経済産業省の施策　独立行政法人情報処理推進機構(IPA)からの受託事業（受託者：大阪商工会議所）

「サプライチェーン強化に向けたセキュリティ対策評価制度」制度の説明および実証参加企業の募集　説明会

★3 取得を目指し専門家の伴走支援を無償で受けることを希望する中小企業等を全国で 80 社募集！

サイバー攻撃は怖いがお金をかけられない！
委託元から★取得を依頼されたが、どうすればいいの？
要求項目の意味や基準も分からず、自力では無理！

- 中小企業がサイバー攻撃被害に遭うと、ウイルス拡散や供給停止により、委託元やサプライチェーンにご迷惑をおかけする場合もあります。対策は、何をどこまでやり、その対策実施状況をいかに他社にご理解頂くか？
- 経済産業省・IPA は、中小企業のセキュリティの内容や程度を業種横断的に★の数で評価する「サプライチェーン強化に向けたセキュリティ対策評価制度(★3・★4)」を新設し 2027 年 3 月から運用を開始します。
- 中小企業の★取得を支援する国の施策が「サイバーセキュリティお助け隊サービス(新類型)」。中小企業が独力で★取得するのは困難と予想される事をふまえ、専門家派遣等により中期的伴走支援を行うサービスです。
- ★取得支援サービスを、IPA から受託したサービス提供事業者(大阪商工会議所)が試行的に提供し商品化を検討する実証事業が 2026 年 10 月頃から最大約 1 年間、経済産業省･IPA により行われます。実証参加の中小企業は★取得に向けた専門家支援(一般的に相当な金額を要する場合が多い)を無償で受けることができます。

経済産業省 Ministry of Economy, Trade and Industry
独立行政法人 情報処理推進機構 Innovation Platform Agency, Japan

サイバーセキュリティお助け隊サービス(新類型)実証
委託 → 大阪商工会議所(サービス提供事業者)
専門家(全国の情報処理安全確保支援士)

各地商工会議所･金融機関(広報･説明会)
㋑診断･助言のうえ改善計画書作成
㋺コンサルティング（訪問 or オンライン）
㋩IT ツールおよびその導入支援

全国の★3 取得希望中小企業等（参加無料）

説明会

①中小企業でのサイバー攻撃の手口と被害（大阪商工会議所 経営情報センター 次長 野田幹稀・副主任 田中翔子）
②本制度と実証の概説（大阪商工会議所 経営情報センター 次長 野田幹稀・副主任 田中翔子）
③要求項目･評価基準の詳説・㋑㋺㋩の支援の方法（情報処理安全確保支援士 又は 大阪商工会議所）

お申込→

10/1(木)	1000~1130	札幌商工会議所 7 階第 5 会議室(札幌市中央区北 1 条西 2 丁目 北海道経済センター)	情報処理安全確保支援士 笹川伸之氏 (合同会社オークニック 代表社員)
10/26(月)	1400~1600	仙台商工会議所 4 階小会議室(仙台市青葉区本町 2-16-12)	情報処理安全確保支援士 後藤武志氏 (GIU コンサルティングオフィス 代表)
10/29 (木)	1400~1600	前橋商工会議所 3 階アネモネ(前橋市日吉町 1-8-1)	情報処理安全確保支援士 内山貢悦氏 (ふくとみ経営研究所 代表)
9/25(金)	1400~1600	高崎商工会議所 2 階第 2 会議室(高崎市問屋町 2 丁目 7 番地 8)	情報処理安全確保支援士 山本哲也氏 (ミニティ㈱ 代表取締役)
11/20(金)	1400~1600	大和商工会議所 2 階第 3 会議室(神奈川県大和市中央 5-1-4)	情報処理安全確保支援士 大久保次郎氏 (ディエスエル㈱ 代表取締役)
10/19 (月)	1400~1600	金沢商工会議所 2 階研修室 1C(金沢市尾山町 9-13)	情報処理安全確保支援士 野澤秀彰氏 (のざわでんき 代表)
10/28(水)	1400~1600	松本商工会議所 3 階 303 会議室(松本市中央 1-23-1)	情報処理安全確保支援士 西村元男氏 (デジタルデマンド㈱ 代表取締役)
10/29(木)	1400~1600	刈谷商工会議所 2 階会議室(愛知県刈谷市新栄町 3-26)	情報処理安全確保支援士 髙木有紀恵氏 (Cerulean Digital 代表)
11/12(木)	1400~1600	橿原商工会議所 4 階会議室 A(奈良県橿原市久米町 652-2)	情報処理安全確保支援士 野村陽子氏 (㈱ブルーオーキッドコンサルティング 取締役)
9/24(木)	1000~1200	大阪信用金庫 3 階中会議室 1(大阪市天王寺区上本町 8-9-14)	情報処理安全確保支援士 吉岡省吾氏 (ワイズ情報技術サービス㈱ 代表取締役)
9/25(金)	1400~1600	大阪シティ信用金庫 梅田支店 5 階 ソア（大阪市北区豊崎 5 丁目 7-12）	情報処理安全確保支援士 浦中究氏 (㈱DigitalAge 代表取締役)
9/28(月)･10/13(火)	0930~1130	大阪商工会議所 2 階経営情報センター会議室(大阪市中央区本町橋 2-8)	大阪商工会議所 経営情報センター
10/28(水)	1500~1700	神戸商工会議所 3 階会議室(神戸市中央区港島中町 6 丁目 1 番地)	情報処理安全確保支援士 原一矢氏 (ビットフロー・マネジメント㈱ 代表取締役)
10/1(木)	1400~1600	岡山商工会議所 4 階 404 会議室(岡山市北区厚生町 3-1-15)	情報処理安全確保支援士 大久保茂人氏 (プラスエス 代表)
10/2(金)	1400~1600	米子商工会議所 7 階大会議室 A(鳥取県米子市加茂町 2 丁目 204)	
11/17(火)	1400~1600	新居浜商工会議所 3 階研修室(愛媛県新居浜市一宮町二丁目 4-8)	情報処理安全確保支援士 藤内伸二氏 (合同会社四国サート 代表)
10/15(木)	1330~1500	大分商工会議所 5 階 A 会議室(大分市金池町 2 丁目 3 番 4 号 九電大分ビル)	情報処理安全確保支援士 清水太氏 (ルーラルウェイ合同会社 代表)
10/26(月)	1400~1600	熊本商工会議所 別館 3 階会議室(熊本市中央区横紺屋町 10)	情報処理安全確保支援士 橋爪兼続氏 (ライトハウスコンサルタント 代表)
10/8(木)	1330~1530	那覇商工会議所 2 階会議室(那覇市久米 2-2-10 中小企業振興会館)	情報処理安全確保支援士 屋良尚平氏 (合同会社 Up70 代表)
10/9(金)	1330~1530	浦添商工会議所 3 階小研修室(浦添市勢理客 4-13-1 浦添市産業振興センター)	
9/29(火)	1500~1630	オンライン(全国対象)	大阪商工会議所 経営情報センター
10/21(水)	1000~1130	※上記説明会に地理的・時間的・定員的にご参加頂けない方	

大阪商工会議所 経営情報センター（田中･野田）050-7105-6004 scs-otasuketai@osaka.cci.or.jp

共催：札幌・仙台・高崎・前橋・大和・松本・金沢・刈谷・橿原・神戸・岡山・米子・新居浜・熊本・大分・那覇・浦添商工会議所・大阪信用金庫・大阪シティ信用金庫　【刈谷】NTT 西日本・(公社)刈谷法人会刈谷支部とも共催

制度について

★3	**最低限実装すべきセキュリティ対策**として、**基礎的な組織的対策**と**システム防御策**…26要求事項81評価基準(全て満たす必要あり)…専門家確認付き自己評価（１年毎に更新）
★4	**標準的に目指すべきセキュリティ対策**として、**組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等**包括的な対策…43要求事項153評価基準(全て満たす必要あり)…第三者評価（３年に１回更新）

大分類	★3	★4
ガバナンスの整備	**企業として最低限のリスク管理体制の構築** ・自社のセキュリティ担当の明確化 [No.1-2-1] ・セキュリティ対応方針の策定 [No.1-3-1]	**継続的改善に資するリスク管理体制の構築** ・定期的な経営層への報告、不備の是正等 [No.1-4-1]
取引先管理	**取引先に課す最低限のルール明確化** ・他社との機密情報の取扱い明確化 [No.2-1-2] ・接続している外部情報サービスの把握 [No.3-1-3]	**取引先の管理・把握及び取引先との役割・責任の明確化** ・機密情報共有先の把握 [No.2-1-1] ・重要な取引先等の対策状況把握 [No.2-1-3] ・インシデント発生時の他社との役割等の明確化 [No.2-1-4]
リスクの特定	**自社IT基盤や資産の現状把握** ・情報資産やネットワークの把握 [No.3-1-1,3-1-2] ・外部情報サービスの管理 [No.3-1-3]	**脆弱性など最新状況の把握と反映** ・脆弱性管理体制、管理プロセスの明確化 [No.3-2-1]
攻撃等の防御	**不正アクセスに対する基礎的な防御** ・ID管理手続、アクセス権限の設定[No.4-1-1,4-1-2] ・パスワードの安全な設定及び管理 [No.4-1-4,4-1-5] ・内外ネットワーク境界の分離・保護 [No.4-5-1] **端末やサーバーの基礎的な保護** ・適時のアップデート適用、不要ソフトウェアの削除[No.4-4-1,4-4-4] ・端末等へのマルウェア対策 [No.4-4-1,4-4-4]	**多層防御による侵入リスクの低減** ・重要な保管データの暗号化 [No.4-3-1,4-3-2] ・ログの収集・定期的な分析の実施 [No.4-4-3] ・社内システムにおける適切なネットワーク分離 [No.4-5-1] ・社外への不正通信の遮断(出口対策) [No.4-5-2]
攻撃等の検知	**ネットワーク上の基礎的な監視等** ・ネットワーク接続・データの監視[No.5-1-1]	**迅速な異常の検知** ・情報機器等の状態、挙動の監視・対応や分析[No.5-1-1,5-1-2]
インシデントへの対応	**インシデント発生に備えた対応手順の整備** ・インシデント対応手順の作成 [No.6-1-1]	*大分類「インシデントへの対応」において、★４での追加項目はなし
インシデントからの復旧	**インシデント発生から復旧するための対策の整備** ・インシデント発生から復旧するための対策の整備[No.7-1-1]	**インシデントからの復旧手順等の整備** ・復旧ポイント、復旧時間を満たす手順等の整備[No.7-1-1]

取引先と自社との ビジネス又はシステム上の関係を把握すること。	★3	2-1-1-1	・自社以外の組織(顧客・子会社・関係会社・クラウドサービス提供者を含む取引先)が管理・提供し、自社の資産が接続しているシステムを把握するための仕組みを整備すること。
		2-1-1-2	・年1回以上の頻度でNo.2-1-1-1において把握した情報の内容を点検すること。
自社の機密情報の取扱い方法を、共有先との間で明確にすること。	★3	2-1-2-1	・自社の機密情報を共有する予会社又は取引先との間で、業務開始前に機密情報の取扱いについて、以下の事項を取り決めること。 - 機密情報の定義 - 機密情報の利用制限、保管方法、複製可否及び第三者への提供可否 - 機密情報の返還又は廃棄
セキュリティインシデント発生時の他社との役割及び責任を明	★3	2-1-4-1	・自社の機密情報を共有する予会社又は取引先との間で、セキュリティインシデント発生時の自社と予会社又は取引先の役割及び責任を定めること。
情報機器、OS及びソフトウェアに関する情報を把握すること。	★3	3-1-1-1	・パソコン及びシンクライアントの製造元、OS及び台数を把握するための仕組みを整備すること。
		3-1-1-2	・サーバ、仮想サーバ及びハイパーバイザの製造元、OS及び台数を把握するための仕組みを整備すること。
		3-1-1-3	・情報機器、OS及びソフトウェアについて、導入、設置、ネットワーク接続及びセキュリティパッチ適用のルールを含む管理ルールを定めること。
		3-1-1-4	・年1回以上の頻度でNo.3-1-1-3で定めた管理ルールの遵守状況について点検すること。
ネットワークに関する情報を把握するための仕組みを整備すること。	★3	3-1-2-1	・ネットワークを把握するための仕組みを整備すること。その際、把握すべき情報の中に各ネットワークの所在地及び用途に関する情報を含めること。
		3-1-2-2	・ネットワーク機器を把握するための仕組みを整備すること。その際、把握すべき情報の中に各機器の製造元、モデル及び保守事業者に関する情報を含めること。
自社の機密情報を扱う外部情報サービスを管理すること。	★3	3-1-3-1	・外部情報サービスを利用する際のセキュリティ要件を定めたうえで、外部情報サービスの利用時に当該要件を満たしているかサービス内容を確認すること。
		3-1-3-2	・外部情報サービスの提供事業者と機密情報の取扱いについて合意を取り交わすこと。
機密区分に応じた情報の管理ルールを定め、それに基づく管理を行うこと。	★3	3-1-4-1	・自社の保有する情報を対象に、以下の内容を含む管理ルールを定めること。 - 機密の特定 - 機密区分のレベル判定及び表示 - 区分に応じた取扱方法 - 取扱エリアの区分及び制限
		3-1-4-2	・年1回以上の頻度でNo.3-1-4-1で定めた管理ルールの内容について点検すること。
		3-1-4-3	・事業と機密情報対応に当該情報ごとの管理責名、部署名、保管場所、保管期限、開示先及び管理者の連絡先を把握するための仕組みを整備すること。

実証参加企業等　募集要項

1．実証の目的・概要

①(独)情報処理推進機構(以下 IPA)から本実証事業を受託したサービス提供事業者(大阪商工会議所)が、中小企業の皆様にセキュリティサービスを提供し、「サイバーセキュリティお助け隊サービス」（新類型）として必要な要件の検証を行うものです。サービス提供事業者(大阪商工会議所)は、SCS 評価制度★3 取得のためのサービスを試行的に提供します（本実証では、大阪商工会議所は★4 は対象としません）。その活用状況や結果を踏まえ、中小企業の皆様にとって導入しやすいサービスであることを担保するため、品質要件や価格要件などについて検討を行います。

②中小企業の皆様には、サービス提供事業者から★取得のための支援サービスを受けていただくことで、サイバーセキュリティお助け隊サービス（新類型）の制度創設に向けた検討にご協力頂きます。具体的には、制度創設に向けた意見の提出や、セキュリティ対策に関する情報提供（不審な通信を検知した際の関連情報の提供を含む）へのご協力をお願いします。実証期間は、2026 年 10 月から 2027 年 9 月までの最大 12 か月（最短 3 か月）です。

2．参加対象・参加要件

①IPA が別途定義する「本事業における中小企業等」に該当しており、本制度の趣旨･要求項目につき一定の理解があること。

②大阪商工会議所(以下、大商)が派遣する情報処理安全確保支援士(国家資格。この分野の専門家。以下、セキスペ)の支援を受けつつ★取得(未達事項の達成)に向け、計画的に(可能な限り短期に。途中辞退することなく)組織的･人的対策、IT ツール等導入による対策向上を行う意志と体制を有していること(担当者を最低 1 名確保でき、経営層･社員の協力が得られること。担当者は兼任でもよく、ICT やセキュリティの専門知識は不問ですが最低限の知識があること)

③経済産業省･IPA･大商･セキスペ等によるアンケート調査、ヒアリングに協力頂けること。また「サイバー対処能力強化法」に基づく国による「集団的防御プラットフォームの構築」の要請から、実証で得られた、貴社名やメールアドレス等の個人情報を含むアラート情報やインシデントレポート等が、本実証参加企業様への事前の連絡なく（その受信とほぼ同タイミングで）経済産業省・IPA およびその委託事業者に提供される可能性がある旨をご了解頂けること。

④上記③の「アラート情報やインシデントレポート」については、★3 の枢要かつ達成難度の高い要求事項である「攻撃等の検知(5-1-1-1、5-1-1-2、5-1-1-3)」を満たすことが前提となるため、実証期間中(ならびに★取得後)、全実証参加企業は、UTM(多機能防御装置)等による「検知」「防御」「遠隔監視」「アラート発報」「アラート分析」「サイバーインシデント発生時の対応支援」を受けられる IT ツールやサービスが必要となります。これ以外にも達成すべき要求項目は多々ありますが、とりわけこの部分の難易度が高いため、この部分に対し、全実証参加企業を対象として、大商がかねてより提供しており、上記全てを一体的に満たすことの出来る「商工会議所サイバーセキュリティお助け隊サービス(IPA 登録 2020-001)」を実証期間中(2026 年 10 月～2027 年 9 月まで)、無償で提供します。またバックアップおよび遠隔地バックアップを実現し、4-3-4-1、4-3-4-2 を満たすため、大商が選定するバックアップソフトおよびバックアップ格納領域用クラウドストレージ(遠隔地バックアップ)を無償で提供します。

⑤実証参加企業は、上記サービスを受けて頂くことが参加要件となります。但し、既に他社提供のツールやサービスを導入しており、かつ上記要求項目を満たしている場合はこの限りではありませんが、この場合でも、上記③の「アラート情報やインシデントレポート(貴社名・個人情報を含む）」の IPA およびその委託事業者への提供は、参加要件となりますので、ご利用先の IT ベンダ様等に提供およびその方法につきご相談願います。

⑥「商工会議所サイバーセキュリティお助け隊サービス」は IT が苦手な中小企業向けに開発された、導入･運用の負荷の低いサービスであり、レンタル UTM（実証期間中のみ国からの支給により無償）はブリッジモードのため設置･設定が容易でネットワーク構成の変更が原則不要。障害発生等の確率は僅少です。

⑦実証で提供する支援は、既存の有償サービスではなく、国の産業政策戦略に基づく“商品化に向けた大商による実地検証のプロセスそのもの(試行錯誤)”であることをご理解頂き、大商･セキスペの支援(役務提供等)の内容･水準(能力)･段取り･対応などがご所望の内容･レベルではない可能性がある点を理解頂けること

⑧本実証参加により損害等(サイバー攻撃、情報の流出･損壊等の被害、ネットワーク障害、機会損失等を含む)を受けた場合、および実証による支援の結果、★取得の水準まで達しなかった場合でも、経済産業省、IPA、IPA 委託先、大商、大商再委託先、セキスペは故意又は重過失による場合を除き、責任を負いかねます(実証参加により自動的に★が付与されるわけではありません。セキスペは原則として所謂“丸投げ”を受けません)ので、その点をご理解頂けること（貴社の機密情報･個人情報の取扱いについては別途、申込サイトをご参照下さい）

3．選考の方法と基準

①実証に参加頂ける企業は、申込順を考慮しつつも、地域的バランス、業種的バランス、従業員規模、現状の対策状況、サプライチェーンにおける立ち位置、各地域でのセキスペの対応力などを総合的に勘案し決定させて頂きます。

②募集枠は全国で 80 社。選考(当落)の経緯･理由は一切開示致しません。実証参加企業に選定された場合でも、セキスペの対応余力･地理的条件･予算執行状況等により、支援を受けられない場合、十分な支援を受けられない場合があります。

4．実証参加企業と情報処理安全確保支援士との関係性

①実証においてセキスペは、実証参加企業への寄り添いの姿勢に基づき、守秘義務、専門知識を以て、主に以下の支援を無償で行います。
(A)「診断・助言サービス（課題の可視化）」(現状アセスメントと支援のロードマップ＆スケジュール作成)
(B)「IT ツールの導入」(未達事項を満たし得る IT ツール又はその代替手段の導入・運用支援)
(C)「IT ツール以外の支援サービス」(★取得を目指してのコンサルティング、各種の規定や手順書等の作成・改善等の支援、社員研修など)
(D)★取得申請手続きの支援(実証参加企業が自己評価結果を記入した★取得申請書を確認･評価し、署名・提出支援。国への申請・登録手数料：今回は免除)

②セキスペと実証参加企業は、雇用･委託･委任･準委任･請負などの契約関係にはありません。社会通念の範囲内で相互の信頼関係を築き、万一トラブル等が発生した場合は、大商にご相談頂くとともに、相互が誠意をもって対処して頂くものとします。セキスペは国家資格者であり、貴社の機密情報・個人情報に関する守秘義務は厳格に遵守されます。なお、セキスペの変更は原則できません。

5．実証参加企業の業務(SCS 評価制度の★取得申請含む)の概要と想定される工数

①実証参加企業の業務概要は、上記４.①(A)～(D)に係る準備･対応業務、★取得(全要求項目の充足：経済産業省「★3 要求事項･評価基準」参照)に向けて必要となる業務(一定の知識･技能の習得、組織体制の整備、技術的な対応など含む)に、主体的に、最後まで諦めずに取り組んで頂くことです。

②実証参加企業およびセキスペは、事前に二者間で策定した「改善計画書」(ロードマップとスケジュール)に基づきつつも、期間が出来るだけ短くなるよう努めて頂くものとします。支援はオンライン又は訪問により行い、前者がメイン（訪問支援の回数はオンライン支援の 1/2 以内の回数）となります。

③１社あたりの支援回数上限は、既達率 20%以下の企業で 21 回まで、21～40%で 18 回まで、41～60%で 15 回まで、61～80%で 12 回まで、81%以上の企業で 9 回までとなります。セキスペによる支援を受けているとき以外にも、その準備や事後処理、各種作成業務、アンケート対応などが発生します。

④支援期間は最短 3 か月以上(IPA の規定)、最長 9～12 か月以内となります。結果的に★取得水準まで達する前に支援を終了させて頂く場合もあり、★取得を保障するものでありません。

⑤セキスペとの打合せの中で“次回までの宿題”や“○月○日までに達成”等の目標や取り決めがある場合は、期限までに着実にご履行願います。

⑥実証参加企業は、原則としてセキスペへの“丸投げ”は出来ません。例えば、規定や手順書の作成につき、セキスペはその雛形･事例･作成法の提示･助言はしますが、作成自体は実証参加企業の責任において行って頂きます。

⑦ネットワーク機器・各種ソフト・クラウドサービス等の導入・保守等に関係する IT ベンダ様等にご協力を求める場合もあります。

⑧全要求項目を達成した場合は、実証参加企業自らが★3 取得申請書に記入(自己適合宣言)し、セキスペの確認･評価を受けたうえで、セキスペから署名を受け、SCS 評価制度事務局に提出し★取得を行って頂きます。実証期間中に限り申請･登録費用は免除（IPA が負担）。

⑨実証参加企業としての業務や工数は各企業様により大きく異なります。のべ十数人日～数十人日(事前準備･事後対応･付随業務含め)、全体の期間は半年～1 年かかる場合もあります。「★を取得したら終わり」ではなく、★の維持には、その後の運用と、年 1 回の「専門家確認付き自己評価」が必要となります。IT ツールの利用料金は実証終了後は自己負担となります。