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基本対策事業
募集要項

1 事業の目的

テレワークの普及やデジタル化、昨今のサイバー攻撃の激化により、中小企業のセキュリティ対策は急務となっていますが、費用面や人手不足といった課題により、いまだ対応が後手になっている企業が多く存在します。
本事業ではこうした状況を踏まえ、都内中小企業の皆様を対象に、サイバーセキュリティに関する事前診断を実施し、対策の第一歩として必要であるセキュリティ機器の設置やソフトウェアの導入を支援します。

また、情報セキュリティポリシーの策定や情報資産管理台帳の整備指導など、専門家によるきめ細かなサポートを実施することで、中小企業の基本的なセキュリティ対策の定着を図ります。支援終了後には、効果的な施策と取組事例の発信を行い、中小企業へのセキュリティ対策普及を進めるとともに、都内産業基盤の安定化を目指します。

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） 過去にサイバーセキュリティ支援事業に参加して支援を受けていない中小企業者
※支援内容は、UTM 機器試用・EDR 試用、情報セキュリティマネジメント指導だが、異なる支援内容を受けていた場合、この限りではない。

（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の補助事業を活用していない中小企業者（会社及び個人事業主）

（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

以下の支援①②③いずれも　令和７年５月 23 日（金）～（※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。）

【支援①UTM 機器設置コース】
【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】

4. 募集企業（定員数）

支援内容	定員
支援①UTM 機器設置コース	５０社
支援②EDR 導入コース	５０社
支援③情報セキュリティマネジメント指導コース	１００社

※事業申込企業のセキュリティ環境に応じて支援①②③を実施します。
※定員に達し次第、募集を締め切らせていただきます。

5. 参加費用

無料

6. 申込

（１）申込方法

事業ホームページ上の申込フォームより必要事項を入力のうえ、お申し込みください。
事業ホームページ URL：**https://kihontaisaku.metro.tokyo.lg.jp/**

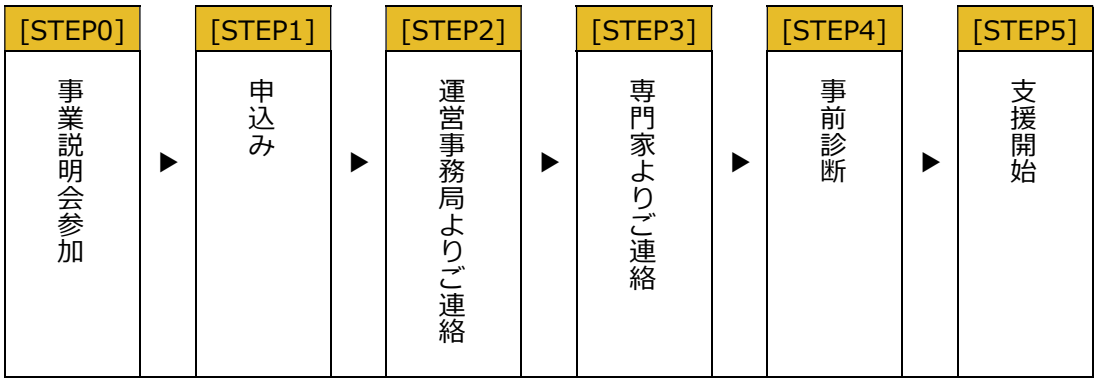
（２）申込みにおける注意事項

ア　お申込み後、3 営業日以内に運営事務局からご連絡（電話もしくはメール）をいたします。参加に当たっての規定や遵守事項についてご説明し、その内容についてご了承いただいた後、申込み完了となります。申込フォームの送信だけでは、申込みは完了しておりませんのでご注意ください。

イ　セキュリティに関する意識調査（アンケート）を支援後に実施いたしますので、ご協力をお願いいたします。
また、次年度（令和８年度）に本支援に関する調査を実施する場合がございます。その際にもご協力ください。

ウ　本事業終了後、参加企業の中から５社程度を対象として、中小企業のサイバーセキュリティ対策の参考となる取組等について、ヒアリング調査を行う場合がございますので、ご協力いただきますようよろしくお願いします。

＜お申込みの流れ＞



[STEP0]
申込みに際して説明会への参加は必須ではございませんが、本事業について詳細な説明をいたしますので、ぜひご参加いただき、事業内容についてご確認された上でお申し込みいただくことをお勧めします。

[STEP1]
事業ホームページ(Web)より参加申込フォームに必要事項を入力してお申込みください。
支援①UTM 機器設置コース（定員 50 社）、支援②EDR 導入コース（定員 50 社）、支援③情報セキュリティマネジメント指導コース（定員 100 社）ともにご応募が対象です。
※先着順で定員に達し次第応募を締め切ります。

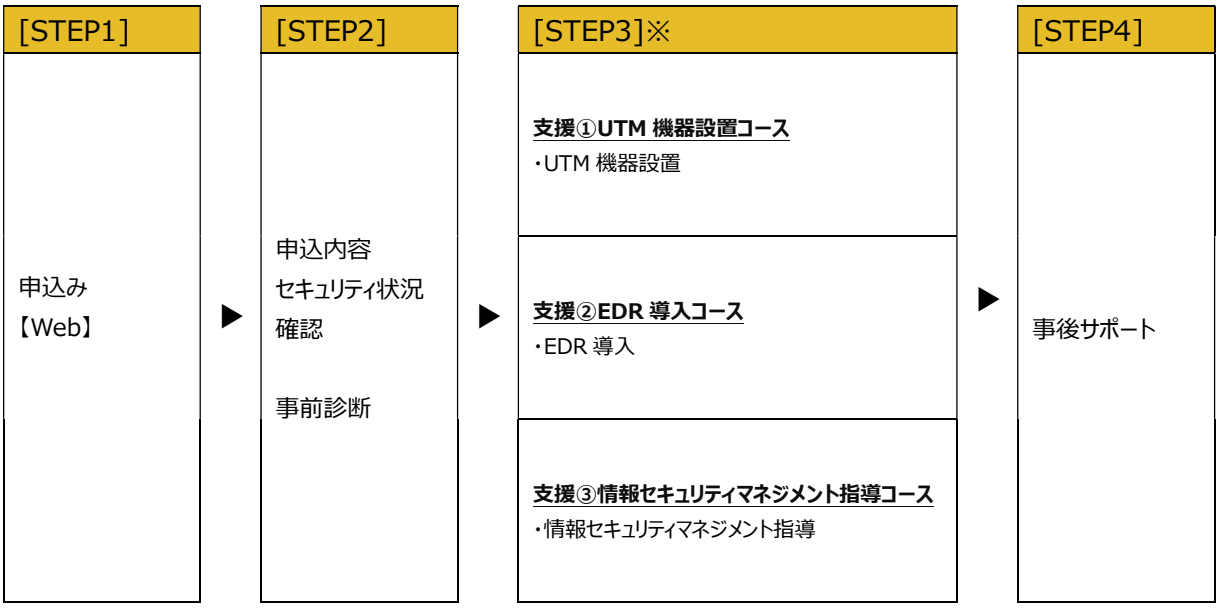
[STEP2]
申込フォーム受信後、3 営業日以内に運営事務局から連絡（電話もしくはメール）を差し上げます。申込内容の確認や参加に当たっての規定や遵守事項をご説明差し上げますので、その内容についてご了解をいただいた後に、申込完了となります。

[STEP3]
申込完了後、3 営業日以内に専門家から連絡（電話もしくはメール）を差し上げます。お申込み企業のセキュリティ機器の設置状況やセキュリティ対策状況を確認させていただき、初回の支援日を調整させていただきます。

[STEP4]
事業申込企業に訪問もしくはオンラインにて事前診断を行います。ご希望の支援内容に沿って事業申込企業のセキュリティ環境をお聞きし、支援コースを決定します。（支援③情報セキュリティマネジメント指導コースのみお申込みの場合は、事前診断を省く。）

[STEP5]
支援コースの決定をもって、参加確定といたします。

7．支援の流れ



※セキュリティ環境に応じて上記支援を実施します。

[STEP1]

事業ホームページ(Web)より参加申込フォームに必要事項を入力してお申込みください。

[STEP2]

初回対応および事前診断を実施し支援コースを決定。

その際に、申込企業のセキュリティ状況を確認させていただきます。

確認事項・ネットワークの接続構成　・HUB の空きポートの有無　・既存の UTM 機器の設置有無
・PC 台数　・お使いの OS　・アンチウイルスソフトの導入の有無　・EDR の有無
・情報セキュリティの基本方針や社内規定についての整備状況　等
※UTM は設置作業が必要になります。

[STEP3]

申込企業の社内のセキュリティ環境に応じて、以下の支援の中から実施します。

支援①UTM 機器設置コース

◆UTM 機器設置

・1 台で複数のセキュリティ機能を有する UTM を無料で 3 か月間体験できます。
・UTM のログからサイバー攻撃状況を確認でき、その機能を実感できます。
・期間中、サポートデスクをご利用いただけます。

支援②EDR 導入コース

◆EDR 導入

・各種サイバー攻撃の検出・分析、自動修復状況を確認できる EDR を 3 か月間無料体験
・期間中、サポートデスクをご利用いただけます。

支援③情報セキュリティマネジメント指導コース

◆情報セキュリティマネジメント指導

・専門家によるサイバーセキュリティに関する基本方針や規程等の策定等に向けた指導・支援を行います（計４回）。

・SECURITY ACTION 二つ星宣言の達成を目指せるようサポートします。

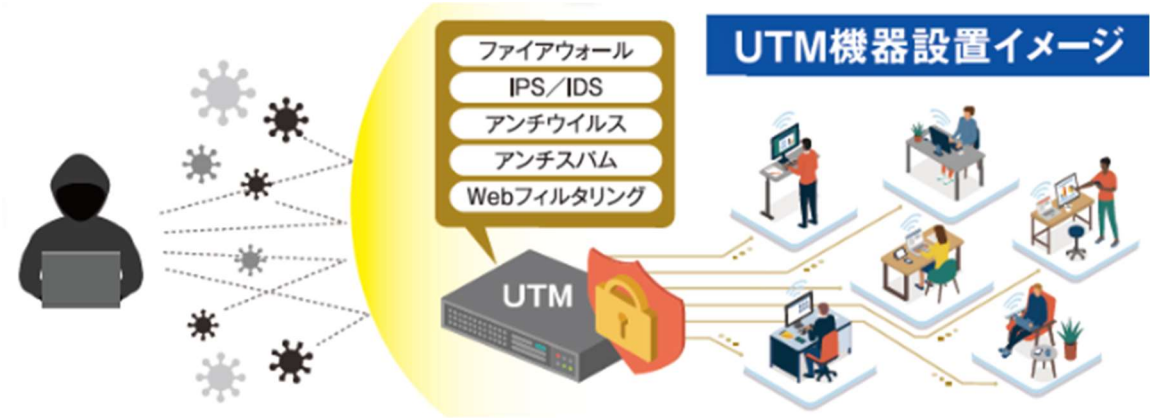
[STEP4]

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します。

８．支援内容の詳細

«支援①UTM 機器設置コース»

セキュリティ対策機器の体験機会の提供



[支援詳細１] セキュリティ機器の設置によるサイバー攻撃状況の把握・分析

・事業所内にセキュリティ対策機器（UTM※1）を設置し、ウイルスや不正アクセスをブロックします。

・不正アクセス等を常時監視し、サイバー攻撃の検知やブロック状況について、月次でレポートを配信します。これにより、自社のサイバー攻撃状況を把握できます。

※1 UTM とは

UTM（統合脅威管理）とは、複数の異なるセキュリティ機能を一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、集中的にネットワーク管理ができる機能を持ち、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。

セキュリティ対策機器（UTM）の設置に関して

- 本事業に基づき、受託事業者が提供する UTM の体験機会（3 か月間・無償）を提供いたします。
- その他、UTM の利用条件については、受託事業者が定める利用規約に準じます。詳しい内容は運営事務局から個別にご説明いたします。
- UTM の設置に当たって、参加企業の皆様の環境を把握するため事前調査を実施いたします。事前調査の結果によっては、UTM の設置ができないことがございますので、ご了承ください。
- 設置台数については基本的に 1 企業 1 台とさせていただきます。
- 設置場所は、都内にある拠点に限ります。
- UTM 設置にあたり必要となる周辺機器（電源タップや HUB、LAN ケーブル等）については、本事業の支援対象外となります。周辺機器のご用意に伴う費用のご負担をいただきますよう、お願いいたします。

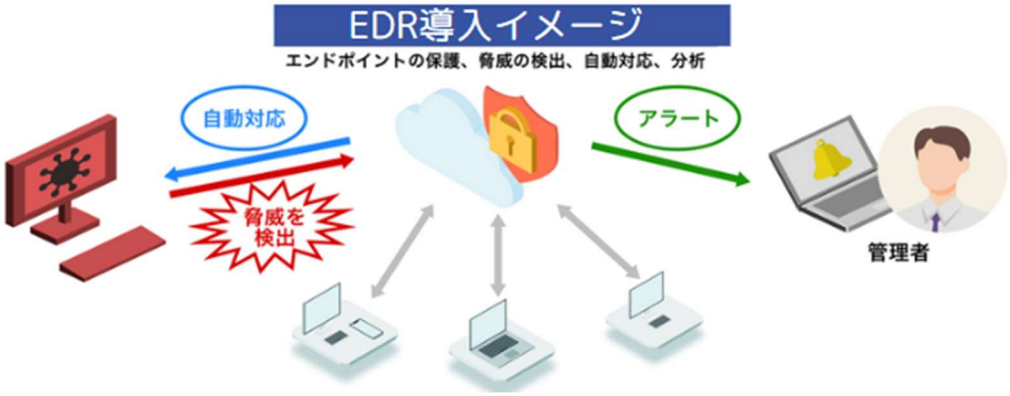
・UTM など機器の設置時にかかる電気代のご負担についてもお願いいたします。
・UTM の体験期間中に、設置中の UTM が取得したウイルスや不正プログラム等の検知状況のレポートを定期的に送付いたします。その他、ご参考となる追加情報を掲載したレポートを別途送付する場合がございます。
・本事業終了後、セキュリティ対策の継続を希望する場合には、運営事務局にご相談ください。参加企業の皆様において、受託事業者と契約し、UTM を継続することができます。希望されない場合は、設置した UTM 機器の撤去工事をいたします。
・UTM 設置に伴う個人情報取扱いの方針については、10.留意事項の（2）個人情報の取り扱いに記載のとおりとさせていただきます。

[支援詳細２] インシデントサポートセンター・オンサイトサポートの提供（UTM の体験期間中）

・サポートセンターにてサイバー攻撃に係る各種お困りごとへのご相談に対応します。
また、UTM の検知内容を確認し、インシデント判断を行い、遠隔駆除を実施します（３か月の無料体験期間中、24 時間 365 日対応）。
・インシデントの発生等により、緊急対応の必要性などから現地での対応が必要な場合は、現地に駆け付け支援を実施します（駆けつけ対応時間 平日 9：00～17：00）。

«支援②EDR 導入コース»

セキュリティ対策アプリケーションソフトの体験機会の提供



[支援詳細１] セキュリティ対策アプリケーションソフト導入によるサイバー攻撃状況の把握・分析

・事業所内の PC や連携しているデバイスにセキュリティ対策アプリケーションソフト（EDR※2）を導入し、異常検出や調査・分析を行います。
・検知したセキュリティリスクを技術担当者が毎日チェックし、月次でセキュリティレポートを配信します。これにより、自社のサイバー攻撃状況を把握できます。
※2 EDR とは
UTM 等を通過した不正な通信を検出し、隔離、通知、分析、処理を行う事でエンドポイントを守るアプリケーションのことです。

セキュリティ対策アプリケーションソフト（EDR）の導入に関して

・本事業に基づき、受託事業者が提供する EDR の体験機会（3 か月間・無償）を提供いたします。
・その他、EDR の利用条件については、受託事業者が定める利用規約に準じます。詳しい内容は運営事務局から個別にご説明いたします。
・EDR の導入に当たって、参加企業の皆様の環境を把握するため事前調査を実施いたします。事前調査の結果によっ

ては、EDR の導入ができないことがございますので、ご了承ください。
・ 導入数については基本的に 1 企業 300 ユーザー※3とさせていただきます。
・ EDR の導入時にかかる通信料等のご負担をお願いいたします。
・ EDR の体験期間中に、設置中の EDR が取得したウイルスや不正な通信等の検知状況のレポートを定期的に送付いたします。その他、ご参考となる追加情報を掲載したレポートを別途送付する場合がございます。

・ 本事業終了後、セキュリティ対策の継続を希望する場合には、運営事務局にご相談ください。参加企業の皆様において、受託事業者と契約し、EDR を継続することができます。希望されない場合は、導入した EDR ライセンスを無効化いたします。
・ EDR 導入に伴う個人情報取扱いの方針については、10.留意事項の（２）個人情報の取り扱いに記載のとおりとさせていただきます。

※3　1 企業 300 ユーザー
１ユーザーあたり 5 デバイスまで接続可能。導入場所は問いません。

[支援詳細２] インシデントサポートセンター・オンサイトサポートの提供（EDR の体験期間中）

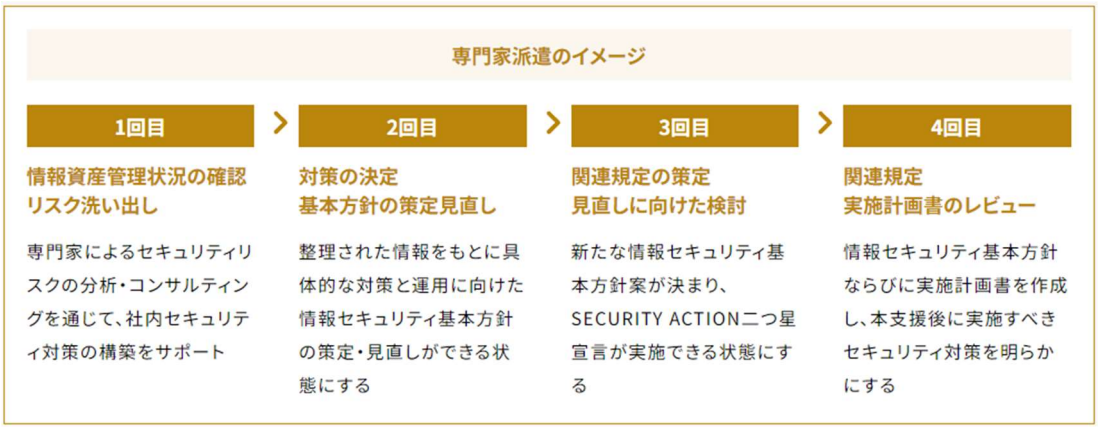
・サポートセンターにてサイバー攻撃に係る各種お困りごとへのご相談に対応します。
また、EDR の検知内容を確認し、インシデント判断を行い、遠隔駆除を実施します（３か月の無料体験期間中、24 時間 365 日対応）。
・インシデントの発生等により、緊急対応の必要性などから現地での対応が必要な場合は、現地に駆け付け支援を実施します（駆けつけ対応時間　平日 9：00～17：00）。

«支援③情報セキュリティマネジメント指導コース»

現状のリスクを把握し、情報セキュリティ対策と運用に向けた基本方針や規定等を策定し、「SECURITY ACTION 二つ星の宣言※4」実施を目指す

[支援詳細１] 情報セキュリティマネジメント指導・支援の実施

・サイバーセキュリティに関する基本方針や規程等の策定に向けた指導・支援を行います。
・専門家が参加企業の皆様のもとへお伺いし、1 社につき全 4 回の指導を実施いたします。ご希望によりオンライン形式でも実施可能です。
・専門家のアドバイスのもと、セキュリティ基本方針や関連規約を策定しながら対策・運用の実施計画を作成することで、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ある、SECURITY ACTION 二つ星宣言を目指すためのサポートを行います。
・情報セキュリティマネジメント指導に伴う個人情報取扱いの方針については、10.留意事項の（2）個人情報の取り扱いに記載のとおりとさせていただきます。



※4 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組むことを宣言する制度です。

宣言実施にはセキュリティ基本方針の策定・公開が必要ですが、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み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。

9．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他、セキュリティの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。お申込みをご検討中の方は、ぜひ説明会にご参加ください。

〈説明会日程〉

第１回	日時	令和７年６月 26 日(木) 13:30～15:30（120 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 8D
	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】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
		【第３部】東京都中小企業サイバーセキュリティ基本対策事業説明
第２回	日時	令和７年７月８日(火) 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10B
	プログラム	【第１部】AI 時代のサイバーセキュリティ対策とは
		【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説明
第３回	日時	令和７年７月 24 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 （JR 立川駅徒歩３分）
	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
		【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説明
第４回	日時	令和７年８月６日(水) 13:30～15:00（90 分）
	場所	東京都渋谷区渋谷 2-22-3 / TKP ガーデンシティ渋谷 カンファレンスルーム E
	プログラム	【第１部】サイバー攻撃から中小企業を守るためのセキュリティ対策と復旧戦略
		【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説明

【申込方法】事業ホームページよりお申し込みください。
https://kihontaisaku.metro.tokyo.lg.jp/
【申込受付期間】各セミナー開催日前日まで
【実施方法】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（zoom）100 名
※第 1 回　6 月 26 日（新宿会場）のみ　会場 50 名
【参 加 費】無料

10. 留意事項

(1) 運営、実施について
・中小企業サイバーセキュリティ基本対策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。
・応募者が、応募に際し虚偽の情報を記載し、その他東京都及び運営受託者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。
・応募企業について、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。

(2) 個人情報の取り扱い
・本事業で知り得た個人情報については、本事業のプライバシーポリシー(個人情報保護方針)(https://kihontaisaku.metro.tokyo.lg.jp/privacypolicy.html)及びサイトポリシー(https://kihontaisaku.metro.tokyo.lg.jp/sitepolicy.html)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。
　また、利用目的の達成に必要な範囲で、お預かりした個人情報を外部委託することがあります。委託する場合は、運営事務局と個人情報保護体制が同等又はそれ以上の水準に達していると運営事務局が判断した法人又は個人に、利用目的の範囲内においてのみ委託いたします。
・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。
・ご記入頂いたご連絡先宛てに、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ご連絡をさせていただく場合があります。

(3)トラブル対応について
・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。
なお、UTM など、本事業の受託事業者の固有のサービスに関する事項については、受託事業者が定める規約に準じます。詳しい内容は運営事務局までお問い合わせ下さい。

11. 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（祝日を除く）
メール： ade.jp.kihontaisaku@cybersecurity-tokyo.com
URL： https://www.kihontaisaku.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。