令和４年度版

運営事務局

令和４年度中小企業サイバーセキュリティ向上支援事業

募集要項

1　事業の目的

近年、IT やAI の技術の進展により、サイバー攻撃の手法も進化し、巧妙になっており、その脅威は自社にとどまらず、サプライチェーンを共有する企業に広く及ぶことになります。

さらに、新型コロナウイルス感染症への対応の一環として、中小企業においてもテレワークの導入が急速に進んでおり、それに伴い、中小企業へのサイバー攻撃の脅威は増大している状況です。

また、多くの中小企業は、知的財産や個人情報を保有していますが、資金や人材不足などの制約があることから、早急に支援が必要な状況となっています。

こうした中、中小企業がサイバー攻撃の脅威から身を守りつつ、テレワーク導入等の業務のデジタル化を推進するためには、中小企業が自社のセキュリティの実態を把握し、必要な対策を講じることが重要です。

そこで、本事業では、こうした中小企業のサイバー攻撃の実態把握やインシデントへの対応支援に加え、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・見直し、情報資産の適切な管理等に向けた専門家による指導助言を行う情報セキュリティマネジメント指導などのサポートを行い、中小企業の自立的なサイバーセキュリティ対策の後押しをいたします。また、こうした取組事例を広く発信することで、都内中小企業全体のサイバーセキュリティ対策に対する意識の向上を目指します。

2　本事業の募集対象

参加申込にあたっては、以下の（１）～（４）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し、中小企業基本法第２条第１項に規定する中小企業及び個人事業主

（２）過去に本事業に参加して支援を受けていない中小企業及び個人事業主

（３）東京都のサイバーセキュリティ対策を目的とする他の補助事業を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

2022 年 4 月 12 日（火）～2022 年 9 月頃

4　募集者数（定員数）

250 社程度　※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

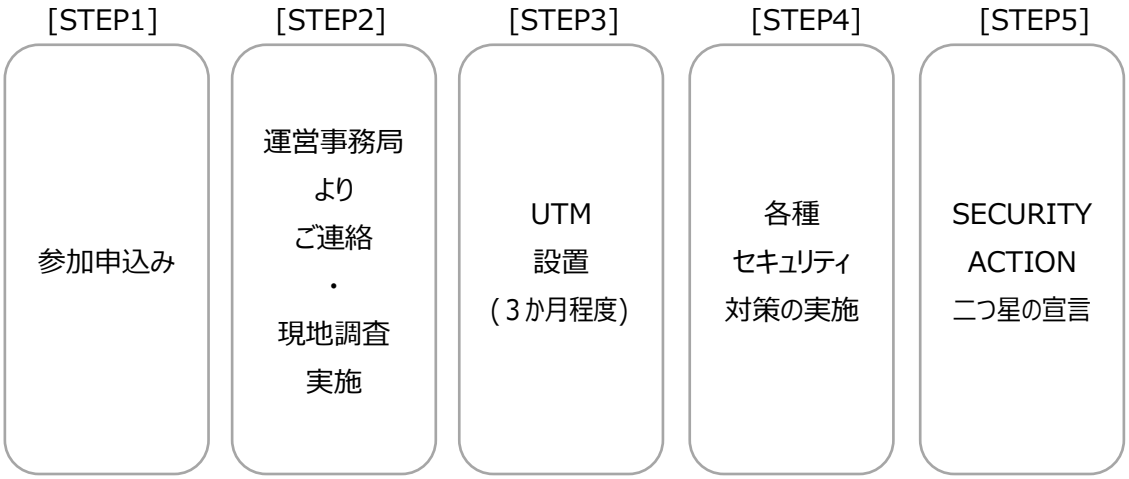
本事業応募ページ

（https://security-kojo.metro.tokyo.lg.jp/application/）より

「参加申込書」「支援開始時アンケート」をダウンロードしていただき、それぞれ必要事項をご記入の上、運営事務局（受託事業者：東日本電信電話株式会社）まで送付ください。

※本募集要項及び参加申込書記載の注意事項をお読みいただき、「東京都中小企業サイバーセキュリティ向上支援事業」の参加申し込みをお願いします。

7　支援の流れ



[STEP1]
申込用紙をダウンロードして、必要事項を入力して運営事務局にメールで送付してください。
本事業応募ページ
（https://security-kojo.metro.tokyo.lg.jp/application/）

[STEP2]
お申込みを確認後、折り返し３営業日以内に運営事務局よりお電話いたします。
その後、実際に運営事務局のスタッフが訪問し、現在のセキュリティ環境を確認して UTM が設置可能か調査します。
調査内容：ネットワークの接続構成、既存の UTM の設置有無、HUB の空きポートの有無等
（UTM は設置工事が必要になります。）

[STEP3]
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。
また、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。

[STEP4]
メール訓練/SMS 訓練・Web 脆弱性診断・サイバー攻撃演習・クラウドセキュリティ対策など、企業の利用環境に応じて必要な対応を実施します。（一部希望制）

[STEP5]
SECURITY ACTION 二つ星の宣言に伴う実施計画書の作成及び宣言までのサポートを実施します。

８　支援内容の詳細

７　支援の流れのSTEP３及びSTEP５が主要事業となります。また、STEP４については、一部希望制の事業となります。

事業内容１　セキュリティ環境の事前診断とセキュリティ対策機器の体験機会の提供

事業詳細Ⅰ　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

（支援の流れSTEP3）主要事業

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「おまかせサイバーみまもり」（UTM）サービスの体験機会（3か月間・無償）を提供いたします。
- その他、おまかせサイバーみまもり（UTM）の利用条件については、受託事業者が定める「おまかせサイバーみまもり利用規約」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。
- おまかせサイバーみまもり（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現場調査を実施いたします。現場調査の結果によっては、おまかせサイバーみまもり（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。
- おまかせサイバーみまもり（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。
- おまかせサイバーみまもり（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。
- おまかせサイバーみまもり（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、おまかせサイバーみまもり（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。
- おまかせサイバーみまもり（UTM）が取得した情報については、9　留意事項の「個人情報の取り扱い」に記載のとおり、活用させていただきます。

事業詳細Ⅱ　セキュリティサポートデスク・駆けつけサポートの提供（UTMの体験期間中）

サポートデスクにてサイバー攻撃に係る各種お困りごとへの相談に対応します。

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か月の無料体験の期間中、24時間対応（休日も含む））

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、駆け付けサポートを実施します。（駆けつけ対応時間9：00～17：00）

事業詳細Ⅲ-1　標的型攻撃メール/SMS訓練（支援の流れSTEP４）

メール訓練：全社実施　/ SMS訓練：希望制

指定いただいたメールアドレス・携帯電話番号宛に「標的型攻撃メール/SMS」を装った訓練用メール/SMSを送付します。

メール/SMSの添付資料等を開いた場合・開かなかった場合どちらの場合でも、本訓練により「職場のセキュリティ意識醸成」に活用することができます。

○標的型攻撃メール訓練に関して

- 本事業の受託事業者により、「標的型攻撃メール訓練」を実施いたします。
- 標的型攻撃メール訓練の実施に当たっては、「標的型攻撃メール訓練提供条件・注意事項」に基づくこととします。
- 標的型攻撃メール訓練は本事業の支援期間中に実施します。詳しい内容は運営事務局から個別にご説明いたします。本事業期間中に、参加企業の皆様からご申告いただいたメールアドレスに予告無く訓練メールを送付いたします。
- 標的型攻撃メール訓練で取得した情報については９　留意事項の「個人情報の取り扱い」に記載のとおり、活用させていただきます。

○標的型攻撃SMS訓練に関して

- 本事業の受託事業者により、「標的型攻撃SMS訓練」を実施いたします。
- SMSを受信する携帯電話（通信費含む）をご用意下さい。
- SMSを受信する携帯電話は090・080・070で始まる電話番号を持ち、音声通話およびデータ通信ができる端末としてください。
- SMSを受信する携帯電話はSSL通信（https）が可能である端末（スマートフォン等）としてください。
- SMSは国外から送付する仕様ですので、携帯電話のSMS拒否設定などを確認し、受信可能な状態としてください。
- 上記を満たしてもSMSが届かない場合がございますが、再送信はいたしません。ご了承ください。
- 標的型攻撃SMS訓練は本事業の支援期間中に実施します。詳しい内容は運営事務局から個別にご説明いたします。本事業期間中に、参加企業の皆様からご申告いただいた電話番号に予告無く訓練SMSを送付いたします。
- 標的型攻撃SMS訓練で取得した情報については９　留意事項の「個人情報の取り扱い」に記載のとおり、活用させていただきます。

事業詳細Ⅲ-2　Web脆弱性診断（支援の流れSTEP４）　希望制

ホームページに情報漏えいやホームページの改ざんにつながる脆弱性が無いか、ホームページが改ざんされて不正なホームページへのリンクが埋め込まれていないか診断し、結果を通知します。

○Web脆弱性診断に関して

- ご希望者を対象に、本事業の支援期間中に受託事業者が提供する「Webセキュリティ診断」を実施いたします。
- Webセキュリティ診断は本事業の支援期間中に実施します。詳しい内容は運営事務局から個別にご説明いたします。
- Webセキュリティ診断で取得した情報については９　留意事項の「個人情報の取り扱い」に記載のとおり、活用させていただきます。

事業詳細Ⅲ-3　サイバーセキュリティ演習の実施（支援の流れSTEP４）　希望制

中小企業経営者や担当者の目線で、サイバー攻撃発生時に適切な判断ができるか、カードゲーム形式で演習を実施します。

○サイバーセキュリティ演習に関して

- ご希望者を対象に、本事業の支援期間中に運営事務局が提供する「サイバーセキュリティ演習」を実施いたします。
- サイバーセキュリティ演習で取得した情報については９　留意事項の「個人情報の取り扱い」に記載のとおり、活用させていただきます。

事業詳細Ⅲ-4　クラウドセキュリティ支援（支援の流れSTEP４）　希望制

テレワーク実施時のクラウドアプリケーション（Microsoft　365、Google Workspace、Box、Dropbox等）に潜む脅威を検知・防御します。

○クラウドセキュリティ支援に関して

- ご希望者を対象に、本事業の支援期間中に受託事業者が提供する「おまかせクラウドアップセキュリティ」を実施いたします。
- おまかせクラウドアップセキュリティの実施に当たっては、受託事業者が定める「おまかせクラウドアップセキュリティ利用規約」に基づくこととします。
- おまかせクラウドアップセキュリティで取得した情報については９　留意事項の「個人情報の取り扱い」に記載のとおり、活用させていただきます。

事業内容２　セキュリティに関する基本方針や規程等の策定を通じて　SECURITY ACTION 二つ星の宣言※2を目指す

事業詳細Ⅰ・Ⅱ　情報セキュリティマネジメント指導・支援の実施（支援の流れSTEP５）主要事業

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。

専門家が参加企業の皆様のもとへお伺いし、1社につき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等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二つ星の宣言を目指していただくためのサポートを行います。

※2　SECURITY ACTION二つ星宣言について
経済産業省の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。
社内で事前にセキュリティ基本方針や規程を準備し、それに沿った行動方針について予め定めておくことで、本当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。

○情報セキュリティマネジメント指導支援に関して

- ご希望者を対象に、本事業の支援期間中に「情報セキュリティマネジメント指導支援」を実施いたします。
- 情報セキュリティマネジメント指導支援で取得した情報については９　留意事項の「個人情報の取り扱い」に記載のとおり、活用させていただきます。

＜情報セキュリティマネジメント指導支援イメージ＞

	1回目	2回目	3回目	4回目
業務の流れ	リスク洗い出し、情報資産管理状況の確認	対策の決定、基本方針の策定・見直し	関連規程の策定・見直しに向けた検討	関連規程、実施計画書のレビュー（指導まとめ）
支援対象企業	・セルフ点検、外部点検により現状のリスクを洗い出し、対策の検討をできる情報が整理された状態になります	・点検結果をもとに具体的な対策と運用に向けた情報セキュリティ基本方針の策定・見直しができる状態になります	・新たな情報セキュリティ基本方針案が決まり、SECURITY ACTION二つ星宣言を実施できる状態になります	・情報セキュリティ基本方針ならびに実施計画書を作成し、本支援後に実施すべきセキュリティ対策が明らかになります

９　留意事項

■応募について

- 中小企業サイバーセキュリティ向上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。
- 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。
- 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。

■アンケートへのご協力のお願い

- セキュリティに関する意識調査（アンケート）を本事業の事前および事後に実施いたします。アンケートへの回答にご協力ください。
- 本事業の支援期間中にも、各支援内容に基づくアンケートを実施する場合がございます。この場合も、アンケートへの回答にご協力ください。

■ヒアリング調査へのご協力のお願い

- 本事業終了後、参加企業の皆様の中から、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。この場合、事前に運営事務局から調査の可否についてご連絡いたします。

■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、本事業のサイトポリシー（個人情報保護方針）（https://security-kojo.metro.tokyo.lg.jp/policy/ ）及び受託事業者のサービスに係るプライバシーポリシー(https://www.ntt-east.co.jp/policy/ ）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。

■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。

10 問い合わせ先

東京都「中小企業サイバーセキュリティ向上支援事業」運営事務局
Mail：cs-tokyo-ml@east.ntt.co.jp
TEL：0800-8005513　（電話受付　平日 9:00～17:30）
URL：https://security-kojo.metro.tokyo.lg.jp
※本事業は東京都より委託を受け、東日本電信電話株式会社が運営しています。