令和６年５月
運営事務局

中小企業サイバーセキュリティ社内体制整備事業
募集要項

1 事業の目的

社会における DX 化が急速に進行していますが、本来、DX 化と車輪の両輪であるべきサイバーセキュリティ対策は、多くの中小企業において体制整備が追い付いていない状況であり、喫緊の課題となっています。

この現状を踏まえ、東京都では、サイバーセキュリティ対策の普及啓発に加え、セキュリティ機器の導入支援等のハード面の整備を進めていますが、こうした整備を実施した後も、各中小企業のリソース不足（人材面・ノウハウ面）が、継続的なサイバーセキュリティ対策の実施に向けて大きな障害になると予想されます。

そこで、本事業では、基本的なセキュリティ機器・ソフトウェアを備え、セキュリティに関する社内方針の策定までは実施したものの、その先どうしたらいいのか分からないと不安を抱える中小企業の皆様を対象に、約 7 ヶ月間にわたり、セミナー・ワークショップで専門知識と実践的な課題解決の手法を学んでいただき、サイバーセキュリティ対策の中核を担う人材の育成を支援します。

また、専門家派遣をあわせて実施することで、ワークショップで洗い出した課題を中心に自社が直面している問題の解決を図り、社内体制の整備を進めます。

さらに、本事業で作成するセミナーテキストや事例集を広く社会へ公開することで、中小企業がセキュリティ対策を実行する際に使えるツールとして利活用し、中小企業全体のセキュリティ対策の強化を目指します。

2. 当事業の募集対象

参加申込にあたっては、以下の（１）～（３）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（会社及び個人事業者）

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
製造業、建設業、運輸業、その他	３億円以下又は 300 人以下
卸売業	1 億円以下又は 100 人以下
サービス業	5,000 万円以下又は 100 人以下
小売業	5,000 万円以下又は 50 人以下

（２） 社内にてセキュリティ対策を継続的に実施することを想定した実践的な内容であることから、UTM や EDR 等の一定程度のセキュリティ機器・ソフトウェアを導入し、情報セキュリティポリシー（セキュリティ対策の方針や行動指針）を整備済みである中小企業者 ※

※ 本事業で必要な社内セキュリティ体制を有していない方には、運営事務局から関連事業（国及び都）をご案内いたします。

（３）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６年５月23日（木）　から　令和６年６月28日（金）まで

4. 募集企業（定員数）

本事業では、サイバーセキュリティ対策を継続的に実施していくための社内体制整備をサポートするだけでなく、取組内容や成果、参加企業の皆様の声などをロールモデルとして広く社会へ普及させ、中小企業全体の体制強化にも役立つ多様な事例の創出を目指しています。

そのため、多様な業種の皆様にご参加いただけるよう、下記の募集枠で合計 40 社を募集いたします。

※業種の区分けについては、日本標準産業分類などを参考にしています。

※なお、各枠の 10 社は目安となります。応募状況により変動することがあります。

募集企業（定員数）40 社	**小売・卸売枠 10 社程度**	小売業
		卸売業
	建設・製造枠 10 社程度	建設業
		製造業
	サービス・その他枠 20 社程度	情報通信業
		運輸業、郵便業
		金融業、保険業
		不動産業、物品賃貸業
		学術研究業、専門・技術サービス業
		宿泊業・飲食サービス業
		生活関連サービス業・娯楽業
		教育・学習支援業
		医療・福祉
		その他の業種

5. 受講対象者

・本事業における取組に意欲的に参加できる経営層、セキュリティ担当者　等

※下記７（２）申込みにおける注意事項ウ及びエ記載の**「参加同意書」及び「機密保持の同意書」について、本事業への参加者ご自身と、所属企業のご同意をいただける方**が対象となります。

※参加人数は、1 社につき 1 名とさせていただきます。

※本事業は継続したプログラムを受講していただく形で構成されている為、原則としてお申し込み時にご登録いただいた方に最後まで受講していただくことが前提となります。ただし、急な商談など、やむを得ない事情が発生した場合は、運営事務局までご相談ください。ご事情をお伺いし、当該回におけるお取り扱いをご案内させていただきます。

6. 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。

7. 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。

https://forms.office.com/e/ZqxgkgJyKt

【受付期間】 令和 6 年 5 月 23 日（木）～令和 6 年 6 月 28 日（金）

（２）申込みにおける注意事項

ア　お申込み後、折り返し運営事務局から 3 営業日以内に電話連絡をいたします。

※本事業は 2（2）のとおり、一定のセキュリティ対策を実行中の企業が対象となることから、運営事務局から電話にてセキュリティレベルを確認させていただきます。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方には、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、運営事務局から関連事業を別途ご案内いたします。

※また、運営事務局から電話確認をさせていただく際に、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。その内容についてご了解をいただいた後に、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　参加者は、支援期間中に行われる**全 10 回のセミナー・ワークショップ及び、１社につき４回の専門家派遣に参加できること**が条件となります。

ウ　セミナー・ワークショップなどにおいて、**企業のセキュリティ体制等の機密情報に係る事項**をテーマとして取り扱い、**参加企業間で自社の状況や課題についてディスカッションを行うことが想定される**ため、参加企業全社に対し、支援開始前に別添「**機密保持の同意書**」においてご同意をいただきます。

※なお、企業の内情に係る事項を採り上げる可能性がある場合には、事前に必ず参加企業への同意を求めることとし、同意を得られない場合には、内容を差替えるなどの配慮を行います。

エ　また、本事業では、取組内容や成果、参加企業の皆様の声などをロールモデルとして広く社会へ普及させ、中小企業全体の体制強化にも役立てるため、セキュリティ課題解決の為のツールとして活用いただくことを目的に、支援終了後に、事業の中で使用したテキストと、**参加企業全 40 社を対象として、本事業で得られた成**

果を取りまとめた「事例集」を事業ホームページ等で公開します。

※事例集作成に当たっては、**事例集を作成することへの同意や、作成に必要な参加企業への取材やアンケートへのご協力**について、参加企業全社に対し、支援開始前に別添「**参加同意書**」にてご同意をいただきます。

※事例集には企業名や担当者の個人名は掲載せず、参加企業が特定できないようにいたします。

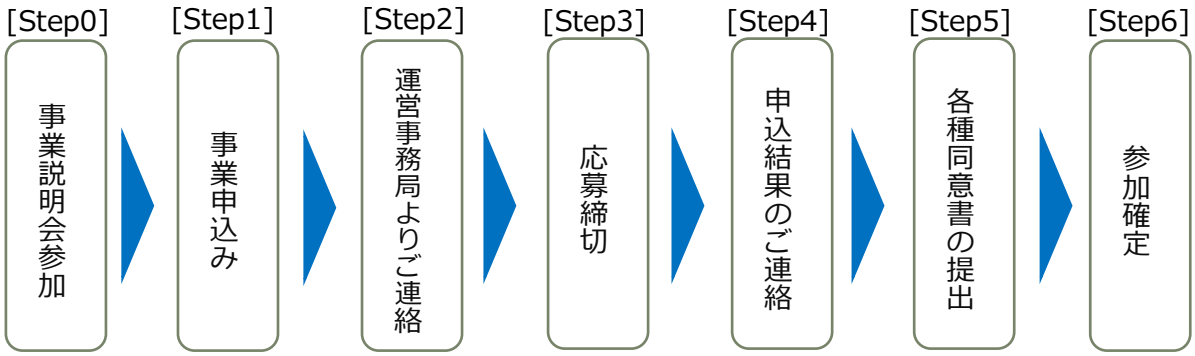
※なお、**事例集も、企業のセキュリティ体制等の機密情報に係る事項をその内容とする**ため、前項ウ同様に、「**機密保持の同意書**」において参加企業の皆様にご同意をいただきます。

オ　本事業の実施に際し、取組内容の記録、広報媒体の作成、事例集の素材収集等の目的で、運営事務局が事業の取組風景等について、参加者を含めた撮影、録音、録画を実施します。

なお、撮影した媒体は、参加者の後ろ姿など個人の特定ができないものに限り、セミナー・ワークショップの実施内容のサマリー内に使用し、ウェブサイト上に公開します。

本事業への参加に当たっては、この点にご同意をいただきますが、運営事務局が記録するこれらの媒体について、東京都及び運営事務局が上記の目的以外に使用する場合には、その使用目的や使用方法について、参加者及びその所属企業に対し事前に確認を行い、許可を得ることとします。

＜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、事業内容についてよく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.　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。

【応募締切：令和６年６月 28 日（金）】

Step2.　申込フォーム受信後、3 営業日以内に運営事務局から電話連絡を差し上げます。お申込み企業のセキュリティレベルが本事業の対象に合致することを確認させていただきます。また、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.　令和６年６月 28 日（金）23 時 59 分に応募を締め切ります。

※応募多数の場合は抽選にて、小売・卸売枠 10 社程度、建設・製造枠 10 社程度、サービス・その他枠 20 社程度の参加企業を決定します。（各枠の社数は目安となります。応募状況により変動することがあります）

Step4.　7 月上旬をめどに、抽選の有無や結果に関わらず、お申込みいただいた皆様全員に、申込みに対する結果通知をメールにて発送いたします。参加対象となられた方へは、結果通知をお送りするとともに、運営事

務局からメールまたは電話にて、参加意思の確認をさせていただきます。

Step5. 運営事務局より、事業参加に当たっての「参加同意書」、「機密保持の同意書」をお送りします。

Step6. 「参加同意書」及び「機密保持の同意書」の運営事務局への提出をもって、参加確定といたします。

【備考】 申込み結果通知後、本事業への参加を辞退される場合には、結果通知の到着後 2 営業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差し上げます。

8. セミナー・ワークショップ開催場所

【所在地】

東京都新宿区西新宿 1-22-2 新宿サンエービル内

ビジョンセンター西新宿会議室

【交通機関】

JR 各線「新宿駅」南口・西口 徒歩 5 分

東京メトロ・都営地下鉄「新宿駅（7 番出口）」徒歩 1 分

9. 支援内容

本事業では、セミナーやワークショップの取組を通じて、セキュリティ対策を計画的に実行できる知識・ノウハウが身に付くだけでなく、参加企業同士のディスカッションを通じたセキュリティ課題の洗い出しや、専門家派遣による課題解決へのサポートを通じ、セキュリティ機器の運用や業務に直結した社内規程の整備をする際に、**次に何をしたらいいか分からない状態**を解消し、本事業の参加後には、自力でセキュリティ対策計画が立てられるようになることを目指します。また、DX 推進に必要なセキュリティの考え方・サプライチェーン対策などの最新のトレンド情報も学ぶことができます。

【 セミナー・ワークショップ（全 10 回）】

セミナーでは、セキュリティ対策の知識だけでなく、役割の違いや DX の推進といった、今後の中小企業のセキュリティを担う中心人物を育成します。ワークショップでは、セミナーで得た知識を基に、グループメンバーで課題や取組事例、問題点を共有し、他社の事例に対して全員で対策を検討・議論します。多様なセキュリティ課題を疑似体験することで、未知の課題にも対応できるようになります。また、インシデント等を題材とした事例に基づく演習により今後発生しうる課題への対応力や実践力を強化します。

セミナー・ワークショップ実施内容（予定）

・実施日程（全日程火曜日です）

第 1 回	第 2 回	第 3 回	第 4 回	第 5 回	第 6 回	第 7 回	第 8 回	第 9 回	第 10 回
7/23	8/6	8/20	9/10	9/24	10/8	10/22	11/19	12/17	1/21

・セミナーとワークショップは同日に開催します。

原則セミナーは 13:00～15:00（２時間）、ワークショップは 15:15～17:15（２時間）で実施します。

参加者のコミュニケーションを図る目的で、座談会を４回程実施予定です（17:30～18:30※任意参加）。

・特別な事情がない限り、原則として会場での対面形式で実施いたします。

・原則として全日程（10 回）への参加が必須となります。

※やむを得ないご事情が生じた場合には、事前に運営事務局までご相談ください。
※各回のセミナー・ワークショップが終わり次第、同日にアンケートを回答していただきます。
（１）セミナー内容
・全 10 回のセミナーで以下の内容について学んでいただきます。

テーマ・概要
【テーマ】サイバーセキュリティを取り巻く背景 ・クラウドワークロードが複雑化し、サプライチェーンの脆弱性が狙われ、生成 AI・IoT・DX などの新しいテクノロジーへのセキュリティ対策が求められている現状を解説します。 ・Society5.0 等で示されている社会の方向性と実現に向けた基本概念を理解するとともに、その環境下で中小企業に求められるセキュリティ対策の考え方を理解することを目的とします。
【テーマ】中小企業に求められるデジタル化の推進とサイバーセキュリティ対策 ・重大なインシデント発生から課題解決までを事例で理解するとともに、IT 活用、サイバーセキュリティ対策の必要性を解説します。
【テーマ】これからの企業経営に必要な IT 活用とサイバーセキュリティ対策 ・企業経営に必要な IT 活用、サイバーセキュリティ対策について、フレームワーク等を参考に、組織の現状と目標に応じた対策手段を解説します。
【テーマ】セキュリティ事象に対応して組織として策定すべき対策基準と具体的な実施 ・インシデント事例に対応したレベル別の具体的な対策方法と対策手順の作成について解説します。
【テーマ】各種ガイドラインを参考にした対策の実施 ・関係機関から提示されている各種サンプル、ひな形をベースとした具体的な対策方法を解説します。
【テーマ】ISMS 等のフレームワークの種類と活用法の紹介 ・組織全体にわたるセキュリティの向上を図るために、各フレームワークの概要と活用法について解説し、損失となりうるサイバーセキュリティのリスクへの効率的な対策を施すために必要なリスクマネジメントの方法を解説します。
【テーマ】ISMS の構築と対策基準の策定と実施手順 ・ISMS に準拠して、自社に必要な管理策を選択することで対策基準を策定し、策定した対策基準の実施手順をひな形等で解説します。 ・中小企業の規模・立ち位置、リスクアセスメント結果等に応じて、必須・選択式の事項と判断基準を明示し、対策（組織、人、物理、技術）の実施手順を学びます。また、セキュリティ対策を実施した結果の評価方法を学びます。
【テーマ】具体的な構築・運用の実践 ・作成した実施手順に沿った具体的な対策（実装・運用）を、国内外の中小企業向けのガイドラインの中から、優先的に実施すべき内容を選び解説します。

・対策（組織、人、物理、技術）の実施手順に沿った具体的な手順のポイントや、ガイドラインのシステム導入工程に沿ってセキュリティ機能を実装・運用するための方法を学びます。

【テーマ】中小企業が組織として実践するためのスキル・知識と人材育成

・サイバーセキュリティ対策を実践するためのスキル・知識の理解を目的とします。IT およびデジタル人材に必要なスキル（ITSS+、Di-Lite（デジタルリテラシー領域）、プラス・セキュリティ等）と知識を持った人材育成・人材確保について解説します。

・チェンジマインド、リスクキリングを含めた実施計画および教育・研修の実施内容について、IT およびデジタル人材のスキル、知識の認定制度と活用方法を学びます

【テーマ】全体総括

・これまでの内容を振り返り、重要な知識を定着させることを目的とします。

・受講者が今後のセキュリティ活動において、自走できるために必要な考え方、経営者等に説明するための組織として実施すべき事項と概要について解説します。

（２）ワークショップ内容

・ワークショップは以下の構成で行います。

①テーマ紹介と目標設定→②グループ討議→③グループ発表と質疑応答→④講師のコメントとフィードバック→⑤意見交換

・各回のテーマと内容は以下表のとおりです。

ワークショップ内容詳細	
第１回	**【テーマ】自社の IT 活用とセキュリティ事情の検討** ・自社の IT 活用状況と、生成 AI など近年のトレンドを踏まえた今後の課題を検討 ・自社のセキュリティ状況と、セキュリティの知識向上に向けた今後の課題を検討 ・自社の状況分析を基にグループでの意見交換、協議、発表
第２回	**【テーマ】インシデント事例を活用した対策基準の検討** ・最新のインシデント事例を踏まえた対策基準の検討 ・最新のガイドラインを参考にした対策基準の検討 ・インシデント事例、ガイドラインを基にグループでの意見交換、協議、発表
第３回	**【テーマ】机上演習：資産台帳作成およびリスクアセスメント** ・リスクアセスメントの実施に必要となる情報資産の洗い出し ・リスクアセスメントを実施し、リスクレベルを算出 ・仮想会社を基にグループでの意見交換、協議、発表
第４回	**【テーマ】机上演習：対策基準の作成** ・リスクアセスメントの結果をもとに必要な管理策を検討 ・管理策をもとに対策基準および適用宣言書を作成 ・仮想会社を基にグループでの意見交換、協議、発表
第５回	**【テーマ】机上演習：実施手順の策定** ・対策基準を参考に実施手順を作成 ・仮想会社を基にグループでの意見交換、協議、発表

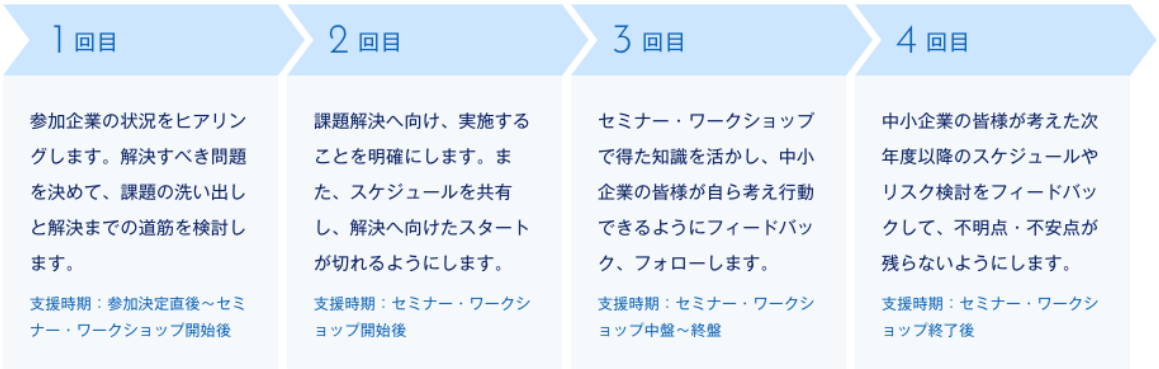
第６回 第７回	**【テーマ】机上演習：実施手順に沿った具体的な対策の検討** ・実施手順を実践するため、情報セキュリティリスク対応計画書を作成 ・仮想会社を基にグループでの意見交換、協議、発表
第８回 第９回	**【テーマ】人材確保の検討** ・求める人材・スキルの設定 ・実施計画書の作成 ・教育・研修の実施内容検討 ・自社の状況分析を基にグループでの意見交換、協議、発表
第 10 回	**【テーマ】振り返りおよび経営者に対する説明事項の検討** ・セミナーやワークショップを振り返り、組織として実践すべき事項の検討 ・経営者に対して実践すべき事項を説明するために必要な事項の検討 ・自社の状況分析を基にグループでの意見交換、協議、発表

【 専門家派遣 （全４回）】

参加企業の皆様がワークショップを通じて洗い出した課題の解決を支援するため、多様な得意分野を持つ専門家（ネットワーク設計・構築などの技術分野での経験、リスク分析、セキュリティ事故対応や再発防止策の検証、監査、セキュリティ教育、各種セミナー・支援の講師経験など）が、現場の状況に対応したサポートを提供いたします。セミナーやワークショップで得た知見を活かし、参加企業の皆様が自ら対策を立案できるよう、アドバイスも行います。

専門家派遣実施内容（予定）
・実施期間は令和６年７月～令和７年１月です。 ・参加企業の都内事業所への訪問、またはオンラインで実施します。 ・1 回の派遣に要する時間は、約 2 時間です。 ・初回の専門家派遣は、7 月中旬から 8 月上旬を予定しています。参加確定後に日程調整を行い、順次実施いたします。 ・原則として、1 社４回の専門家派遣の受け入れが必要です。

〈専門家派遣支援イメージ〉



10. オンライン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	6 月 6 日(木)	14:00～15:30
第 2 回	6 月 12 日(水)	14:00～15:30
第 3 回	6 月 18 日(火)	14:00～15:30

実施方法：Zoom を利用したオンライン開催

申込方法：以下の事業説明会申込 URL、または右上 QR コードよりお申込みください。受付後に参加用 URL をお送りいたします。

＜事業説明会申込 URL＞

https://forms.office.com/e/kkhhrtR6kz

定員：各回先着 100 名　※定員になり次第、締め切らせていただきます。

申込締切：各開催日前日までとさせていただきます。

※説明会後にアンケート回答にご協力をお願いいたします。

11. 留意事項

(1) 応募に当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) 本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) 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。

(4) 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。

(5) 本事業への参加に当たっては、9 支援内容に記載の本事業のセミナー・ワークショップ・専門家派遣にすべてご参加いただくこと、また、7 (2)に記載の申込みにおける注意事項の全項目について、本事業への参加を希望される本人及び所属企業のご理解とご了解をいただくことが条件となります。

12. 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。

中小企業サイバーセキュリティ社内体制整備事業運営事務局

TEL：0120-138-166

受付時間：平日 9:00～17:00（祝日を除く）

メール：ade.jp.shanaitaisei@jp.adecco.com

URL：https://shanaitaisei.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。

別添 1

参加同意書

私／当社は東京都が主催し、アデコ株式会社（以下、「運営事務局」という。）が受託し運営する「中小企業サイバーセキュリティ社内体制整備事業」（以下、「本事業」という。）に参加するに当たり、本事業の参加者及び参加者の所属する企業として、以下の事項について同意します。

第１　事業参加について

（ア）参加者及び参加者の所属企業が、暴力団等の反社会的勢力でないこと、反社会的勢力との関係を有しないこと及び反社会的勢力から出資等の資金提供を受けていないこと。

（イ）参加者及び参加者の所属企業が、訴訟や法令遵守上の問題を抱えていないこと。

（ウ）公的な資金に基づく本事業への参加について、社会通念上、不適切であると判断されるものではないこと。

（エ）運営事務局等スタッフの案内に従わない、他の参加者の迷惑になる行為を行う等、運営事務局が本事業への参加を不適切と判断した際には、支援期間途中であっても事業参加の辞退を求める場合があること。

（オ）参加者は、特別な事情がある場合を除き、原則として、支援期間中に積極的に本事業へ参加し、達成目標の実現を目指すこと。具体的には、原則、セミナー・ワークショップの全日程（10 回）への参加及び１社につき４回の専門家派遣の受け入れを行うこと。

ただし、この点についてやむを得ない事情が生じた場合には、事前に運営事務局へ相談すること。

（カ）運営事務局が提供する参加企業間の相互学習や、コミュニケーションを目的としたコミュニティに対し、積極的に参加すること。

（キ）参加者は、本事業の内容について、録音、撮影及び録画を行わないこと。

（ク）参加者は、本事業の内容について、ＳＮＳ等メディアに投稿するなど、第三者に公開しないこと。

第２　広報施策、支援内容の公開について

（ア）本事業の実施に際し、運営事務局は、取組内容の記録、広報媒体の作成、事例集の素材収集等の目的で、事業の取組風景等について、参加者を含めた撮影、録音、録画を実施する。なお、撮影した媒体は、参加者の後ろ姿など個人の特定ができないものに限り、セミナー・ワークショップの実施内容のサマリー内に使用し、ウェブサイト上に公開する。参加者及びその所属企業は、本事業への参加に当たり、上記の趣旨目的を理解の上、これに同意することを要する。

ただし、運営事務局が記録するこれらの媒体について、東京都及び運営事務局が上記の目的以外に使用する場合には、その使用目的や使用方法について、参加者及びその所属企業に対し事前に確認を行い、許可を得るものとする。

（イ）本事業では、参加企業全 40 社を対象として、本事業で得られた成果を「事例集」として、支援期間終了後に事業ホームページ等で公開することを目標とする。その趣旨及び目的としては、取組の過程や得られた成果、参加者及び所属企業のコメントなどを取りまとめ、セキュリティ対策のロールモデルとして広く社会へ普及させ、事業に直接参加していない中小企業の体制強化にも役立てることにある。

参加者及びその所属企業は、本事業への参加に当たり、事例集を作成すること及びその作成に必要な参加企業への取材やアンケート等への受け入れに関し、その趣旨目的を理解の上、これに同意することを要する。

ただし、事例集については、得られた成果のレベルや、セキュリティ体制等の企業の機密情報に係る事項を含むことから、その記載内容については、運営事務局から参加者及び参加者の所属企業に対し、事前の確認や綿密な相談を実施することを前提とし、企業の許可を得てから公表するものとする。

なお、事例集作成だけでなく、本事業ではその取組に際し参加企業の機密情報に関する事項を内容とするため、参加者及び参加者の所属企業は、別途「機密保持の同意書」において定める事項について、その趣旨目的を理解の上、これに同意することを要する。

第３　免責事項について

（ア）セミナー・ワークショップ会場内で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する。

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、この限りでない。

（イ）セミナー・ワークショップ会場内での盗難・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する。

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、この限りでない。

（ウ）荒天等の予期せぬ災害・地震その他天変地異や社会情勢等により、セミナー・ワークショップ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する。

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、この限りでない。

第４　支援期間中に、本同意書のいずれかの内容に関する変更が発生しうる事象が生じた場合は、下記の取り扱いに従うこと。

（ア）東京都及び運営事務局に関する事象が発生した場合

東京都及び運営事務局側からの案内に従うこと。

別添 1

（イ）参加者及び参加者の所属企業に関する事象が発生した場合
　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。

令和　　年　　月　　日

＜企業同意部分＞

企業名：

企業所在地：

代表者氏名：　　社　印

＜参加者同意部分＞

参加者氏名：　　本人印

＜個人情報の取扱いについて＞
・ご記入いただきました事項は万が一、事故等が起きた場合の対応等に使用させて頂く場合がございます。
・その他において第三者に対し、これらの情報を提供する事はありません。

別添2

機密保持の同意書

私／当社は東京都が主催し、アデコ株式会社（以下、「運営事務局」という。）が受託し運営する「中小企業サイバーセキュリティ社内体制整備事業」（以下、「本事業」という。）に参加するに当たり、下記の守秘義務及び諸条件について誓約し、同意します。

第１　機密情報保持義務

本事業に参加することにより知り得た（１）に係る情報については、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・漏洩することがないよう、厳重に管理すること。

ただし、（２）のいずれかに該当する事項については、この限りでない。

（１）機密情報の対象となる事項

本事業において実施されるセミナー、ワークショップ及び専門家派遣について配布される資料、参加企業とのディスカッション等を通じて触れることとなる項目など、事業を通じ入手する参加企業に関する情報のうち、下記①から⑥に該当する一切の情報について、機密情報の対象とする。

① 参加企業の情報セキュリティ対策に関する情報
② 参加企業の内情に関わる情報
③ 参加企業の一般に公表されていない情報
④ 参加者のプライバシーに関わる情報
⑤ その他、参加企業や参加者に不利益をもたらすと想定される情報
⑥ その他、特に機密情報の対象として運営事務局が指定した情報

（２）機密情報の対象外となる事項

本事業において参加者が知り得た情報のうち、下記のいずれかに該当する事項については、（１）に該当する場合であっても機密情報とみなさないものとする。

① 参加者が知り得た時点で、すでに公知であった情報
② 参加者が知り得た後に、参加者の責によらず公知となった情報
③ 本事業に参加する以前に、正当な方法により、既に参加者が保有していたことを立証し得る情報
④ 本事業とは無関係に、参加企業間の合意形成などの正当な方法により、当該企業間で取り扱いを定めた情報
⑤ 正当な権限を有する第三者から正当な方法により取得した情報

第２　セミナーやワークショップでの撮影、録音、録画の禁止

前項で規定する守秘義務が発生する情報流出を防止するため、事業への参加時には、参加者が個別に録音、録画、写真撮影を行わないこと。

第３　機密情報返還、破棄の義務

第１において規定する情報について、参加企業からの求めに従い運営事務局が情報の返還若しくは破

別添2

棄の指示をした場合は、本事業を通じて取得した機密情報並びに複製物及び複写物等を返還、または指定された方法で破棄すること。

第４　機密保持義務の存続

本同意書に記載された機密情報保持義務は、本事業の支援期間後も存続するものとする。

以上

「中小企業サイバーセキュリティ社内体制整備事業」への参加に当たり、当社及び参加者が、上記機密事項に関わる条件に同意した証として、下記に記名捺印の上、運営事務局に提出します。

令和　　年　　月　　日

＜企業同意部分＞

企業名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

企業所在地：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

代表者氏名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿　社　印

＜参加者同意部分＞

参加者氏名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿　本人印