令和７年度版
運営事務局

令和７年度中小企業サイバーセキュリティ啓発事業　募集要項

1．事業の目的

テレワークの普及、デジタル化の進展、そしてサイバー攻撃の激化により、中小企業におけるセキュリティ対策は急務となっています。しかし、依然としてセキュリティ対策の必要性を認識していない企業や、対策を継続的に実施することが困難な企業も多く存在しています。

このような状況を踏まえ、本事業では、東京都のサイバーセキュリティ対策関連事業に未参加の企業の経営層、従業員、セキュリティ担当者を対象に、サイバー攻撃による被害を学ぶ体験型演習や、標的型攻撃メール訓練を通じた実践的な疑似体験、さらに専門家によるネットワーク調査とリスク分析を実施します。これらの活動を通じて、企業全体のセキュリティ意識を高め、実際のセキュリティ対策の導入・実践を後押しします。

また、支援終了後には、参加企業の効果的な施策と取組事例の発信を行い、都内中小企業全体のサイバーセキュリティ意識と対策の向上を目指します。

2．当事業の募集対象

参加申込にあたっては、以下の全ての要件を満たす必要があります。

（１）東京都内に主たる事業所を有する中小企業者（会社及び個人事業主）

次の表のいずれかに該当する中小企業基本法第２条第１項に規定する中小企業者

業種	資本金及び従業員
①　製造業、建設業、運輸業、その他の業種（②～④を除く）	３億円以下又は 300 人以下
②　卸売業	１億円以下又は 100 人以下
③　サービス業	5,000 万円以下又は 100 人以下
④　小売業	5,000 万円以下又は 50 人以下

（２）原則は、過去に東京都サイバーセキュリティ対策関連事業の支援を受けていない中小企業および個人事業主。ただし、令和６年度までに東京都サイバーセキュリティ対策関連事業に参加された中小企業者でも、同一内容の支援でなければ、ご参加いただけます。

（３）本事業と同等のサイバーセキュリティ対策の内容を支援する東京都・東京都中小企業振興公社の補助事業を同時に活用していない中小企業者。

（４）セキュリティに関する意識調査（アンケート）、ヒアリングを支援後にご協力いただける企業。

（５）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。

3．申込受付期間

令和７年５月 23 日（金）　から受付開始

※各支援定員に達し次第、募集を締め切らせていただきます。

4．募集企業（定員数）

本事業では、下記３つの支援を募集いたします。

支援内容	定員
（１）サイバー攻撃対応演習セミナー	100 社
（２）標的型攻撃メール訓練	50 社
（３）ネットワーク調査・構成図作成	50 社

※１社で複数の支援へお申し込みが可能です。詳しくは７.支援内容の詳細をご覧ください。

※平日（土日祝並びに年末年始の事務局閉局日を除く）に支援時間を確保していただける方。

※(2)(3)の支援は企業様の現状把握と支援実施のため、専門家が企業の事業所に訪問いたします。
専門家の訪問時間は原則 9:00～17:00、訪問先は都内のみとなります。

5．参加費用

無料

※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。

6．申込方法

募集要項及び参加規約をご確認の上、本事業ウェブサイトの各申込フォームから必要事項を入力してお申し込みください。

＜事業詳細 URL＞ https://keihatsu.metro.tokyo.lg.jp/#support

7．支援内容の詳細

（１）サイバー攻撃対応演習セミナー

項目	内容
定員数	100 社（先着順）　　１回あたり 10 社程度 ※原則、１社につき１名。複数名でのご参加を希望される場合は、事務局までご相談ください。

<table>
<tr><td>開催目的</td><td>経営層を対象に、サイバー攻撃発生時の対応や攻撃による企業損失リスクを体感できる体験型プログラムを通じて、セキュリティ対策を経営課題として捉える重要性に気付いていただくことを目的としています。</td></tr>
<tr><td>実施方法</td><td>会場対面参加
※臨場感のある意思決定体験と講師陣や参加企業間での双方向の深い議論を実現するため、原則会場参加とさせていただきます。</td></tr>
<tr><td>支援期間</td><td>７月上旬から 10 回程度開催　（同一内容・1 回あたり 3 時間程度）
下記日程のうち、ご都合の良いいずれかの 1 回にご参加ください。

<table>
<tr><th></th><th>開催日</th><th>時間</th><th>開催場所</th></tr>
<tr><td>第 1 回</td><td>７月 3 日(木)</td><td>13:30～16:30</td><td rowspan="4">新宿センタービル 34 階
（アデコ株式会社　会議室）</td></tr>
<tr><td>第 2 回</td><td>７月 8 日(火)</td><td>13:30～16:30</td></tr>
<tr><td>第 3 回</td><td>７月 10 日(木)</td><td>13:30～16:30</td></tr>
<tr><td>第 4 回</td><td>７月 29 日(火)</td><td>13:30～16:30</td></tr>
<tr><td>第 5 回</td><td>８月 6 日 (水)</td><td>13:30～16:30</td><td>霞が関東急ビル 9 階
（アデコ株式会社　会議室）</td></tr>
<tr><td>第 6 回</td><td>８月 26 日(火)</td><td>13:30～16:30</td><td>新宿センタービル 34 階
（アデコ株式会社　会議室）</td></tr>
<tr><td>7 回目以降</td><td colspan="3">詳細が決定次第、順次募集を開始いたします。</td></tr>
</table>

※7 回目以降は順次、情報公開いたします。
※演習では少人数のグループに分かれてグループワークを実施しますので、原則お申し込み後のキャンセルはご遠慮ください。
参加日確定後、欠席せざるを得なくなった場合は、必ず事前に事務局までご連絡ください。</td></tr>
<tr><td>支援対象者</td><td>経営層
※経営課題としてサイバーセキュリティ対策を捉えていただく内容となっているため、経営判断を行う立場の方を対象とさせていただきます。
（例）・会社全体の方向性を決定し、最終的な責任を負う立場の方
・会社の経営に関する重要な役割を担う方
・会社の運営や戦略に関する重要な決定を行う方・関与する方
・部門や部署の責任者で、部門運営や戦略を担当する方
※上記に該当するほか、経営層から参加の承認を得た方も対象となります。</td></tr>
<tr><td>支援内容</td><td>①講義：一般的なセキュリティ知識と対策方法を解説
└最新のサイバー攻撃の手法や被害実態、対処方法などをご紹介します。
②演習：ウイルス感染などのサイバー攻撃に対して適切に判断をするための体験型ワーク
└複数のシナリオをもとに、ご自身の選択がもたらす損害や被害額を可視化します。
シナリオごとに演習結果を持ち寄り、各グループ内で意見交換・対策を検討します。
③座談会：小グループにて、今後経営者として取り組むべき事項を議論
└演習の振り返りを通じ、各自で今後のアクションプランを検討します。
少人数での開催のため、専門家に直接相談することも可能です。</td></tr>
<tr><td>期待できる効果</td><td>・日常のセキュリティリスクの認知や対策方法の理解</td></tr>
</table>

	・現時点の対策知識レベルの認知とインシデント発生時の適切な対処方法の理解 ・他社の状況把握と自社理解
注意事項	・本支援申込企業に対し、申込後３営業日以内に事務局より電話連絡させていただきます。 ▶申込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します。 ▶セキュリティ対策状況などの簡易ヒアリングも同時に行い、個社に適した支援もご提案します。 ・座談会で知りえた他の参加企業の情報は秘密を保持し、いかなる場合においても第三者に対し利用・開示・漏洩する事がないよう厳重に管理をお願いします。

（２）標的型攻撃メール訓練

項目	内容
定員数	50 社（先着順）
開催目的	従業員を対象に、社員教育の一環として標的型攻撃メールを疑似体験する訓練を実施します。更に、標的型攻撃メールに関する従業員としての対策方法を指導することで、従業員全体のセキュリティ意識向上を図ります。
実施方法	企業訪問 ※調査等にあたり、企業様を訪問させていただく必要があるため、原則は事業所への訪問が可能であることを条件といたします。
支援期間	約３か月　・1 社あたり、2 回の専門家訪問と 2 回のメール訓練
支援対象者	従業員等
支援内容	①訓練前コンサルティング 【専門家訪問 1 回目／所要時間:2 時間程度】 －訓練全体の流れの説明 －メール環境の確認 －訓練メールの送付日や内容などの調整 ②訓練メール（1 回目） ③訓練メール（2 回目） ④訓練後コンサルティング 【専門家訪問 2 回目／所要時間:2 時間程度】 －メール開封結果の共有（組織別・部署別・役職別） －セキュリティ機器設置等の事前策などのアドバイス －社内対応（エスカレーション）ルールの策定支援
期待できる効果	・不審なメールを見極める力の醸成 ・セキュリティにおける人的対策 ・社内対応（エスカレーション）ルールの構築
注意事項	・本支援申込企業に対し、申込後３営業日以内に事務局より電話連絡させていただきます。 ▶申込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します。 ▶セキュリティ対策状況などの簡易ヒアリングも同時に行い、個社に適した支援もご提案します。 ・参加が確定した企業様には、改めて、担当専門家より訪問に際してのご連絡をいたします。 ・訓練前コンサルティング後（1 回目の訪問後）にテストメールを送付します。 テストメールが何らかの理由（メールフィルタリングやセキュリティ装置機能等）により受信できない

	場合、本支援はご参加いただけません。 ・テストメールの添付ファイルが何らかの理由（サンドボックス機能や Outlook 設定等）により強制的に開封扱いとなる場合、訓練メールの開封確認方式は URL 方式のみ対応可能となります。

（３）ネットワーク調査・構成図作成

項目	内容
定員数	50 社（先着順）
開催目的	セキュリティ担当者等を対象として、ネットワーク調査や構成図を作成し、必要な対策を指導・助言することで、自社のセキュリティ実態を可視化するとともに、技術的対策の意識向上を図ります。
実施方法	企業訪問　※調査等にあたり、企業様を訪問させていただく必要があるため、原則は事業所への訪問が可能であることを条件といたします。
支援期間	約 2 か月　・1 社あたり、2 回の専門家訪問
支援対象者	セキュリティ担当者・情報システム部門担当者　※管理部門（総務等）の方も可
支援内容	事前に確認させていただくこと ※ご担当者様が把握している項目のみで結構です。 例）PC 端末台数 / サーバ台数（オンプレミスの物理サーバ、仮想サーバの有無） ネットワーク機器（ルータ、スイッチ、無線 AP 等）の台数 セグメントの数（社内 LAN が 1 つだけなのか、複数 VLAN があるのか） 調査希望場所（本社１フロアの調査を希望 など） ①ネットワーク調査・物理環境調査　【専門家訪問 1 回目／所要時間:2 時間程度】 －平日 9:00～17:00 の間で専門家が現地にて調査 －回線/ONU/ルーター/スイッチ/PC 端末等の品番・品名確認を実施 （電話機・複合機は調査対象外） －調査は最大 100 台まで・フロア跨ぎや拠点跨ぎの調査については不可 ②フィードバックコンサルティング　【専門家訪問 2 回目／所要時間:2 時間程度】 －提供資料：ネットワーク構成図、平面図、機器一覧表、物理環境調査レポート －現状のセキュリティ実態と今後必要な対策についてレポートを基にアドバイス －希望の方に、ログ監視・インシデント対応ミニ研修、運用マニュアル・チェックリストの作成演習
期待できる効果	・現状のネットワーク構成とセキュリティリスクの可視化 ・予期せず発生した故障や通信障害にもスムーズに対応可能 ・通信トラブルの原因となる機器の配線・接続・設置状況や LAN ケーブルの保護状況など通信機器の周辺環境の現状把握が可能
注意事項	・本支援申込企業に対し、申込後 3 営業日以内に事務局より電話連絡させていただきます。 ▶申込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します。 ▶セキュリティ対策状況などの簡易ヒアリングも同時に行い、個社に適した支援もご提案します。 ・参加が確定した企業様には、改めて、担当専門家より訪問に際してのご連絡をいたします。

	・ネットワーク調査時はご担当者様の立ち合いをお願いします。 ・本事業では ONU（※１）が複数のフロアにあった場合、１フロアのみ調査します。 ・ネットワーク調査は、専門家が指定した調査対象物に対して実施します。 ・専門家が入室できないエリアや高所（高さ 2 メートルまでの脚立を活用して届く、またはそこから目視できる範囲）に設置されている機器、または棚等に保管されている予備機等は可能な範囲で調査を実施します。 ・調査方法、調査内容については、専門家にて判断します。 ・状況によりネットワーク機器及び機器周辺を撮影させていただく場合があります。 ※１光回線終端装置（Optical Network Unit）のことで、光信号をデジタル信号に変換する機器

８．事業説明会のご案内

本事業の特徴や支援内容の概要について詳しくご案内するほか、セキュリティ専門家による最新のサイバー脅威情報などのセミナーを併せた説明会を開催します。本事業へのお申し込みをご検討中の方は、ぜひ説明会にご参加ください。

※開催日が近くなりましたら、メールにて詳細（開催日時や会場・参加 URL）をご案内します。
Zoom の URL は使い回しができませんので、おひとり 1 フォームでお申し込みください。

第１回		
開催日時	６月 18 日（水）　14:00～15:30　（90 分）	
プログラム	第１部	ミニセミナー：『経営者がおさえておきたい生成 AI の実践法』 講師: 飯田 剛弘 氏（中小企業 AI 活用協会 代表理事）
	第２部	事業説明
開催方法	オンライン開催（Zoom ウェビナー）	
申込方法	以下の事業説明会申込 URL、または、QR コードからお申込みください。 URL：第１回 事業説明会申込フォーム	
申込締切	開催日前日まで	

第２回		
開催日時	６月 19 日（木）　14:00～15:30　（90 分）	
プログラム	第１部	ミニセミナー：『社内データが漏洩したらどうしますか？』 講師: 中大路 智崇 氏（株式会社ワールドスカイ 執行役員）
	第２部	事業説明
開催方法	オンライン開催（Zoom ウェビナー）	

申込方法	以下の事業説明会申込 URL、または、QR コードからお申し込みください。 URL：第２回 事業説明会申込フォーム
申込締切	開催日前日まで

第３回	（サイバーセキュリティ基本対策事業との合同開催）	
開催日時	６月 26 日（木） 13:30～15:30 （120 分）	
プログラム	第１部	警視庁から「サイバー犯罪の情勢について」
	第２部	ミニセミナー：『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』 講師：北川 慎人 氏（株式会社レオンテクノロジー）
	第３部	事業説明
開催方法	①オンライン開催（Zoom ウェビナー） ②会場参加 がお選びいただけます。 ▶会場：TKP 新宿西口カンファレンスセンター （新宿区西新宿１丁目 10−1） https://www.kashikaigishitsu.net/facilitys/cc-shinjuku-nishiguchi/access/	
定員	会場参加の場合は、先着 50 名様	
申込方法	以下の事業説明会申込 URL、または、QR コードから参加方法を選択の上、お申し込みください。 URL：第３回 事業説明会申込フォーム ※お申込フォームは合同開催用のフォームとなります。	
申込締切	開催日前日まで	

経営層が関心を持つテーマとセキュリティを掛け合わせたウェビナーも開催します。セキュリティ対策の重要性をご確認いただきながら、本事業の特徴や支援内容の概要についても詳しくご案内します。サイバー攻撃対応演習セミナー支援にもつながる内容となります。

経営層向けセミナー		
開催日時	７月 14 日（月） 16:30～18:00 （90 分）	
プログラム	第１部	セミナーテーマ：『投資と会社の成長を考えよう』 講師：安達 裕哉 氏（ティネクト株式会社 代表取締役）
	第２部	事業説明
開催方法	オンライン開催（Zoom ウェビナー）	
申込方法	以下のセミナー申込 URL、または、QR コードからお申し込みください。 URL：経営者向け特別セミナー兼事業説明会申込フォーム	

申込締切	開催日前日まで

9．問い合わせ先

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。

東京都「令和 7 年度中小企業サイバーセキュリティ啓発事業」運営事務局

TEL：050-4560-7553

受付時間：平日 9:00～17:00（土日祝並びに年末年始の事務局閉局日を除く）

メール： ade.jp.keihatsu@cybersecurity-tokyo.com

URL： https://keihatsu.metro.tokyo.lg.jp/

※本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。

参加規約

この度は「令和 7 年度中小企業サイバーセキュリティ啓発事業」（以下、本事業）の参加申し込みをいただき誠にありがとうございます。注意事項をご確認の上、お申し込みをお願いいたします。

1．本事業への参加資格

(1) 東京都内に主たる事業所を有し、中小企業基本法 第 2 条 1 項 に規定する中小企業及び個人事業主。
※本社が都外にある場合でも、事業所が都内にある場合は本事業への参加が可能です。

(2) 原則は、過去に東京都サイバーセキュリティ対策関連事業の支援を受けていない中小企業及び個人事業主。

(3) 本事業と同等のサイバーセキュリティ対策の内容を支援する東京都・東京都中小企業振興公社の補助事業を同時に活用していない中小企業及び個人事業主。

(4) 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、霊感商法など社会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。

2．参加規約及び留意事項

(1) 中小企業サイバーセキュリティ啓発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。
また、本事業へのお申し込みは定員に達し次第、締め切らせていただきます。申込多数の場合は参加いただけない事がございますのでご了承ください。

(2) 参加企業は下記 ①～③ に協力をお願いします。

① 専門家派遣の受け入れや意識調査へ積極的に協力し目標の達成を目指すこと。
ただし、やむを得ない事情で対応が難しい場合には、事前に運営事務局へ相談すること。

② 参加企業が支援期間中に企業譲渡や継承等で申し込み情報に変更が生じた場合は、東京都及び運営事務局に状況を申告し対応を協議すること。

③ 支援期間前後にセキュリティに関する意識調査及び本事業に関するアンケートへ協力すること。

(3) 本事業では、他の中小企業のセキュリティ対策の意識向上を目的としたヒアリング調査、アンケートを行います。
これらの回答を基に作成された成果事例を支援期間終了後に事業ホームページへ掲載します。
ただし、成果事例は企業のセキュリティ体制や機密情報に関する事項を含むことから、掲載内容については対象

企業の許可を得てから公開するものとします。

(4) 参加企業が応募時に虚偽の情報を記載、又は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。

(5) 次の ①～③ に該当し運営事務局が本事業への参加を不適切と判断した場合には支援期間中であっても事業参加を辞退していただく場合がございます。

① 説明会及びセミナーにおいて、運営事務局等スタッフの案内に従わない場合。

② 他の参加者の迷惑になる行為を行うなど、事業運営に悪影響を与える場合。

③ 参加申込後、申込者と連絡が取れない等で支援期間中に支援実施が困難な場合。

具体的には、お申し込みから 1 か月以内にセミナー参加日・専門家訪問日が調整できない、あるいは 4 回以上の日程変更が続いた場合は、支援ご辞退として取り扱わせていただきます。

(6) 本事業において実施されるセミナーを通して知り得た他の参加企業の情報は秘密を保持し、いかなる場合においても第三者に対し利用・開示・漏洩する事がないよう厳重に管理をお願いします。
また、参加企業からの要求に従い運営事務局が情報の返還もしくは破棄の指示をした場合は速やかに対応を実施してください。

(7) 参加者は、本事業の内容について、録音・録画、撮影及び SNS 等のメディアに投稿するなど、第三者に公開することを禁じます。

(8) 本事業に関するトラブルなどのご相談については、運営事務局までご連絡ください。

(9) サイバー攻撃対応演習セミナーでは、セミナー中に事務局が記録写真を撮影させていただきます。公開の予定はございませんが、予めご承知おきください。

3. 感染症の拡大抑制対策

(1) 各支援において、マスク着用等の感染症対策は自主的な判断ではありますが、感染症の拡大防止のためマスク着用等の協力をお願いする場合がございます。

(2) 発熱等の症状がある、または体調が悪い場合には各支援への参加をお控えいただき、事前に支援日の振替や日程調整などのご依頼を事務局宛てにいただけますようお願いいたします。

(3) 感染症の感染拡大の状況によっては、事業の延期若しくは中止又は開催方法の変更の可能性がございます。

4. 個人情報の取り扱い

(1) 本事業で知り得た個人情報については、本事業のサイトポリシー（個人情報保護方針）に定めるところにより取り扱い、本事業の範囲内の利用に限定いたします。

(2) 本事業の支援において取得したデータやアンケート結果等、本事業期間中に知り得た情報については、本事業の一環で成果報告書へ活用いたします。また、事業の成果については東京都産業労働局において匿名で公表する場合がございます。

(3) ご記入いただいた連絡先宛てに、東京都から中小企業関連施策についてのご案内や、本事業に関する周知等のご連絡をさせていただく場合があります。

5. 免責事項について

(1) サイバー攻撃対応演習セミナー会場内や専門家派遣時のけが等の傷害又は事故等について、東京都及び運営事務局は、あらゆる損害賠償責任から免責されるものとします。ただし、東京都及び運営事務局に故意また

は重過失が認められる場合には、この限りではございません。

(2) サイバー攻撃対応演習セミナー会場内や専門家派遣時の盗難・紛失について、東京都及び運営事務局は、あらゆる損害賠償責任から免責されるものとします。ただし、東京都及び運営事務局に故意または重過失が認められる場合には、この限りではございません。

(3) 荒天等の予期せぬ災害・地震その他天変地異や 会情勢等により、サイバー攻撃対応演習セミナー会場内及び専門家支援が中止となった場合について、東京都及び運営事務局は、あらゆる損害賠償責任から免責されるものとします。ただし、東京都及び運営事務局に故意または重過失が認められる場合には、この限りでございません。