令和6年度中小企業サイバーセキュリティ
基本対策事業

事業説明会

東京都中小企業
サイバーセキュリティ
基本対策事業について

1. 事業概要
2. 支援内容
3. 募集概要

東京都中小企業
サイバーセキュリティ
基本対策事業について

本事業について

中小企業の皆様が自主的にサイバーセキュリティ対策を実施できるように支援する東京都の事業です

情報資産

- ▸企業・機密情報
- ▸顧客情報
- ▸従業員情報

VS

脅　威

- ▸異常アプリ
- ▸不正アクセス
- ▸ウイルス
- ▸スパム

本事業の支援

対　策

各種脅威への直接的な防衛
- ▸セキュリティ機器の設置
- ▸EDRの導入

脅威に対する適切な対応方針
- ▸現状を把握し不安・課題を払拭
- ▸ポリシー・社内規定の整備
- ▸セキュリティ対策の定着化

本事業について

《主な支援》

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

対策①　セキュリティ機器の設置

- **セキュリティ機器（UTM）の導入**に向け、その機器を無償で3ヵ月間体験できる機会の提供

対策②　エンドポイントセキュリティソリューションの導入

- **エンドポイントセキュリティソリューション（EDR）の導入**に向け、そのシステムを無償で3ヵ月間体験できる機会の提供

対策③　情報セキュリティマネジメント指導

- 情報セキュリティに対する不安や課題を払拭すべく、サイバーセキュリティに関する**基本方針や社内規定の策定**等のサポートにより、**SECURITY ACTION二つ星宣言を目指す**支援の提供

《支援対象》

（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

本事業について

《支援対象》

（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となるが、異なる支援内容の場合、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

（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

UTMとは

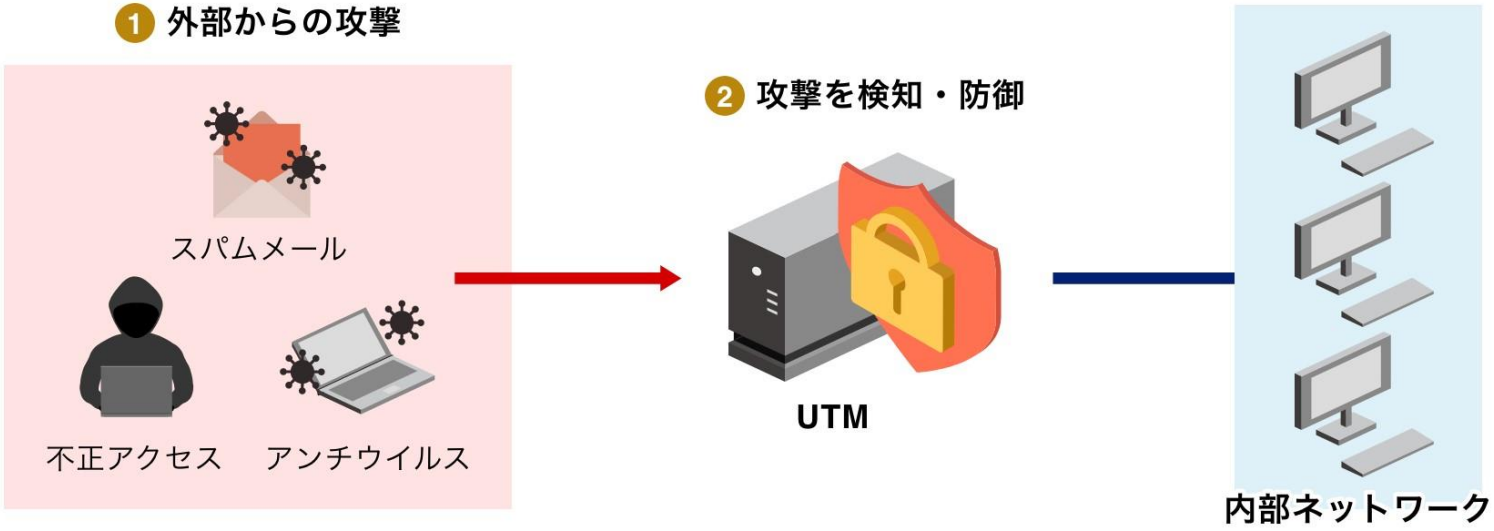
UTM（Unified Threat Management ： 統合脅威管理）

▶ 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

なぜUTMなのか？

ウイルス対策ソフトやファイヤウォールなどでは、ウイルスを防げても、不正アクセスや侵入は防げない

▶ **UTMは、1台でウイルスをはじめ、スパム攻撃や異常アプリ、不正アクセスまで、様々な脅威に有効！**



UTMを社内ネットワークの出入口に設置することで集中的なネットワーク管理 ▶ 各種脅威による不正な通信を検知・ブロック

EDRとは

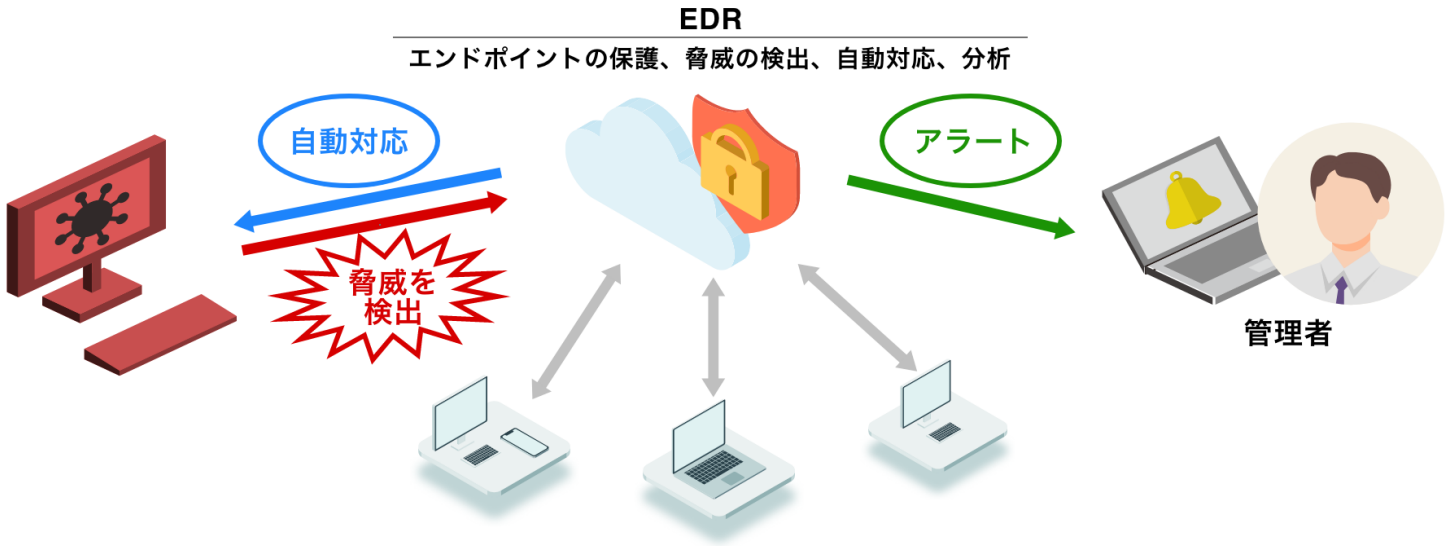
EDR（Endpoint Detection and Response ： デバイス検知と対応）

▶エンドポイント端末（PCやスマートフォンなどの接続デバイス）を監視し、不正侵入を検知して対処するシステム

なぜEDRなのか？

高度に巧妙化するサイバー攻撃は、従来型のアンチウイルスやファイアウォールでは防護できない

▶ **EDRは、攻撃者が侵入した場合を想定し、検知・対応して被害を防ぐことが目的！**



EDRはサイバー攻撃を検知し、マルウェア駆除や被害の最小化、迅速な復旧を支援する ▶ リスクと負担を軽減

SECURITY ACTION 二つ星宣言とは

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

SECURITY ACTION 一つ星宣言

▸「情報セキュリティ5か条※」に取組むことを宣言

SECURITY ACTION 二つ星宣言

▸「5分でできる！情報セキュリティ自社診断※」で自社の状況を把握したうえで、情報セキュリティポリシー(基本方針)を定め、外部に公開し、宣言

※中小企業の情報セキュリティ対策ガイドライン付録 → 中小企業 情報セキュリティ対策ガイドライン で検索

Point 1

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、
実際に攻撃を受けた際に適切な対応を取ることができる

Point 2

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る

東京都事業における本事業の位置づけ

レベル１	レベル２	レベル３	レベル３以降
普及・啓発	**機器・規定整備**	**社内体制整備**	**インシデント対応力強化**
中小企業サイバーセキュリティ **啓発事業** セキュリティ対策について まだ考えていない中小企業へ 必要性を認知いただき、 セキュリティ診断により 必要な支援をご案内します。	中小企業サイバーセキュリティ **基本対策事業** セキュリティ対策をこれから 始める中小企業に対し、 機器の導入や規定策定など 一歩目を踏み出す支援を 行います。	中小企業サイバーセキュリティ **社内体制整備事業** セキュリティ対策を自走 出来ない中小企業を対象に、 継続的なセキュリティ 対策が出来る人材を 育成します。	中小企業サイバーセキュリティ **特別支援事業** サイバー攻撃を受けたときの 的確な対応方法や事業の 復旧までを考慮した セキュリティ対策を 支援します。

情報発信

中小企業サイバーセキュリティ
フォローアップ事業

サイバーセキュリティに関する幅広い情報のコンテンツを、成熟度に応じて提供します。

東京都中小企業
サイバーセキュリティ
基本対策事業について

支援の流れ

1 申込み

Webより参加申込フォームに
必要事項を入力

参加要件・同意についての確認

2 事前診断

現在のセキュリティ環境を確認

【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
・UTMの設置有無
・EDR導入の有無
・アンチウィルスソフトの導入の有無
・EDRのユーザー数の確認
・UTMのデバイス数の確認
・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は設置工事が必要です

3 支 援

セキュリティ環境に応じて
支援コースを確定・支援実施

- 支援①　UTM機器設置コース
- 支援②　EDR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 事後サポート

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

※支援③のみにご参加の場合は事前診断はございません。
お申込内容確認後、初回訪問日（セキュリティマネジメント指導日）について専門家からお電話させていただきます。

支援の流れ

1 申込み

Webより参加申込フォームに
必要事項を入力

参加要件・同意についての確認

2 事前診断

現在のセキュリティ環境を確認

【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の設置有無
・既存のEDR導入の有無
・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は設置工事が必要です

3 支 援

**セキュリティ環境に応じて
支援①、支援②、支援③を実施**

- **支援①　UTM機器設置コース**
- **支援②　EDR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 事後サポート

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

支援概要

支援①UTM機器設置コース

・UTM機器設置

▸UTMを3か月間無料体験
▸期間中、サポートデスクによる支援を実施

支援②EDR導入コース

・EDR導入

▸EDRを3か月間無料体験
▸期間中、サポートデスクによる支援を実施

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

▸専門家によるオンサイトでの個別指導・支援（計4回）
-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の策定
-基本方針に基づいた実施計画書を作成し、継続したセキュリティ対策を目指す
-SECURITY ACTION二つ星宣言実施をサポート

支援詳細

支援①UTM機器設置コース

・UTM機器設置

▸UTMを3か月間無料体験
▸期間中、サポートデスクによる支援を実施

支援②EDR導入コース

・EDR導入

▸EDRを3か月間無料体験
▸ 期間中、サポートデスクによる支援を実施

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

▸専門家によるオンサイトでの個別指導・支援(計4回)
-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の策定
-基本方針に基づいた実施計画書を作成し、継続したセキュリティ対策を目指す
-SECURITY ACTION二つ星宣言実施をサポート

支援詳細　支援①UTM機器設置コース

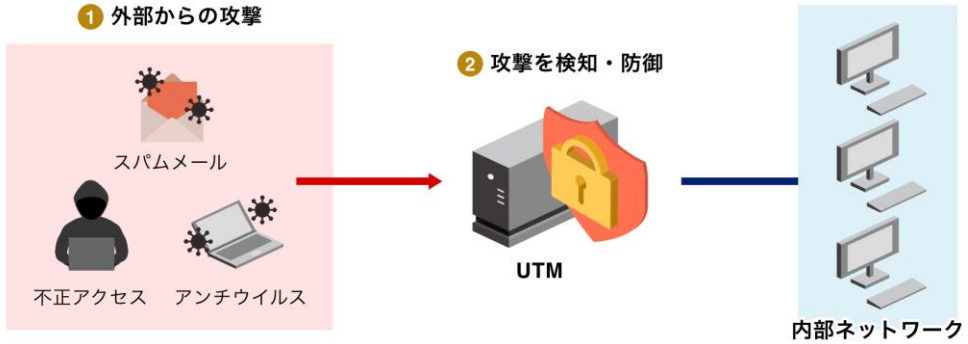
◆UTM機器設置

Point 1

UTMの3か月間無料体験

▸現状のセキュリティ環境を専門家がチェック

▸UTMを設置して各種サイバー攻撃の状況を確認でき、
社内ネットワークの出入り口対策の効果を実感



※UTM設置には工事が必要です
専門家の事前診断の結果により事業参加確定となります

Point 2

体験期間中、サポートデスクによる支援を実施

▸UTM利用者向けのサポートデスクの機能も無料で体験

※このコースで利用するUTM機器は、Check Point社製“Quantum Sparkアプライアンス シリーズ”です。

支援詳細

支援①UTM機器設置コース

・UTM機器設置

▸UTMを3か月間無料体験
▸期間中、サポートデスクによる支援を実施

支援②EDR導入コース

・EDR導入

▸EDRを3か月間無料体験
▸期間中、サポートデスクによる支援を実施

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

▸専門家によるオンサイトでの個別指導・支援（計4回）
-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の策定
-基本方針に基づいた実施計画書を作成し、継続したセキュリティ対策を目指す
-SECURITY ACTION二つ星宣言実施をサポート

支援詳細　支援②EDR導入コース

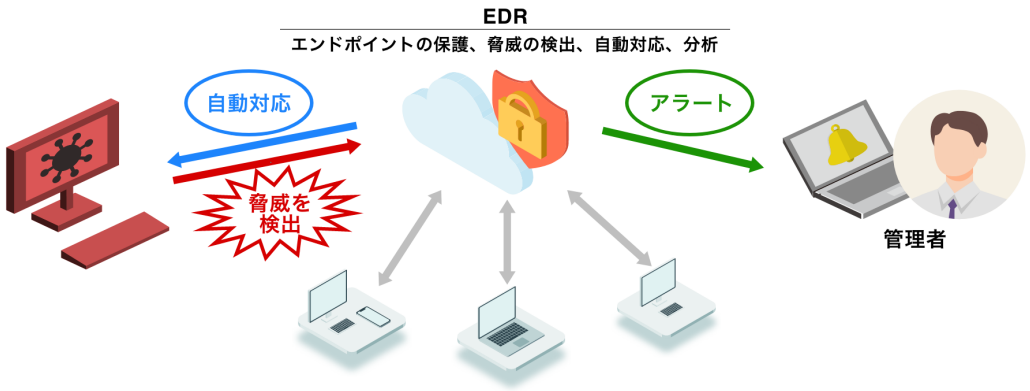
◆EDR導入

Point 1

EDRの3か月間無料体験

▸現状のセキュリティ環境を専門家がチェック

▸EDRを導入して各種サイバー攻撃の検出･分析、自動修復状況を確認でき、 エンドポイントセキュリティ対策の効果を実感



※EDRの導入は最大300ユーザー／社です。
既にEDR製品導入済みの場合はご参加いただけません。
専門家の事前診断の結果により事業参加確定となります。

Point 2

体験期間中、サポートデスクによる支援を実施

▸EDR利用者向けのサポートデスクの機能も無料で体験

※このコースで利用するEDR製品は“Microsoft Defender for Business”です。

支援詳細　支援③情報セキュリティマネジメントコース

支援①UTM機器設置コース

・UTM機器設置

▸UTMを3か月間無料体験
▸期間中、サポートデスクによる支援を実施

支援②EDR導入コース

・EDR導入

▸EDRを3か月間無料体験
▸ 期間中、サポートデスクによる支援を実施

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

▸専門家によるオンサイトでの個別指導・支援（計4回）
-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の策定
-基本方針に基づいた実施計画書を作成し、継続したセキュリティ対策を目指す
-SECURITY ACTION二つ星宣言実施をサポート

支援詳細　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

Point 1

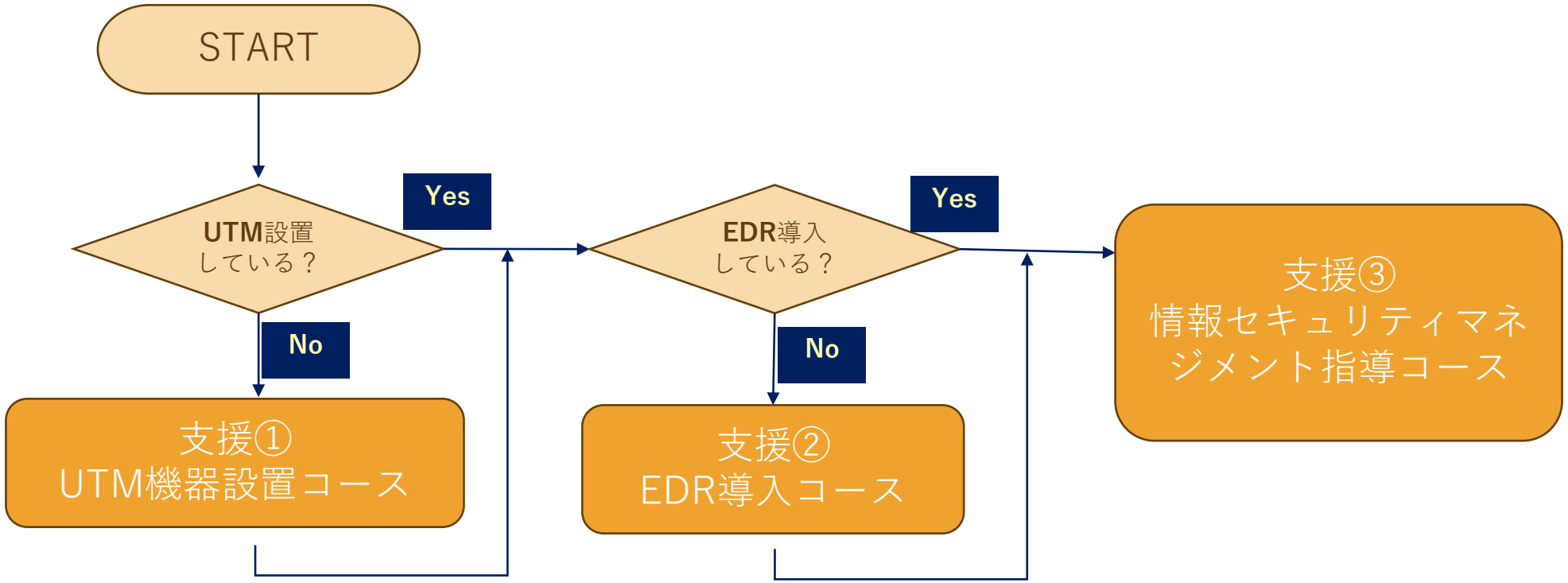
サイバーセキュリティに関する基本方針や
規程等の策定等に向けた、
専門家による個別指導・支援（計4回）

Point 2

SECURITY ACTION二つ星宣言の達成を
目指せるようサポート

支援内容	1回目	2回目	3回目	4回目
支援の流れ	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	関連規定の策定・ 見直しに向けた検討	関連規定、実施計画書のレビュー（指導まとめ）
具体的支援	自社診断ツール兼ヒアリングシートを作成し、現在のレベルと問題点を把握。 情報資産管理台帳を用いて管理すべき情報資産とその管理状況も把握。	基本方針とその作成を補助する情報セキュリティ基本方針策定雛形ツールや、関連規定作成のための情報セキュリティ関連規定雛形ツールについて説明し、それらを用いた検討の実施。 また実施計画を作成する課題の具体化と、SECURITY ACTION二つ星自己宣言の準備。	診断結果FBシートを用いた具体的な対策内容と優先順位を検討。情報セキュリティ関連規定雛形ツールでの基本方針策定の確認と実施計画書作成の支援。SECURITY ACTION二つ星自己宣言実施への支援。	策定された関連規定や実施計画書の作成状況の確認・レビューを実施。 自社診断ツール兼ヒアリングシートでの再診断を行い、今後のの継続的な取組に向け支援。

支援コース選択　＜基準＞



複数の支援コースを選択、参加することが可能です。

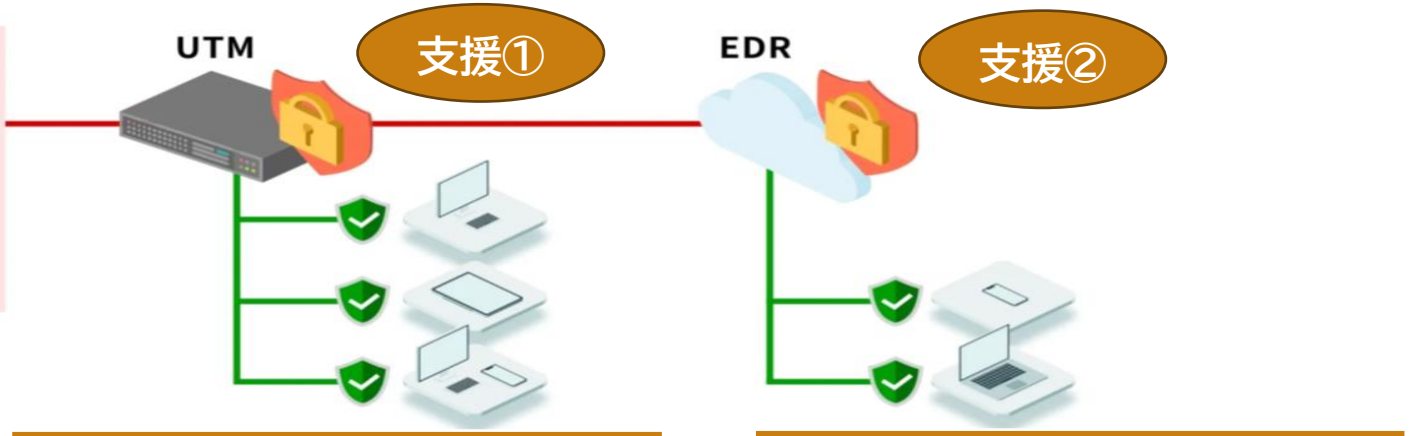
支援の組み合わせにより、期間が異なります。
いずれのコースも無償です。

※セキュリティ環境や機器設置箇所の状況により、必ずしも上記のとおりになるとは限りません。
　支援①、支援②は“事前診断”の結果により支援コース確定となります。

支援コース選択 ＜支援①＋支援②＞

UTM／EDRのどちらか一つでは巧妙化するセキュリティ攻撃を防ぐことは難しくなっているため、より強力な対策を考えると、両方の利用が有効

UTM・EDR両方の採用でより強固なセキュリティ対策を実施



UTM機能（24h365日）

- アンチウィルス・アンチスパム・IPS・ファイヤーウォール アンチボット・URLフィルタリング・アプリケーション制御

EDR機能（24h365日）

- 異常検出・調査・分析、メール通知、自動修復

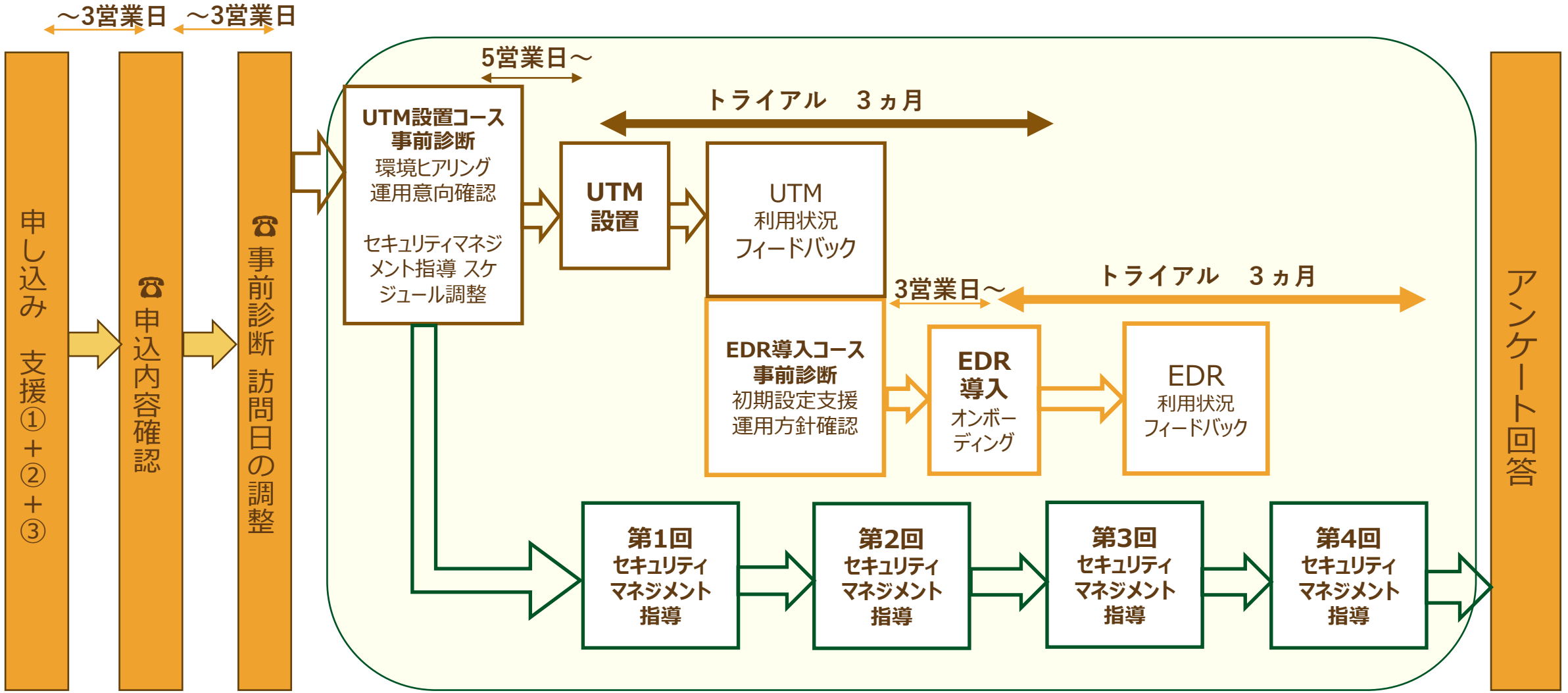
インシデント発生時の対応

1．リアルタイム通知	2．有効な対応	3．報告書の作成
UTM 1.異常な通信を検知 2.検知ログ送信 3.企業担当者へ連絡	**UTM対応** ・通信を遮断	**SE対応** ・インシデント発生端末の探索支援 ・マルウェアの確認及び駆除 ・端末復旧作業支援 ・報告書作成（原因、対処方法）	**SEの取りまとめ** ・発生日時 ・インシデント内容 ・インシデントの原因 ・対応方法 ・対応の効果
EDR 1.異常な通信を検知・分析・処置 2.検知ログ送信 3.企業担当者へ連絡	**EDR対応** ・感染したデバイス側で検知・分析・通知・復旧		

迅速 → 有効対応 → 対応後

支援コース選択　＜支援①＋②＋③の流れ＞

前提条件により全ての支援を受けることも可能です。その際、訪問回数、各回の時間は調整となります。



東京都中小企業
サイバーセキュリティ
基本対策事業について

1 事業概要

2 支援内容

3 募集概要

募集概要

申込締切	支援①UTM機器設置コース	令和6年11月29日(金)※まで
	支援②EDR導入コース	令和6年11月29日(金)※まで
	支援③情報セキュリティマネジメント指導コース	令和6年11月29日(金)※まで
対象企業	東京都内に主たる事業所を有し、 サイバーセキュリティ対策への意欲を持つ中小企業	
募集数	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
支援期間	3ヵ月程度(選択コースにより変更有)	
参加費用	無料	

※事務局からの確認のお電話はお申込みから3営業日以内にいたします。

申込みにおける注意事項

1 規定・遵守事項への同意

お申込み後、運営事務局から3営業日以内に運営事務局から電話でご連絡いたします。
ご連絡の際に、参加に当たっての規定や遵守事項への同意確認をさせていただきます。
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。
事務局よりお電話が行きます（電話番号：050ー4560－3824）

2 アンケートへのご協力

セキュリティに関する**意識調査（アンケート）を支援終了後に実施**いたしますので、ご回答への協力を
お願いします。
次年度（令和7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。その際にはご協力いただきますよう
お願いします。

3 ヒアリング調査（成果事例）へのご協力

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。その際にはご協力いただきますようお願いします。

申込み・問い合わせ

1 事業申込

事業HP
https://kihontaisaku.metro.tokyo.lg.jp

2 問い合わせ

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

050-4560-3824
相談窓口対応時間　平日9:00～17:00

ade.jp.kihontaisaku@jp.adecco.com

事業HP　問合せフォームよりお問い合わせください
https://kihontaisaku.metro.tokyo.lg.jp

東京都中小企業
サイバーセキュリティ
基本対策事業

皆様のお申込みを
お待ちしております