア業・情報処理サービス業	3 億円以下	300 人以下
旅館業	5,000 万円以下	200 人以下
その他の業種（上記以外）	3 億円以下	300 人以下

３　支援内容（詳細）

参加企業は、企業の状況に応じて、「CSIRT 構築コース」と、「IT-BCP 策定コース」から支援コースを選択していただきます。支援コースは、第１回派遣時に専門家がヒアリングを行い、参加企業と相談したうえで、確定されます。また、「共通支援」として、参加企業向けの相談窓口やコミュニティ形成支援を提供します。

【　専門家派遣実施期間　】

令和６年７月中旬　～　令和７年１月下旬（予定）

※上記期間内に、１社あたり全６回を３～４か月間で実施予定です。

（１）CSIRT 構築コース：事故発生時の対応手順の整備支援

支援概要	インシデントが発生した際に備えて、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。日本シーサート協議会が提示する基本的なステップと汎用的な構築項目をベースに、各企業の状況やニーズに合わせた CSIRT を構築します。参加企業の独自の課題や要件を反映し、個社の状況に合わせてドキュメントを作成することで、インシデントが発生した際の迅速な対応を可能にし、被害を最小限に抑えます。机上演習では、作成した対応フローをウォークスルー形式で実施し、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。これにより、参加企業が継続的に取り組むことができる環境を整えます。

CSIRT 構築コース全６回の支援の流れは以下の通り。

派遣回	実施項目	実施内容
第１回	ヒアリング	支援内容の説明とコースの確認を行います。ヒアリングシートをもとに、次の内容についてヒアリングいたします。 ➢ セキュリティ体制 ➢ 既存のインシデント対応状況 ➢ 組織内の関係者と利害関係者 ➢ 既存のセキュリティポリシーと関連文書 ➢ 守るべき情報資産と脅威 ➢ その他課題

		<u>使用するドキュメント</u> ● ヒアリングシート
第２回	インシデント対応体制整備①	CSIRT 構築に必要な事項を説明します。また、第１回のヒアリング結果を踏まえ、次の内容について方向性を決定いたします。 ➢ CSIRT 基本構想（サービス対象、ミッション、取り扱うインシデント）の検討 ➢ サービスの検討 ➢ 社内体制の検討 ➢ 社外連携の検討 ➢ リソース、予算の検討 ➢ CSIRT 構築後の期待される成果や効果 <u>使用するドキュメント</u> ● ヒアリング結果報告書 ● CSIRT 構築チェックリスト
第３回	インシデント対応体制整備②	専門家が準備した CSIRT 枠組み文書をもとに、次の内容を定めます。また、CSIRT 基本文書とインシデント対応基本フローについて説明いたします。 ➢ CSIRT 基本構想（サービス対象、ミッション、取り扱うインシデント）の検討 ➢ サービスの定義 ➢ 社内体制の定義 ➢ 社外連携の定義 ➢ リソース、予算の定義 ➢ CSIRT 基本文書（案）の検討 ➢ インシデント対応基本フロー（案）の説明 <u>使用するドキュメント</u> ● CSIRT 枠組み文書 ● CSIRT 基本文書（案） ● インシデント対応基本フロー（案）
第４回	インシデント対応体制整備③	専門家が準備した CSIRT 基本文書（修正版）とインシデント対応基本フロー（修正版）を基に、次の内容を実施します。 ➢ CSIRT 基本文書（修正版）の説明 ➢ CSIRT 基本文書（修正版）の確認 ➢ インシデント対応基本フロー（修正版）の説明

		➢ インシデント対応基本フロー（修正版）の確認 使用するドキュメント ● CSIRT 基本文書（修正版） ● インシデント対応基本フロー（修正版）
第５回	インシデント対応机上演習①	専門家が準備した机上訓練説明資料をもとに、次の内容を実施します。 ➢ インシデント対応シナリオの確認 ➢ 対応手順の確認 ➢ 訓練時準備資料の確認（インシデント対応マニュアル、インシデント対応フロー、インシデントトリアージ基準表、CSIRT 取扱いインシデントリスト、連絡先一覧表、体制図） 使用するドキュメント ● 机上訓練説明資料
第６回	インシデント対応机上演習②	インシデント対応シナリオと、対応手順をもとに、次の内容を実施します。 ➢ インシデント発生シナリオをもとに、机上演習（全体レビュー） ➢ 問題点の協議 ➢ 改善に向けた指導・助言 ➢ 今後の定期的見直し方法について指導・助言 使用するドキュメント ● 机上演習計画 ● 定期見直しチェックシート

（２）IT-BCP 策定コース：IT システムに対する組織ルールの整備支援

支援概要	インシデントが発生した際に、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。 NISC（内閣サイバーセキュリティセンター）「政府機関等における情報システム運用継続計画ガイドライン」の実施プロセスと具体的な検討事項をもとに、各企業の状況やニーズに合わせた IT-BCP を策定します。参加企業の独自の課題や要件を反映し、個社の状況に合わせてドキュメントを作成することで、インシデントが発生した際の迅速な対応を可能にし、被害を最小限に抑えます。机上演習では、作成した対応フローをウォーク

	スルー形式で実施し、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。これにより、参加企業が継続的に取り組むことができる環境を整えます。

IT-BCP 策定コース全６回の支援の流れは以下の通り。

派遣回	実施項目	実施内容
第１回	ヒアリング	支援内容の説明とコースの確認を行います。ヒアリングシートをもとに、次の内容についてヒアリングいたします。 ➢ 利用している IT インフラの整備状況 ➢ 重要データのバックアップ状況 ➢ セキュリティ体制、対応状況 ➢ 重要な業務のビジネスプロセス ➢ リスク管理の手法と評価 ➢ その他課題 <u>使用するドキュメント</u> ● ヒアリングシート
第２回	インシデント対応体制整備①	第１回のヒアリング結果をもとに、事業影響度を分析し、次の内容について方向性を決定いたします。 ➢ システム停止系（ランサムウェア）対策か、情報漏えい系（マルウェア、フィッシング等）対策か ➢ 復旧時間目標（RTO）と復旧ポイント目標（RPO） ➢ 復旧の優先順位 <u>使用するドキュメント</u> ● ヒアリング結果報告書 ● 簡易版事業影響分析
第３回	インシデント対応体制整備②	専門家が準備した IT-BCP 計画案を基に、次の内容を実施します。 ➢ IT-BCP 計画案についての説明 ➢ 実施体制の策定 ➢ 連絡フローの策定 ➢ 復旧フローの策定 ➢ システム復旧プランの策定 ➢ データ復旧プランの策定 ➢ 予防策の策定

		➢ 対象システム復旧手順など、既存の手順について具体的な内容確認 <u>使用するドキュメント</u> ● IT-BCP 計画案
第４回	インシデント対応体制整備③	専門家が準備した IT-BCP 計画案（修正版）をもとに、次の内容を実施します。 ➢ IT-BCP 計画案（修正版）の説明 ➢ IT-BCP 計画案（修正版）の確認 ➢ 実施体制の策定 ➢ 連絡フローの策定 ➢ 復旧フローの策定 ➢ システム復旧プランの策定 ➢ データ復旧プランの策定 ➢ 予防策の策定 ➢ 対象システム復旧手順など、既存の手順について具体的な内容確認 <u>使用するドキュメント</u> ● IT-BCP 計画案（修正版）
第５回	インシデント対応机上演習①	専門家が準備した IT-BCP 対応手順概要をもとに、次の内容を実施します。 ➢ IT-BCP 手順概要の確認 ➢ 既存手順との紐づけ確認 <u>使用するドキュメント</u> ● IT-BCP 対応手順概要
第６回	インシデント対応机上演習②	IT-BCP 対応手順概要と、自社既存手順をもとに、次の内容を実施します。 ➢ インシデント発生シナリオをもとに、机上演習（全体レビュー） ➢ 問題点の協議 ➢ 改善に向けた指導・助言 ➢ 今後の定期的見直し方法について指導・助言 <u>使用するドキュメント</u>

		● 机上演習計画 ● 定期見直しチェックシート

（３）共通支援（相談窓口、コミュニティ形成支援）

支援概要	参加企業向けに、本事業に関する相談や日常的なセキュリティ課題に対応する窓口を開設します。また、コミュニティ形成を通じて、参加企業同士の連携や課題解決を支援いたします。
具体的支援	●相談窓口 専門的な相談に対しては、専門家と連携し、回答いたします。 電話　050-4560-7553（土日祝日を除く　9:00～17:00） メール：ade.jp.tokubetsu@jp.adecco.com ●コミュニティ形成に向けた支援 参加企業 40 社を対象としたセキュリティセミナー・懇親会の開催 予定開催時期：令和 6 年 11 月～令和 7 年 1 月、1 回程度

４　申込方法

申込受付期間に申し込みがあった企業の中から、2 ページに記載している要件を満たす企業を抽選により決定いたします。参加を希望する企業は、以下の手順に従ってお申し込みください。

【　申込受付期間　】

令和６年５月２３日（木）　～　令和６年７月３日（水）

※7 月 3 日（水）23 時 59 分に申し込みを締め切ります。

【　参加企業数　】

40 社（CSIRT 構築コース　20 社　/　IT-BCP 策定コース　20 社）

※各コースの参加企業数は申込状況により変動します。
※40 社を超える申込があった場合は、締切後に抽選を実施して参加企業を決定します。

【　参加費用　】

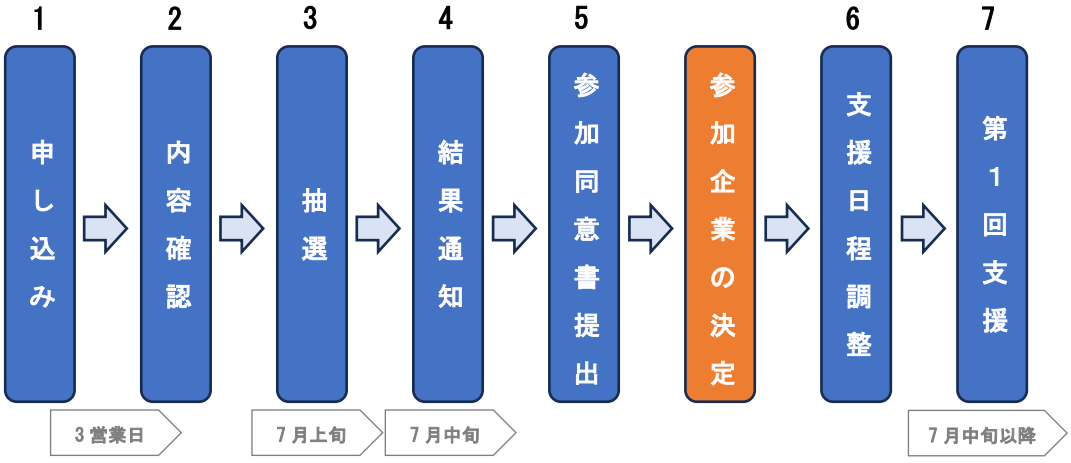
無料　※ただし、参加にかかる実費（通信費、交通費等）は自己負担です。

【　申込方法　】

申込受付期間内に、事業 WEB サイト上の申込フォーム（以下 URL または QR コード）より、必要事項を入力のうえ、お申し込みください。

＜事業申し込み用 URL＞
https://forms.office.com/e/Y6ngAKf9rD

【　申込から支援開始までのフロー　】



1. 申込フォームから、ご希望のコース（「CSIRT 構築コース」または「IT-BCP 策定コース」）を選択のうえ、お申し込みください。
   ※支援コースは、参加企業のご希望と、第１回支援の中での専門家によるヒアリングを基に、最適なコースを確定いたします。そのため、ご希望いただいたコースが必ずしも支援コースとは限らないことをご了承ください。
   ※申込時からコースが変更される場合は、必ず参加企業の了承を得たうえで決定されます。
2. 申込受付順に、申込フォームの記載内容の確認のため、3 営業日以内に電話によるヒアリングを行います。
   ※ヒアリングの際、参加にあたっての規定や遵守事項をご説明差し上げます。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。申込フォームの送信だけでは、申し込みは完了しておりませんのでご注意ください。
   ※また、確認の結果、本事業で必要なセキュリティ体制を有していない企業には、やむを得ず参加をお断りすることがございます。その場合には、運営事務局から本事業で必要なセキュリティ体制を整備するために有用な関連事業を別途ご案内いたします。
3. 40 社を超える申込のあった場合は、締切後に申込時に受け付けたコース（CSIRT 構築コース、IT-BCP 策定コース）ごとに抽選を実施して参加企業を決定します。
   ※抽選の実施は、7 月上旬を予定しております。
4. 結果通知のご連絡は、7 月中旬を予定しております。
   ※結果通知後、本事業への参加を辞退される場合には、通知から 2 日以内に運営事務局へご連絡ください。辞退される企業が発生した場合、再抽選を実施し、繰り上げ当選された企業にご連絡いたします。
5. 参加対象企業について、運営事務局への参加同意書の提出をもって、参加確定とさせていただきます。
6. 参加が確定した企業について、運営事務局から具体的な支援日時の相談をさせていただきます。
7. 第１回支援の中で専門家がヒアリングを行い、参加企業と相談したうえで、支援コースを確定します。
   ※第１回支援時の専門家によるヒアリングの結果、支援コースが当選コースから変更となる場合がありますが、その際は、参加企業の了承を得たうえで決定されます。
   ※専門家支援は原則として対面で行いますが、状況によってはオンライン形式でも対応可能です。詳細につきましては、支援日程の調整の際にご相談ください。

５　事業説明会

本事業の特徴や支援内容の概要、参加することのメリットなどを詳しくご案内いたします。当日は、セキュリティの専門家による中小企業のインシデント対応力強化に必要な対策と知識を解説するセミナーも予定しております。お申し込みをご検討中の方は、まずは説明会にご参加ください。

日程	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強化』 【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	以下の事業説明会申し込み URL、または QR コードよりお申し込みください。 受付後に参加用 URL をお送りいたします。 ＜事業説明会申し込み URL＞ https://forms.office.com/e/YXU4wLefV3

６　留意事項

(1) 申込にあたってご提供いただく個人情報を含む情報は、東京都及び運営事務局にて、必要な範囲にて利用、共有いたします。なお、個人情報を事前の承認なく、都及び運営事務局以外の第三者に提供することはありません。

(2) 中小企業サイバーセキュリティ特別支援事業の参加企業の受付、申込内容の確認は、運営事務局が行い、東京都が承認するものとします。

(3) 申込者が、申込に際し虚偽の情報を記載し、その他東京都及び運営事務局に対して虚偽の申告を行った場合は参加対象外といたしますので予めご了承ください。

(4) 参加企業は、参加同意書（別添１）に記載の内容に全て同意いただき、記入・署名のうえ、提出いただいた場合にのみ参加が確定します。

(5) 参加企業について、事業参加に不適切であると東京都及び運営事務局が判断した場合には、参加を辞退していただく場合がございますのでご留意ください。

(6) 東京都、運営事務局及び専門家（支援者）は、参加企業の目標達成を保証するものではなく、本事業における結果については一切の責任を負わないものとします。また、本事業において、参加企業に如何なる損害が発生したとしても、東京都、運営事務局及び専門家（支援者）は参加企業に一切の責任を負わないものとします。

(7) 参加企業は、東京都及び運営事務局から提供された情報を機密扱いし、第三者に漏洩せず、個人的な利益や目的に使用しないことにご同意ください。情報の使用や公開に関しては、東京都または運営事務局からの指示に従ってください。

(8) この要項に定めのない事項は、別途東京都が定めます。

本事業に関するお問い合わせは、以下運営事務局までお願いいたします。

中小企業サイバーセキュリティ特別支援事業

〒160-0023　東京都新宿区西新宿 1-22-2

電話 050-4560-7553（土日祝日を除く 9:00～17:00）

メール ade.jp.tokubetsu@jp.adecco.com

事業 WEB サイト：

https://tokubetsushien.metro.tokyo.lg.jp/

別添１

参加同意書

記載事項をすべてお読みいただき、枠内のすべての事項にチェックと記入・署名が確認できた場合のみ、参加可能となります。本同意書提出の依頼のあった際は、ご記入後に速やかにご提出ください。

同意できる事項にチェックを付けてください（６か所）

- □ 支援期間中［令和６年７月中旬～令和７年１月下旬（予定)］に、全６回の専門家派遣（３～４か月で実施）を受け入れ可能です。
- □ インシデント対応体制整備及びインシデント対応力向上に強い意欲があります。
- □ 支援期間中は、運営事務局からの電話連絡やメールに迅速かつ適切に対応し、専門家（支援者）からの支援や助言を積極的に活用します。また、本事業で実施するコミュニティイベントに原則参加します。
- □ 支援期間中及び支援期間終了後に運営事務局が実施するアンケートやヒアリング調査に協力します。
- □ 東京都、運営事務局または専門家（支援者）から提供された情報を機密扱いし、第三者に漏洩せず、個人的な利益や目的に使用しないことに同意します。情報の使用や公開に関しては、東京都または運営事務局からの指示に従います。
- □ その他、募集要項記載事項について、全て内容を理解し了承します。

私／当社は、上記記載のチェックリストを確認し、項目について順守いたします。

参加者氏名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

所属企業名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

連絡先電話番号（携帯電話）：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

本参加同意書は、運営受託者であるアデコ株式会社が保管し、本年度事業終了時に破棄いたします。法令等に基づく開示請求を受けた場合を除き、第三者への開示提供や他の目的での利用は行いません。