「中小企業向けサイバーセキュリティ対策支援者リスト」申請書（登録）

【基本情報】

情報処理安全確保支援士登録番号 ※必須	第 ＿＿＿＿＿＿ 号
氏名 ※必須	
氏名カナ ※必須	
居住地（都道府県と市区町村まで） ※必須	
所属状況 ※必須（いずれか○で選択）	独立 ・ 企業勤務 ・ その他（ ）
所属企業・組織名	
メールアドレス ※必須	
参考 URL（リンク先の情報に関してはご自身で管理願います。IPA は一切の責任を負わないものとします）	
写真（上半身正面、10MB 以下）	

その他保有資格（複数選択可）

- □ IT コーディネータ
- □ 中小企業診断士
- □ 税理士
- □ 社会保険労務士
- □ 行政書士
- □ 医療情報技師
- □ IT ストラテジスト
- □ システム監査技術者
- □ CISA（公認情報システム監査人）
- □ CISSP
- □ その他（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

所属する団体や組織（複数選択可） ※必須

- □ 商工会議所・商工会
- □ 中小企業庁関連（中小企業基盤整備機構・よろず支援拠点・都道府県等中小企業支援センター等）
- □ 金融機関
- □ 日本自動車工業会・日本自動車部品工業会
- □ 情報処理安全確保支援士会
- □ IT コーディネータ協会
- □ 中小企業診断士協会
- □ 税理士会
- □ 社会保険労務士会
- □ 行政書士会
- □ その他（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）
- □ 該当なし

【経験・実績】

セキュリティ分野での実務経験年数 ※必須

○ 3 年未満
○ 3-5 年
○ 5-10 年
○ 10 年以上

企業に対するセキュリティ対策支援の経験有無 ※必須

○ 経験なし
○ 経験あり

「経験あり」の場合、支援実績（件数・年数・内容） ※必須

支援件数 ※必須	_____ 件
支援年数 ※必須	_____ 年
主な内容 ※必須 50 字以内	

【支援可能な範囲等】

支援可能な業界（複数選択可） ※必須

□ 自動車産業
□ 半導体産業
□ その他製造業
□ 建設業
□ 防衛産業
□ 電力産業
□ 運輸・交通業
□ 小売業
□ 卸売業
□ サービス業
□ 金融業
□ 医療
□ 教育
□ その他（_____）
□ 該当なし

支援可能な企業規模（複数選択可） ※必須

- □ 従業員 10 名以下
- □ 従業員 11-50 名
- □ 従業員 51-100 名
- □ 従業員 101-300 名
- □ 従業員 301 名以上
- □ 該当なし

支援可能な地域・都道府県（複数選択可） ※必須

□ 北海道・東北
□ 北海道 □ 青森県 □ 岩手県 □ 宮城県 □ 秋田県 □ 山形県 □ 福島県

□ 関東
□ 茨城県 □ 栃木県 □ 群馬県 □ 埼玉県 □ 千葉県 □ 東京都 □ 神奈川県

□ 甲信越
□ 新潟県 □ 山梨県 □ 長野県 □ 富山県 □ 石川県 □福井県

□ 東海
□ 岐阜県 □ 静岡県 □ 愛知県 □ 三重県

□ 近畿
□ 滋賀県 □ 和歌山県 □ 京都府 □ 大阪府 □ 兵庫県□ 奈良県

□ 中国
□ 鳥取県 □ 島根県 □ 岡山県 □ 広島県 □ 山口県

□ 四国
□ 徳島県 □ 香川県 □ 愛媛県 □ 高知県

□ 九州・沖縄
□ 福岡県 □ 佐賀県 □ 長崎県 □ 熊本県 □ 大分県 □ 宮崎県 □ 鹿児島県
□ 沖縄県

□ 全国（47 都道府県すべて）

支援可能な形態（複数選択可） ※必須

- □ 訪問によるコンサルティング
- □ オンラインコンサルティング
- □ 講演・研修
- □ インシデント発生時の緊急対策支援
- □ セキュリティ製品の選定・導入支援
- □ 長期的支援（顧問契約等）
- □ その他（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）
- □ 該当なし

支援可能なテーマ（マネジメント指導ツールに準拠）（複数選択可） ※必須

- □ 情報セキュリティ規程の整備
- □ 情報資産の洗い出しとリスク分析
- □ クラウドサービスの安全利用
- □ セキュリティインシデント対応
- □ 従業員向け情報セキュリティ教育
- □ 該当なし

支援の際に希望する報酬額（1 回 2 時間あたり） ※必須

- ○ 20,000 円未満
- ○ 20,000 円以上～30,000 円未満
- ○ 30,000 円以上～40,000 円未満
- ○ 40,000 円以上

初回相談の無料特典の有無（初回の相談を無料にする・しない） ※必須

- ○ あり
- ○ なし

指導先 1 社につき支援可能な期間（複数選択可） ※必須

- □ スポット対応
- □ 1～3 か月
- □ 3 か月～半年
- □ 半年～1 年程度
- □ 1 年以上の長期的支援（顧問契約等）
- □ その他（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

支援における自己 PR（あなたの強み） 50 文字以内

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

【保有スキル】

S1. サイバーセキュリティ対策の方針策定と管理体制づくり

a. 経営戦略の理解、経営者とのコミュニケーション

（0：知識・経験なし 1：基礎知識のみ 2：サポートがあれば実行可能 3：単独実行可能）

次の項目の習熟度を選択してください。		0	1	2	3
(1)	経営戦略の理解：企業のビジョン、経営目標、マーケティング戦略を理解し、サイバーセキュリティインシデントがもたらすビジネスリスクを正しく評価できる	○	○	○	○
(2)	経営層への説得（サイバーセキュリティ対策）：サイバーセキュリティ対策の重要性を他のビジネスリスクと比較しながら経営者に説明できる	○	○	○	○
(3)	経営層への説得（セキュリティ文化の醸成）：企業全体がセキュリティ意識をもつことの重要性について経営者に説明できる	○	○	○	○
(4)	リスクの定量化：サイバー攻撃による潜在的な経営損失を具体的な数値で算出できる	○	○	○	○
(5)	サイバーセキュリティ対策保険の知識：リスクに基づく加入要否の判断から、各保険商品の補償内容・適用範囲・費用対効果を考慮した最適な商品を選定するための支援を実行できる	○	○	○	○

b. サイバーセキュリティ対策体制の構築、 サイバーセキュリティ対策の基本方針の構築と運用

（0：知識・経験なし 1：基礎知識のみ 2：サポートがあれば実行可能 3：単独実行可能）

次の項目の習熟度を選択してください。		0	1	2	3
(1)	サイバーセキュリティ対策責任者の設定：サイバーセキュリティ対策の企画・実行における責任者を特定し、その役割・権限・責任範囲を明確にするための支援を実行できる	○	○	○	○
(2)	サイバーセキュリティ対策の方針の策定と運用：サイバーセキュリティ対策の方針の策定から周知、運用、維持を行うための支援を実行できる	○	○	○	○

c. 外部リスク評価力、コンプライアンス対応

（0：知識・経験なし 1：基礎知識のみ 2：サポートがあれば実行可能 3：単独実行可能）

次の項目の習熟度を選択してください。		0	1	2	3
(1)	サプライチェーンリスクの評価：取引先やクラウドサービス提供者のセキュリティリスクを評価できる	○	○	○	○
(2)	サイバーセキュリティに関する法令、規制、業界固有ガイドライン等の知識：サイバーセキュリティセキュリティに関する法律や、規程、取引要件となる業界のサイバーセキュリティガイドラインを理解し、適用のための支援を実行できる	○	○	○	○

S2. セキュリティリスクの識別

a. 情報資産の洗い出しと情報資産管理台帳の運用設計、潜在リスクの特定と評価

（0：知識・経験なし 1：基礎知識のみ 2：サポートがあれば実行可能 3：単独実行可能）

次の項目の習熟度を選択してください。		0	1	2	3
(1)	情報資産の管理：情報資産管理台帳を作成し、継続的に更新・運用するプロセスを設計・実施できる	○	○	○	○
(2)	情報資産リスクの評価：情報資産持つリスクを体系的に分類、評価し、優先順位付けができる	○	○	○	○

b. リスクに基づくサイバーセキュリティ対策の策定、現存対策の評価及び改善点の指摘

（0：知識・経験なし 1：基礎知識のみ 2：サポートがあれば実行可能 3：単独実行可能）

次の項目の習熟度を選択してください。		0	1	2	3
(1)	リスク対応策の策定と文書化：リスク管理表に基づき、各リスクへの対応策を具体化し、文書化する支援を実行できる	○	○	○	○
(2)	サイバーセキュリティ対策の評価：既存のサイバーセキュリティ対策の効果について評価し、改善点を指摘できる	○	○	○	○

c. 社内外における、サイバーセキュリティ対策の推進

（0：知識・経験なし 1：基礎知識のみ 2：サポートがあれば実行可能 3：単独実行可能）

次の項目の習熟度を選択してください。		0	1	2	3
(1)	サイバーセキュリティ対策の社内外への発信（コミュニケーション）：サイバーセキュリティ対策やポリシーの内容、実施計画や運用について企業内外に発信する支援を実行できる	○	○	○	○
(2)	セキュリティ文化の醸成 ：企業全体のセキュリティ意識向上のための具体的な施策を提案・実施ができる	○	○	○	○

S3. サイバーセキュリティ対策の実践と運用の強化

a. アカウント管理、アクセス管理

（0：知識・経験なし 1：基礎知識のみ 2：サポートがあれば実行可能 3：単独実行可能）

次の項目の習熟度を選択してください。		0	1	2	3
(1)	アカウント管理・アクセス管理：適切なアカウント・アクセス管理ポリシーを設計し、アカウントの分類や権限管理を効果的に実施できる	○	○	○	○

b. データ管理、システムセキュリティ管理、コンテンツセキュリティ管理

（0：知識・経験なし 1：基礎知識のみ 2：サポートがあれば実行可能 3：単独実行可能）

次の項目の習熟度を選択してください。		0	1	2	3
(1)	システム更新：ソフトウェア、OS の更新管理に関する支援を実施できる	○	○	○	○
(2)	データバックアップ：適切な方式や頻度でのデータバックアップ実施と管理の支援を実施できる	○	○	○	○
(3)	暗号化：暗号化を実施すべき情報機器を特定し、データ保護対策実施のための支援を実施できる	○	○	○	○

c. 社内セキュリティ教育の策定と運用

（0：知識・経験なし 1：基礎知識のみ 2：サポートがあれば実行可能 3：単独実行可能）

次の項目の習熟度を選択してください。		0	1	2	3
(1)	社内セキュリティ教育の策定：既存の社内セキュリティ教育を評価し、効果的な教育の策定と運用のための支援を実施できる	○	○	○	○

S4. サイバー攻撃の検知と監視、検知後の運用策定

a. セキュリティインシデント対処教育の策定と実施

（0：知識・経験なし 1：基礎知識のみ 2：サポートがあれば実行可能 3：単独実行可能）

次の項目の習熟度を選択してください。		0	1	2	3
(1)	セキュリティインシデント対処の教育：セキュリティインシデントの一般的な兆候を識別する方法について、効果的な社員教育を実施できる	○	○	○	○

b. ウイルス対策ソフトの運用、システム・ネットワークの監視、外部監視サービスの導入

（0：知識・経験なし 1：基礎知識のみ 2：サポートがあれば実行可能 3：単独実行可能）

次の項目の習熟度を選択してください。		0	1	2	3
(1)	ウイルス対策ソフトの運用：適切なウイルス対策ソフトの選定、導入、運用設計を行い、効果的に実行する支援を実行できる	○	○	○	○
(2)	システム・ネットワークの監視：システムおよびネットワークの監視に関する知識を持ち、必要な運用体制を設計・実装できる	○	○	○	○
(3)	外部監視サービスの導入：中小企業向けの外部監視サービスについて熟知し、適切なサービスの選定と導入のための支援を実行できる	○	○	○	○

c. インシデント初動の運用設計と教育実施能力

（0：知識・経験なし 1：基礎知識のみ 2：サポートがあれば実行可能 3：単独実行可能）

次の項目の習熟度を選択してください。		0	1	2	3
(1)	初動対応設計：セキュリティ事象の検知時の初動について、適切な運用を設計できる	○	○	○	○

S5. セキュリティインシデント発生時の対応

a. セキュリティインシデント対応（セキュリティインシデント対応計画の策定、セキュリティインデント調査・対応、セキュリティインシデント報告・公表支援）

（0：知識・経験なし 1：基礎知識のみ 2：サポートがあれば実行可能 3：単独実行可能）

次の項目の習熟度を選択してください。		0	1	2	3
(1)	セキュリティインシデント対応計画の策定：情報セキュリティインシデント対応計画の策定と管理・運用体制を構築する支援を実行できる	○	○	○	○
(2)	セキュリティインシデント分析：発生した事象に基づき、セキュリティインシデントの原因、被害とその影響範囲を正確に分析できる	○	○	○	○
(3)	封じ込め戦略立案：発生した事象に基づき、適切なセキュリティインシデント封じ込め対策を設計できる	○	○	○	○
(4)	セキュリティインシデントの報告と公表：セキュリティインシデント発生時における関係者への報告・公表プロセスを適切に実施および管理する支援を実行できる	○	○	○	○

S6. セキュリティインシデントからの復旧とコミュニケーション

a. セキュリティインシデント復旧支援

（0：知識・経験なし 1：基礎知識のみ 2：サポートがあれば実行可能 3：単独実行可能）

次の項目の習熟度を選択してください。		0	1	2	3
(1)	インシデント復旧支援：セキュリティインシデント発生時のビジネス復旧に関する責任の所在を正しく理解するための支援を実行できる	○	○	○	○
(2)	インシデント事後報告書作成：インシデントの詳細、時系列、影響範囲から、実施された対応・教訓までを正確かつ簡潔に文書化する支援を実行できる	○	○	○	○
(3)	データ復旧：セキュリティインシデントからの復旧時に、正しいバックアップデータを選定し、効果的な復旧を行うための支援を行える	○	○	○	○
(4)	復旧行動の優先順位付け：セキュリティインシデント復旧対応について、適切に優先順位付けを行える	○	○	○	○
(5)	ステークホルダーとのコミュニケーション：インシデント対応中の関係者、顧客等利害関係者への適切な頻度と内容での情報共有を管理できる				