

# 経済産業省の登録セキスぺ活用の取組

2025年12月

経済産業省 商務情報政策局

サイバーセキュリティ課

# サイバーセキュリティ人材の育成促進に向けた検討会最終取りまとめ（要点）

- 我が国においてサイバーセキュリティ人材が不足しているとの声は多く、国内で約11万人不足しているとの民間調査結果※もある。  
（出典）ISC2 Cybersecurity Workforce Study 2023
- サイバーセキュリティ人材の不足に対応するためには、トップ人材や高度専門人材から、地域の中小企業等でセキュリティ対策を推進する人材まで、各層の課題に応じた施策を戦略的に進めることが重要。
- このため、これまで一定の効果を生み出している既存の施策の拡充・改善をベースとして、実際に政策ニーズを有する組織の方へのヒアリング等も通じ、令和7年5月に政策対応の方向性を取りまとめ。今後も各施策の継続的な改善を実施。

## 対応の方向性

### ①セキュリティ・キャンプ※の拡充

- AI等の特定領域と掛け合わせた高度セキュリティ人材の育成を目的とする新たな「キャンプ」を実施
- 修了生の継続的な知見研鑽・社会還元・活躍状況共有等を目的とした「コミュニティ」を整備



※世界に通用するトップクラスの人材を育成・発掘する取組

### ②登録セキスぺ※の活用促進

- 個社の状況に応じた個別相談・支援等が可能な登録セキスぺのリストを整備し、中小企業支援機関等を通じて中小企業との人材マッチングを促進
- 所定の実務経験を有する者を対象に、資格更新時の講習のみなし受講制度を導入 等



※セキュリティに係る専門的な知識・技能を備えた国家資格（情報処理安全確保支援士）

### ③中堅・中小企業等における人材確保策の提示

- 中堅・中小企業が実施すべきセキュリティ対策に応じた人材確保・育成の実践的方策ガイドをβ版として整理
- 人材を「育成」する際に参照できる教材・資格等も提示

## 今後の取組

- 「セキュリティ・キャンプコネクト」として新たなキャンプを開催（令和8年春頃）
- 修了生向けコミュニティの活動開始（令和7年度中）

- リストの整備・運用開始（令和7年度中）
- 同リスト活用促進に向けた支援機関等との連携策具体化
- 省令改正により講習のみなし受講制度を創設（令和8年度中に制度開始想定）

- 中小企業に対するβ版の実証事業を実施等しながら成案化  
※リストの活用方法も提示
- 中小企業向けセキュリティ促進施策との連携や広報資材の改善含め、普及活動を実施

## 目指す効果

- 「トップガン」人材育成スケール拡大（現状の2倍以上）
- セキュリティ人材のキャリアの魅力化

- 登録セキスぺの活躍機会（中小企業のセキュリティ確保等の実務経験機会）増加
- 登録セキスぺ資格更新時の負担軽減
- 中堅・中小企業におけるセキュリティ人材探索コストの低減
- 中堅・中小企業内での内部人材育成容易化

**2030年までに登録セキスぺ5万人  
（2025年4月時点で約2.4万人）を達成**

# IPA「情報セキュリティ10大脅威」

情報セキュリティ10大脅威 2025	
順位	組織向け脅威
1位	ランサム攻撃による被害
2位	サプライチェーンや委託先を狙った攻撃
3位	システムの脆弱性を突いた攻撃
4位	内部不正による情報漏えい等
5位	機密情報等を狙った標的型攻撃
6位	リモートワーク等の環境や仕組みを狙った攻撃
7位	地政学的リスクに起因するサイバー攻撃
8位	分散型サービス妨害攻撃（DDoS攻撃）
9位	ビジネスメール詐欺
10位	不注意による情報漏えい等

中小企業の被害が全体の6割以上を占める

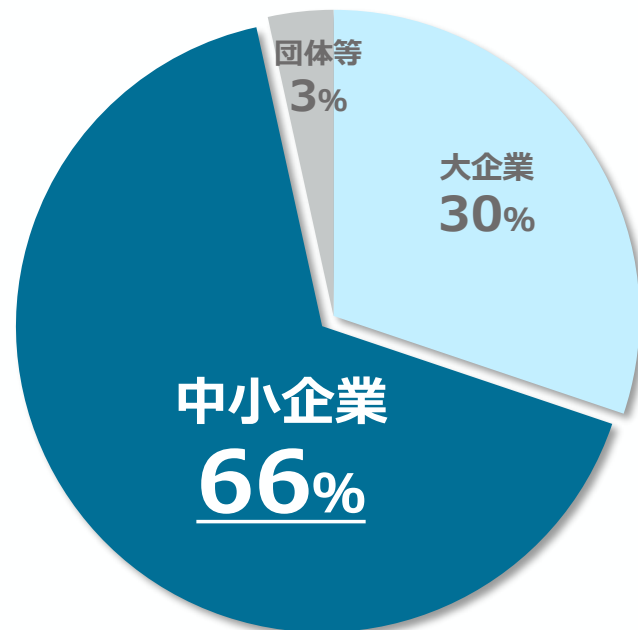
相対的にセキュリティ対策の弱い中小企業を起点に、大企業含むサプライチェーンを共有する企業を攻撃

初選出

# 中小企業等にとってもサイバー攻撃は他人ごとではない

- 「サイバー攻撃」は身近なところで起きている。ランサムウェア被害件数は令和6年から増加しており、中小企業が狙われる状況が過去最多となった。
- ランサムウェアの被害による調査・復旧費用が高額化しており、実際に、復旧までに1か月以上を要するケースや数千万円規模の被害が生じるケースが5割を超えている。

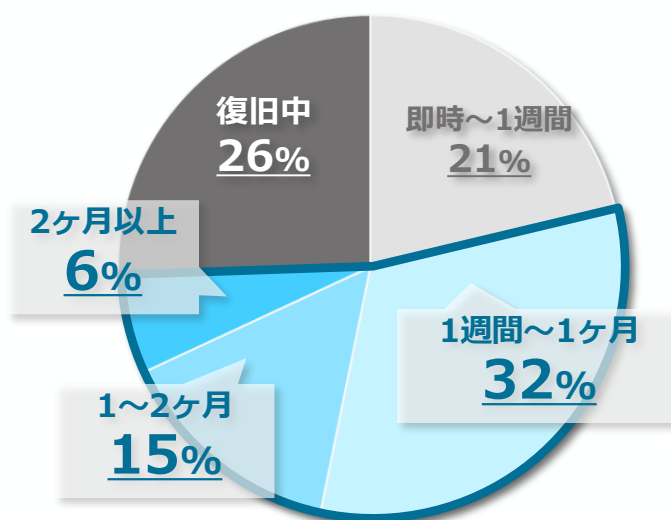
ランサムウェア被害企業等の規模別件数



➡ランサムウェア被害の6割以上が中小企業  
(令和6年から3ポイント増加)

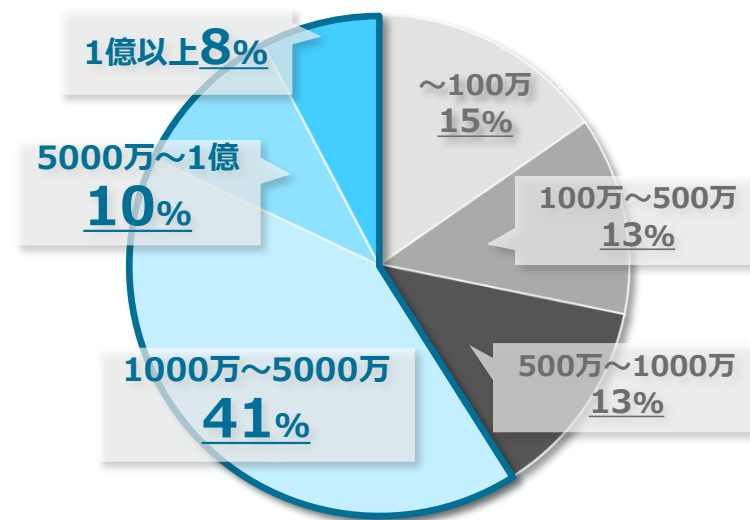
ランサムウェア被害（復旧に要した時間、調査費用総額）

【復旧に要した時間】



➡ランサムウェア被害による調査・復旧費用が高額化しており、1000万円以上を要した割合は59%(令和6年から9ポイント増加)

【調査費用総額】



# セキュリティ対策の中小企業支援策における人材施策の位置付け

- 本検討会の成果物「**中小企業向けサイバーセキュリティ対策支援者リスト**」や「**人材確保・育成の実践的方策ガイド**」については、中小企業等が抱える課題・ニーズや各種施策の中に位置付けて取組を推進。

## セキュリティ対策として何を実施すべきか

どこから始めれば  
良いか分からない



セキュリティ対策自己宣言



セキュリティ対策自己宣言

リスクを正しく評価しそれに即した  
取組を選択できない、異なる様々な  
対策水準を要求される

＜サプライチェーン対策評価制度＞

★3・★4取得に必要な要求事項  
(大分類) (案)

- ✓ ガバナンス
- ✓ 取引先管理
- ✓ リスクの特定
- ✓ 攻撃等の防御・検知
- ✓ インシデントへの対応
- ✓ インシデントからの復旧

セキュリティ対策の  
きっかけを提供

必要な取組水準の共通化・  
対策状況の可視化

登録セキスペ  
(外部人材)  
でカバー

補助施策との連動  
(補助要件化、導入費用  
補助)、業界団体等を通じた働きかけにより浸透

業界団体等を通じた働きかけ、法令解釈の明確化等により浸透

## セキュリティ対策の実施のためにどのような支援があるか

十分なコストをかけられない



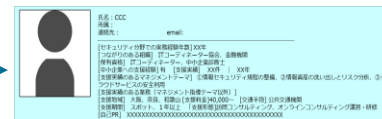
お助け隊でカバー  
※カバー範囲を広げる  
見直しも検討

必要最低限の対策を安価に提供  
(監視、駆付け、  
保険)

補助施策との連動  
(補助要件化、導入費用  
補助)、業界団体等を通じた働きかけにより浸透

対策を実施できる人材がいない  
(内部で育成出来ない／外部で見つけれない)

＜中小企業向けサイバーセキュリティ対策  
支援者リストを活用したマッチング＞



参照

人材探索コストを  
低減、効率的な人材  
確保手段の提示

＜人材育成・確保の  
実践的方策ガイド＞

既存ガイドと  
の整合確保



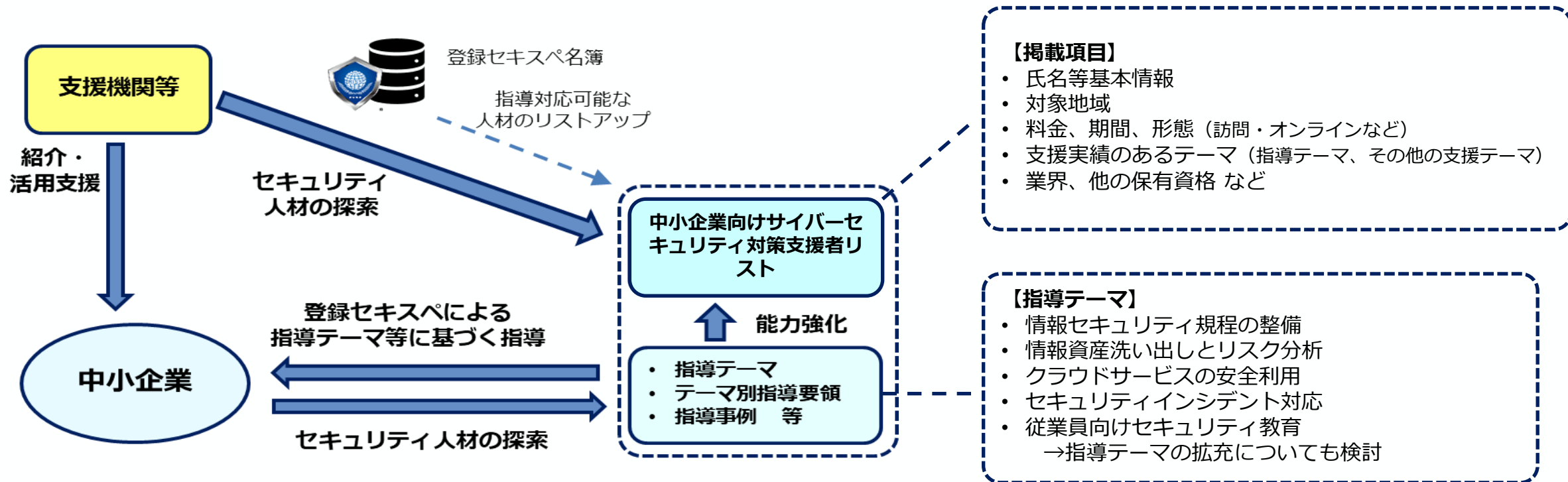
(etc.)

中小企業の支援  
機関等が行う  
マッチング、教育  
訓練機会の提供  
事業者・ITベン  
ダ等を通じた  
働きかけにより  
浸透



# 「中小企業向けサイバーセキュリティ対策支援者リスト」を通じた中小企業支援

- 中小企業等と情報処理安全確保支援士（登録セキスペ）とのマッチング実証を行い、**中小企業等に対するセキュリティコンサルが可能な登録セキスペの得意分野・専門領域を可視化する「中小企業向けサイバーセキュリティ対策支援者リスト」をHP上で公表**
  - リスト掲載項目の一つである**指導テーマの拡充**など、**継続的にリストの掲載内容・運用を改善**。
- リストの活用を通じて、中小企業が**多大な探索コストをかけることなく**、地域の支援機関等を通じて**登録セキスペを活用**。**登録セキスペにとっても活躍の機会が広がることを期待**。



# (参考) 指導テーマ

- 業種を問わない「基本の基」のセキュリティ対策として、**中小企業ガイドライン（付属書を含む）の指示項目の実装を目的とした指導のテーマ**を設定し、各テーマについて指導マニュアルを整備。
- 令和7年度以降、既存の指導テーマのブラッシュアップや指導テーマの拡充について検討。

	1 情報セキュリティ 規程の整備	2 情報資産の 洗い出しと リスク分析	3 クラウドサービスの 安全利用	4 セキュリティ インシデント対応	5 従業員向け 情報セキュリティ 教育
ターゲット企業	サイバー攻撃の増加や法令遵守の必要性に直面しつつも、情報セキュリティ規程が未整備な中小企業。特に、従業員が多様なITツールを使って業務を行っているが、具体的な指針がなく、責任範囲が曖昧な企業に必要である。	デジタル化が進み、膨大な情報を管理しているが、どの情報が重要か、リスクがどこにあるかが把握できていない企業。特に、製造業やサービス業など、顧客情報や技術情報を大量に扱う企業に必要である。	業務効率化のためにクラウドサービスを導入しているが、セキュリティリスクに対する理解や対策が不十分な企業。特に、情報管理の外部委託が進んでいるが、適切な安全対策ができていない中小企業に必要である。	セキュリティインシデントが発生した際の対応が曖昧で、事後対応に時間がかかり、被害が拡大するリスクがある企業。特に、サプライチェーンの一部として他社との連携が多い企業に必要である。	従業員のセキュリティ意識が低く、パスワード管理やフィッシング攻撃に対する対応が不十分な企業。特に、ITリテラシーの差が大きい企業や、非専門職の従業員が多く、日常的なセキュリティ対策が徹底できていない企業に必要である。
期待される効果	不足していた情報セキュリティ規程が整備され、社内での運用・周知方法まで確立されることで、社内セキュリティ体制の継続的・自律的な改善が図れるようになる。	企業が保有する情報資産が洗い出され、リスク分析シートとして整備することで、自律的な運用が図れるとともに、リスク低減策等の検討の題材にもなる。	当該支援先企業における「クラウドサービス安全利用の手引き」を策定することで、クラウドサービス利用に伴うリスクを理解できるようになる。	インシデント対応プロセスを整備し、必要に応じ、従業員の訓練も実施することで、セキュリティインシデント発生時に迅速かつ効果的に対応できる体制が構築できる。	セキュリティ教育プログラムを策定するとともに、定期的に見直しと更新を行う体制を構築。実際に従業員に対するセキュリティ教育を実施することで、社内の意識向上にもつなげられる。

# リストのイメージ

- ・既にIPAのホームページに掲載されているが、リストのイメージは以下のとおり

中小企業向けサイバーセキュリティ対策支援者リスト（支援対象地域＝関東）

※情報セキュリティ対策に関する講師や相談相手

（関東：茨城県,栃木県,群馬県,埼玉県,千葉県,東京都,神奈川県）

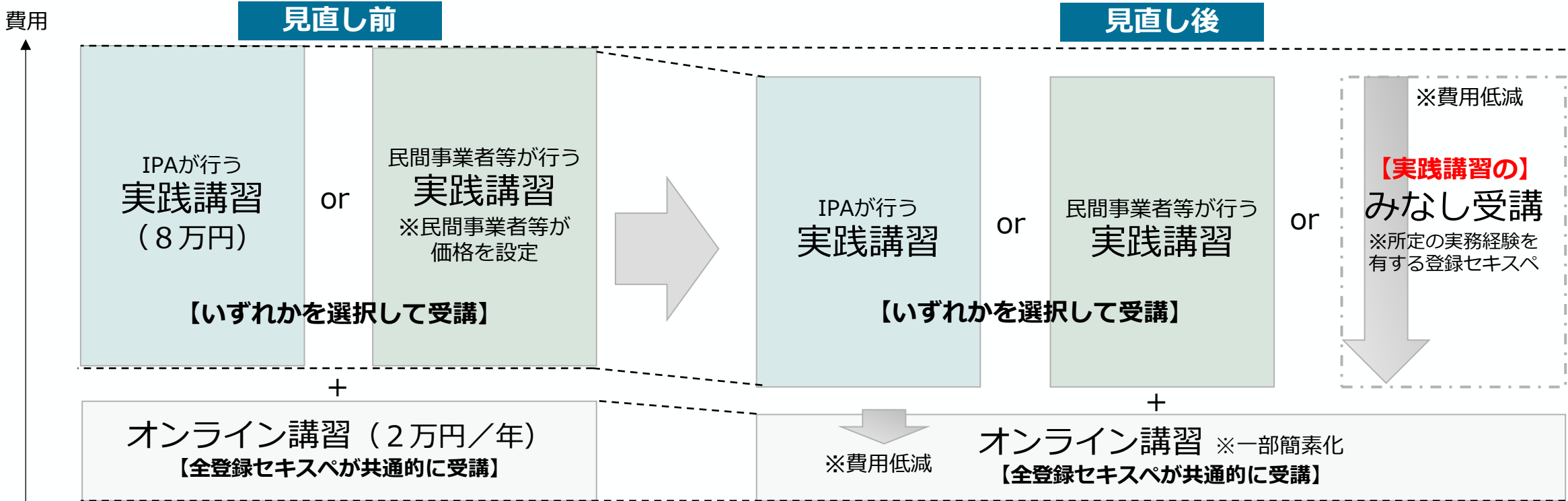
居住地	情報処理 安全確保 支援士 登録番号	氏名	カナ	メールアドレス	支援可能な指導テーマ					企業 支援経験	中小企業 支援経験	中小企業支援実績	得意とする業界	支援対象地域	支援期間
					1.情報セ キュリティ規 程の整備	2.情報資 産の洗い出 しとリスク分 析	3.クラウド サービスの 安全利用	4.セキュ ティインシ デント対応	5.従業員 向け情報セ キュリティ教 育						
東京都新宿区					可	可	可	可	可	経験あり	支援件数12件 / 支援年数6年	1.中小企業情報セキュリティマネジメント指導業務においてセキュリティー基本方針と関連規程類の作成、Security Action 2 つ星申請支援 2.工場セキュリティガイドラインを利用した中小企業の工場セキュリティ診断支援とセキュリティ強化案のアドバイス 3.テレワークセキュリティ支援 4.Windows10のサポート切れ対策支援	自動車産業/その他製造業/建設業/教育/地方公共団体	北海道,東北,関東,甲信越,東海,近畿,中国,四国,九州	スポット対応 1～3か月 半年～1年程度 1年以上の長期的支援 （顧問契約等）
茨城県つくば市					可	可			可	経験なし			医療	茨城県,東京都	スポット対応 1～3か月
茨城県鉾田市					可	可	可		可	経験なし			新聞社	茨城県,栃木県,埼玉県,千葉県	スポット対応 1～3か月 半年～1年程度 1年以上の長期的支援 （顧問契約等）
栃木県足利市					可	可	可		可	経験あり	支援件数5件 / 支援年数3年	1.中小企業の情報セキュリティマネジメント指導業務 1 件 2.自動車産業サイバーセキュリティガイドラインへの対応を求められた金型製造業への対応方法指導、 3.よろず支援拠点のコーディネーターとして軽微なアドバイスを3件程度	自動車産業/その他製造業/建設業/運輸・交通業/小売業/卸売業/サービス業/教育	全国	スポット対応 1～3か月 半年～1年程度 1年以上の長期的支援 （顧問契約等）



# みなし受講制度検討の背景とイメージ

- 技術進歩に応じて適切に知識及び技能を更新しなければ、新たな脅威に対応できず、社会全体に甚大なサイバー被害をもたらす事態を招きかねないことから、講習受講が資格更新（3年ごと）の要件（令和2年5月～）。
  - 一方、登録セキスぺの中には、講習と同等以上実務（企業のサイバーセキュリティ対策の支援等）に携わっている者が存在しており、必ずしも講習の受講義務という形を採らずとも、最新の知識・技能が担保される場合もあるものと想定。
  - また、更新制度が実施されている中で、実務から遠のいている登録セキスぺを実務に向かわせるインセンティブを設定することが、登録セキスぺの一層の活用促進、ひいては事業者のサイバーセキュリティ対策向上に資する。
- ※ 更新のための講習費用は合計して少なくとも10万円を超えるものが大半を占めており、登録消除者のアンケートによれば費用負担が大きいとの意見あり。

資格更新に際して、国家資格としての責務や倫理等に関する講習受講は引き続き義務としつつ一部の講習については所要の実務経験をもって代替し、受講したものとみなす制度を創設。



# I - 3 登録セキスぺ③（その他の登録セキスぺ活用促進策等）

## 登録セキスぺの活用促進の取組

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における活用	<ul style="list-style-type: none"><li>企業が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の★3の対策を満たす旨を自己評価する際に、対策を評価する専門家として登録セキスぺを活用。</li><li>評価者としての登録セキスぺを育成するために、令和7年度予算事業では、①サプライチェーン対策評価制度の実施を見据えた指導テーマを拡充し、★3の対策が実施できているかを登録セキスぺが評価するための指導要領を作成。②併せて、登録セキスぺに対して、企業評価のためのスキル（監査スキル）習得機会を提供。</li></ul>
DX施策との連動 （デジタルガバナンス・コードへの紐づけ等）	<ul style="list-style-type: none"><li>企業のDX推進に関連する各種文書に登録セキスぺの活用・配置の紐づけを推進（令和6年9月）。</li><li>取組例として、「デジタルガバナンス・コード」（DX銘柄やDX認定の基準）や「中堅・中小企業等向けDX推進の手引き」に登録セキスぺの活用を明記（令和7年3月）。</li></ul>
各種投資促進施策における要件化	<ul style="list-style-type: none"><li>経済産業省の各種補助施策において登録セキスぺ配置の要件化を進め、投資を通じた事業の毀損リスクを低減させるために必要なサイバーセキュリティ対策を推進する人材としての登録セキスぺの活用を促進。</li><li>取組例として、「令和5年度補正予算グローバルサウス未来志向型共創等事業費補助金」や「特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律による補助」において、登録セキスぺの配置を要件化。</li></ul>
公的機関・重要インフラ事業者等における配置促進	<ul style="list-style-type: none"><li>政府機関、地方自治体などの公的機関、重要インフラ事業者の内部における配置のみならず、それらの組織の委託先における配置まで含めた、登録セキスぺの活用を推進。</li><li>取組例として、総務省において新たに作成された「（自治体DX全体手順書・別冊）デジタル人材の育成ガイドブック（令和6年12月策定）」において、デジタル人材が取得することが想定されるIT関連資格として、登録セキスぺを明記。また、令和6年12月にNISC主催の全分野一斉演習の参加企業等に対して、登録セキスぺ制度の紹介及び活用策について周知。</li></ul>

（注）上表のほか、セキュリティ要件適合評価及びラベリング制度（JC-STAR）における登録セキスぺの活用についても引き続き検討。

## 登録セキスぺの能力向上、スキル・実績の見える化（登録セキスぺアクティブリスト以外）

デジタル人材育成・DX推進プラットフォーム整備との連携	<ul style="list-style-type: none"><li>「Society 5.0時代のデジタル人材育成に関する検討会」において、個人のデジタルスキル情報の蓄積・可視化によりデジタル技術の継続的な学びを実現するとともに、スキル情報を広く労働市場で活用するための仕組みとして、デジタル人材育成・DX推進プラットフォームの構想について検討。</li><li>デジタル人材育成・DX推進プラットフォームが具体化（令和8年下期リリース予定）されれば、登録セキスぺの能力向上及びスキル・実績の見える化促進が期待。</li></ul>
情報処理安全確保支援士試験の見直しとの連携	<ul style="list-style-type: none"><li>「デジタル人材のスキル・学習の在り方ワーキンググループ」において、デジタル人材の類型ごとに求められるスキル習得の考え方・学習の在り方について検討。サイバーセキュリティ分野については、本検討会においても議論。</li><li>検討会においては、自社内のマネジメント需要への登録セキスぺによる対応として、①試験制度自体の複雑化は避けるべきとの考え方とともに、②資格更新時の講習で対応していく考え方や、③試験問題においてマネジメントの要素を増やす考え方を提示。</li></ul>
更新時の義務講習におけるマネジメント要素の習得	<ul style="list-style-type: none"><li>自社内のマネジメント需要への登録セキスぺによる対応として、IPAの実践講習では、インシデント対応や、新規事業立上げの際に考慮すべきセキュリティリスクの検討など、経営層と連携したセキュリティ対策を行う能力を習得する講習を提供。</li><li>民間事業者等の実践講習においても、マネジメント要素を強化した講習の実施を期待。</li></ul>