経済産業省

資料３

サイバーセキュリティ人材の育成促進に向けたこれまでの議論の整理と継続的な検討事項

2024年11月

経済産業省 商務情報政策局

サイバーセキュリティ課

目次

Ⅰ　これまでの議論の整理（全体像）

- サイバーセキュリティ人材不足への対応として、本検討会では、既存施策の拡充や改善などを基本として、**①セキュリティ・キャンプの拡充、②登録セキスペの活用及び制度の見直し、③中堅・中小企業等の内部でセキュリティ対策を推進する者の確保に向けた新たな施策**、の３つの論点にスコープを絞って議論を進めてきたところ。
- 今般、これまで頂いた御意見等を踏まえ、各論点について**政策対応の方向性やとりまとめに向けた継続議論事項を整理**。

サイバーセキュリティ人材育成の現状

セキュリティに関する知識・スキル水準の程度

トップガン

例）大手セキュリティ企業に就職する者、ベンダーとして起業する者など

高度専門人材

例）規模が大きいユーザー企業のセキュリティ担当者、大手ベンダー実務担当者など

専門人材

例）中堅・中小企業のユーザーのセキュリティ担当者など

※プラス・セキュリティ人材については、セキュリティに関する知識・スキル水準の高低とは別軸であるため、対象外とする。

施策の空白地帯

各層の育成・確保に向けた主な施策

セキュリティ・キャンプ ①

中核人材育成プログラム

登録セキスペ制度 ②

③

政策的な課題

- １年間に**育成できる人数が限定的**であり、スケールしていない。
- 修了後の**状況を追跡できていない**。

- ①実態を伴う**登録セキスペの活躍イメージを提示できていない（活躍の場がない）**場合や、②人手不足の**中小企業と登録セキスペとのミスマッチ**が起きている場合がある。
- 結果として、**登録更新に係る費用を支払うだけの動機が失われ**、登録者数の大幅な増加には至っていない。

- 中堅・中小企業においてサイバーセキュリティ人材が不足している一方、**社内育成・確保は困難**。参考事例もほぼ無い。
- 中堅・中小企業といっても多様であり、必要なセキュリティ対策や体制・人材水準は**各々の状況により異なる**。

対応の方向性

- 単純拡大ではなく、裾野を広げる観点から、特定領域（AI等）の専門性と高度なサイバーセキュリティの知見の双方を兼ね備えた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**。

- 登録セキスペの得意分野・専門領域を可視化したリスト（アクティブリスト）の整備等を通じた**市場への働きかけ**や、各種制度における登録セキスペ配置の要件化等の**企業側への働きかけ**を多層的に実施。
- 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受講みなし制度を導入**する等により、資格維持コストを低減。

- 中堅・中小企業が実施すべきセキュリティ対策の状況に応じた**人材確保・育成の実践的方策**（「実践的方策を示したガイド）を整理し、様々な媒体で広報。
- 自社のセキュリティ対策における現在の立ち位置、目指すべき姿の参考となる事例、人材を「育成」する際に参照できる実際のセミナー・資格等も提示。

とりまとめに向けた継続議論事項

- 登録セキスペアクティブリストの詳細設計（掲載項目、活用促進策等）、更新講習の「みなし受講」の対象とする実務経験の範囲・判断方法等
- 中堅・中小企業向け「実践的方策を示したガイド」（β版）の策定、来年度におけるβ版の改善活動等（取組事例の収集、有効性の確認、普及方法）

⇒ 引き続きこれらの点について議論を行い、**令和６年度末までに①～③に係る具体的政策対応をとりまとめることを目指す**。

Ⅱ　セキュリティ・キャンプ

１．セキュリティ・キャンプの現状・課題・方向性
２．第２回までの主な御意見
３．新たなキャンプの実施
４．修了生コミュニティの整備
５．セキュリティ・キャンプに関する継続的な検討事項

1．セキュリティ・キャンプの現状・課題・方向性

（1）近年、セキュリティ・キャンプへの応募は、全国大会・ネクストキャンプともに増加しているものの、演習を提供する講師側のリソース等から、参加者数（育成者数）は横ばい（同旨 第１回事務局資料）。

（2）また、キャンプ修了生との継続的な関係を維持する枠組みが十分には整備されていないため、修了後の状況把握が不十分（同旨 第１回事務局資料）。

（1）講師側のリソース等の問題をクリアしつつ、セキュリティ・キャンプへの参加者数を拡大させ、セキュリティ人材の裾野を広げる必要。

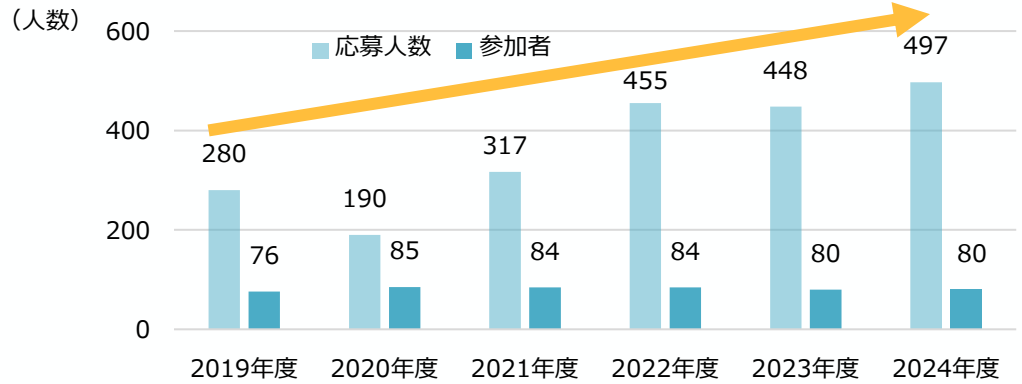
（2）キャンプ修了生との継続的な関係を維持する枠組みを整備する必要。

※　枠組みの整備については、①修了生に対する継続的な価値提供、②修了生の知見の社会への還元、③政府機関等と修了生との連携・協力、④人材供給、⑤セキュリティ・キャンプ自体の価値向上/有効性の確認といった観点あり。

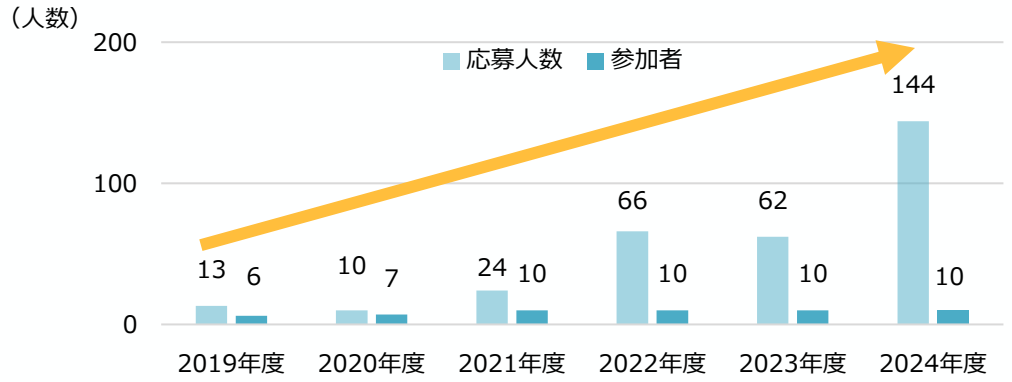
（1）新たなキャンプの実施

（2）修了生コミュニティの整備

全国大会の参加状況

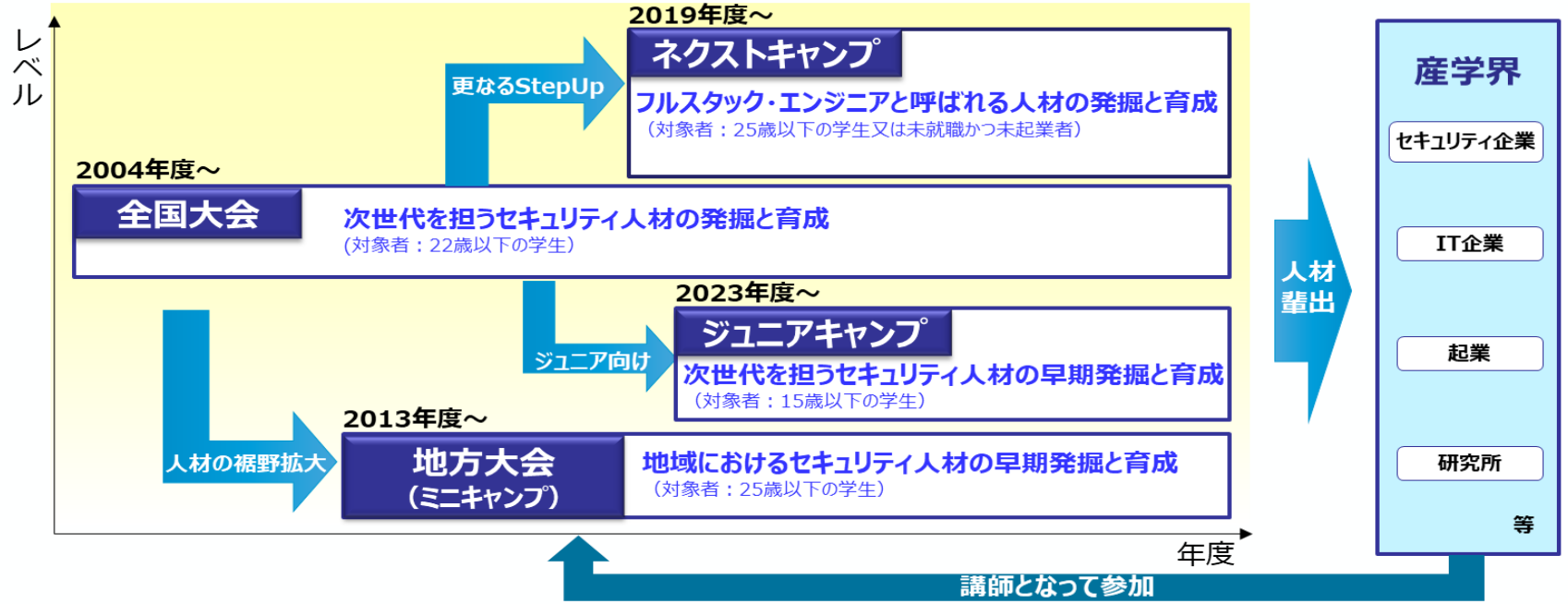


ネクストキャンプの参加状況



（参考）セキュリティ・キャンプの目的・全体像

- 複雑かつ高度化しているサイバー攻撃に適切に対応するため、若年層のセキュリティ人材発掘の裾野を拡大し、世界に通用するトップクラス人材を創出することが必要。
- IPAとセキュリティ・キャンプ協議会は、選抜された22歳以下の学生・生徒を対象とした、次代を担う情報セキュリティ人材発掘・育成する「セキュリティ・キャンプ全国大会」を開催。最新ノウハウも含めたセキュリティ技術を、倫理面と併せ、第一線の技術者から伝授。2004年度の開始からこれまでに、累計で1,232名が修了。
- 2019年度からは、全国大会修了生の次のステップとして、選抜された25歳以下の学生・生徒等を対象とした、情報セキュリティの多様なシーンに対応し新たな価値を生み出していけるトップオブトップの人材（フルスタック・エンジニア）を発掘・育成する「セキュリティ・ネクストキャンプ」を開催。これまでに累計で53名が修了。また、2023年度からは、全国大会の一部ゼミとして開催していたジュニアゼミを、「セキュリティ・ジュニアキャンプ」として、15歳以下の生徒を対象に開催。これまでに累計で11名が修了。



２．第２回までの主な御意見

＜新たなキャンプの実施に関するもの＞

- 現状の枠組みの良い部分は維持しつつ、落とさざるを得なかったが優秀だった応募者に対して、しっかりと育てる、再度応募してもらう、地方キャンプに回っていただくなどのフォローが可能になると良い。
- **育成する人数を増やすことが重要**。セキュリティ・キャンプの募集人数を２倍程度に増やしてみてはどうか。
- **改善の上で積み上げていくことの方が実務的**。応募倍率から考えるに、原石はまだまだ潜んでいる。
- **トップガンの人材拡大と、裾野の拡大は分けて考えるべき**ではないか。

＜修了生コミュニティの整備に関するもの＞

- IPA産業サイバーセキュリティセンターが実施している中核人材育成プログラムについては、修了生同士が活発につながっている一方で、セキュリティ・キャンプの修了生同士のつながりについて、**現状がどのようになっているのかを明確にすべき**。
- 修了生のプライドを**社会にも認めてもらえるような環境**を作れると良い。
- 拡大していく上では教える側の体制も重要。**修了生を講師に参画させる等の組織的な仕組みが必要**ではないか。

3．新たなキャンプ（セキュリティ・キャンプ・コネクト（仮称））の実施

（１）基本的な考え方

- 「Society5.0」における産業社会において、①サイバー攻撃の起点が拡大するとともに、サイバー攻撃がフィジカル空間に及ぼす影響も増大し、②サイバー攻撃の影響が社会全体に広範に及ぶ可能性がある中、③一部の業界・分野においては、その特性に応じた「サイバーセキュリティ対策」が一層求められる領域＊が生じてきていることから、**サイバーセキュリティに関する知見と、サイバーセキュリティ以外の特定の専門領域における知見をトップレベルで併有する人材が活躍**することで、**特定の専門領域の知見を踏まえた一層充実したサイバーセキュリティ対策の実装や新規ビジネス・技術開発の促進等が可能**になると考えられる。

  ＊　例えば、生成AI分野においては、悪意あるプロンプトを注入することで機密情報を盗む「プロンプトインジェクション」等の新たな脅威が出現しており、こうした特定領域に応じたセキュリティ対策の必要性が高まっている。

- また、現行のセキュリティ・キャンプの応募者の増加にもかかわらず、参加者数が横ばいとなっている状況の中で、**同キャンプの参加時に求められる知見・技術の水準には達しないものの、特定の専門領域における高度な知見・技術を有する者が一定数存在**することもうかがえる。

- こうしたことを踏まえ、セキュリティ人材の裾野の拡大に向けては、**現行のセキュリティ・キャンプの対象者を単純に拡大するのではなく、特定の専門領域における高度な知見・技能を有する者の中からサイバーセキュリティに関する一定の知見を有する者を発掘**し、**サイバーセキュリティに関する知見と、サイバーセキュリティ以外の特定の専門領域における知見をトップレベルで併有する人材を育成**する**新たなキャンプ（セキュリティ・キャンプ・コネクト（仮称））**を実施することを検討。

  ※　リソース面において、現行のセキュリティ・キャンプの単純拡大については、演習を提供する側のキャパシティの論点があるところ、新たなキャンプでは、現行のセキュリティ・キャンプとは別途の講師を確保することを想定（特定の専門領域に関する大学等の関係機関との連携を予定）。

  ※　新たなキャンプの対象者については、若年層のセキュリティ人材発掘を目的とする現行のセキュリティ・キャンプと同様に、学生を中心として想定するものの、サイバーセキュリティ以外の特定の専門領域の高度な知見・技能を有している者を対象とすることに鑑み、高等専門学校・大学の専門課程・大学院への在籍者を中心に検討。

  ※　セキュリティ・キャンプ協議会の下にワーキンググループを設置し、新たなキャンプの令和７年度中の開催に向けて、産業界とも連携しつつ検討中。

3．新たなキャンプ（セキュリティ・キャンプ・コネクト（仮称））の実施

（2）新たなキャンプ（セキュリティ・キャンプ・コネクト（仮称））の骨子

開催イメージ

- 対象者：一定水準のサイバーセキュリティに関する知見・技能を有する者であって特定の専門領域における高度な知見・技能を有するもの（高等専門学校、大学の専門課程及び大学院の各在籍者を中心に検討）
- 全体構成：複数の専門領域に関するテーマ（ゼミ）を用意
- 受入れ人数：50人程度
- 開催期間：既存のキャンプ期間（夏休み）と重ならず、対象者が参加しやすい時期（春休みなど）を想定

対象分野の例

○AIとセキュリティ

- AIシステム・サービスの開発・提供・利用それぞれにおいて、どのようなセキュリティリスクが存在するか等をゼミ形式で議論することで、普段AIを研究・開発する立場からもセキュリティを意識して課題を討議し、AIの機密性・完全性・可用性を維持するための合理的な対策や、AIの特性を踏まえた正常な稼働に必要なシステム間の接続等を検討してもらうこと等が考えられる。

詳細制度設計については、セキュリティ・キャンプ協議会の下に設置されているワーキンググループにおいて議論をすることとしたい。

4．修了生コミュニティの整備

- 修了生がセキュリティ・キャンプへの参加で培った知識・技術・人脈を活用し、**修了年次を超えて相互に、情報交換、議論、交流、パートナーシップ構築等を行う**ことを支援するためのコミュニティを整備する。（→修了生に対する継続的な価値提供）
- **修了生の知見やノウハウを社会に還元**していくために、修了生による情報発信・普及啓発・人材育成などの活動を居住地中心に展開できるよう支援する。講師の立場としてのキャンプへの参画も促進する。（→修了生の知見の社会への還元）（→政府機関等と修了生との連携・協力）
- 修了生が**政府機関や各産業分野におけるセキュリティ対策を先導する人材**として、または、**新規ビジネスの立ち上げや新規技術の開発に携わる人材**として**活躍をしている状況を広報・PR**する。（→セキュリティ・キャンプ自体の価値向上/有効性の確認）
- **令和７年度中に修了生コミュニティを開始**すべく準備を進めていく。

コミュニティ整備の趣旨

① 修了生同士のつながりを強化し相互に知見・技能を研鑽する機会を継続的に提供すること
② 講師の立場としてのキャンプへの参画や政府機関等での活動を含め、修了生の知見・技能を社会に還元していくこと
③ 修了生の活躍状況を対外的に広報・PRすることで、セキュリティ・キャンプの取組やサイバーセキュリティ人材の価値向上につなげること

後方支援等（案）

修了生活躍状況の可視化による産業界へのアピール、裾野拡大支援、など

- 修了生対象のワークショップの開催支援
- 修了生コミュニティへの参加レポートのウェブページ公開
- 政府機関等の施策検討における意見募集・参加案内
- 修了生のキャンプ後の活躍状況のウェブページ公開　等

コミュニティの活動（案）

＊未踏事業：ITを駆使してイノベーションを創出することのできる独創的なアイディアと技術を有するとともに、これらを活用する優れた能力を持つ、突出した人材を発掘・育成することを目的としたIPAが主催する事業。

コンセプト	目的	アクション
社会体験・社会貢献機会の提供	修了生が知識・技術によって「社会に貢献できる」＝「社会での成功体験を積む」機会を獲得し研究開発のモチベーション維持に繋げる	・サイバー技術研究室への参画によるサイバー攻撃情報の調査・分析/OSS開発など ・脆弱性情報の届け出
		・情報セキュリティ10大脅威選考への参加 ・情報セキュリティ白書コラムの執筆
	修了生の地元におけるサイバーセキュリティの有識者候補として、知名度の向上と人脈形成の機会を獲得	・講師としてミニキャンプ参加 ・チューターとしてミニキャンプへ参加
情報発信・情報交換機会の提供	修了生が活動状況/研究成果を発表する機会を得る	・キャンプフォーラムへの参加
	セキュリティ・キャンプの修了年次を超えた人脈形成、および同世代のIT人材との交流機会を得る	・修了生イベントへの参加 ・未踏発企業との交流/連携 ・講師/チューターとの情報交換
知識・技能の向上	修了生の”学び欲”を満たすとともに、起業等へのステップアップも目指す	・ミニキャンプの聴講 ・修了生対象のワークショップ開催 ・未踏事業イベントへの紹介/勧誘

5．セキュリティ・キャンプに関する継続的な検討事項

（１）新たなキャンプ（セキュリティ・キャンプ・コネクト（仮称））について、骨子等を踏まえ、同キャンプの具体的な実施内容等について御議論いただきたい。

- 対象分野、産業界側のニーズ
- 参加者に求める水準、育成により目指す水準
- 講師選定、大学等との連携の在り方　等

（２）修了生コミュニティの整備について、コミュニティの活動など具体的な実施内容等について御議論いただきたい。

- 修了生同士の知識研鑽の在り方、修了生・産業界（雇用者）のニーズ
- 講師側の立場としてのキャンプ参画の促進手法
- 政府機関等と修了生との連携・協力方法
- 事務局が行うべき後方支援　等

Ⅲ　情報処理安全確保支援士（登録セキスペ）

1．登録セキスペの現状・課題・方向性
2．第２回までの主な御意見
3．施策の分類・整理
4．登録セキスペの活用促進・活躍の場の拡大
5．資格の更新コストの低減
6．登録セキスペに関する継続的な検討事項

１．登録セキスペの現状・課題・方向性

（１）2016年に資格創設後、登録者は2019年以降横ばいで推移。試験合格者のうち、６割以上は未登録。

（２）資格更新のため、３年間で少なくとも10万円以上が必要。

※　消除者のアンケート結果によると、メリットがない、金銭的な負担が大きいとのコメントあり。

（同旨 第１回検討会資料）

（１）実態を伴う活躍イメージを十分に提示できておらず、大幅な登録者数の増加につながっていない。

活躍の場がないとする登録セキスペがいる一方、人材不足を課題に上げる中小企業等もおり、ミスマッチも発生。

（２）資格更新時の高額なコストの見直しが必要。

（同旨 第１回検討会資料）

（１）

ユーザ企業における活用促進・活躍の場の拡大

（２）

資格維持コストの低減

（参考１）情報処理安全確保支援士（登録セキスペ）制度

- サイバーセキュリティの確保を支援するため、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として、「情報処理安全確保支援士」**（通称：登録セキスペ）**制度を2016年に創設。2024年10月１日時点の登録者数は22,845人。
- 2020年５月より、**登録に３年間の有効期限**を設け、**更新が行われない場合**には、**登録が失効**する**更新制を導入**。

◆ 政府機関や企業等のサイバーセキュリティ対策を強化するため、専門人材を見える化し、活用できる環境を整備することが必要。

➡ **情報処理安全支援士の名称を有資格者に独占的に使用させることとし、登録簿を整備。**

◆ 技術進歩等が早いサイバーセキュリティ分野においては、知識等が陳腐化するおそれ。

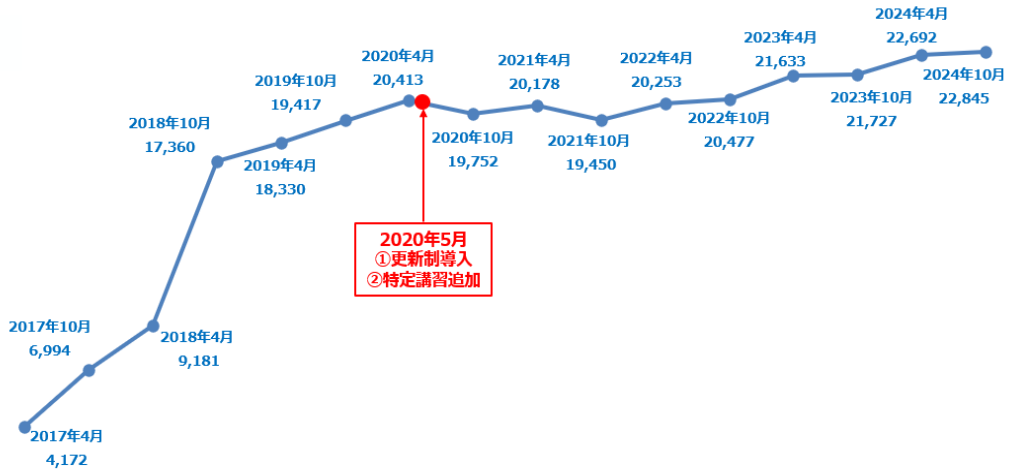
➡ **有資格者の継続的な知識・技能の向上を図るため、講習の受講を義務化。**
※登録の更新制導入により、義務講習を受講したもののみ登録を更新。

◆ 民間企業等が安心して人材を活用できるようにするには、専門人材に厳格な秘密保持が確保されていることが必要。

➡ **業務上知り得た秘密の保持義務を措置。**

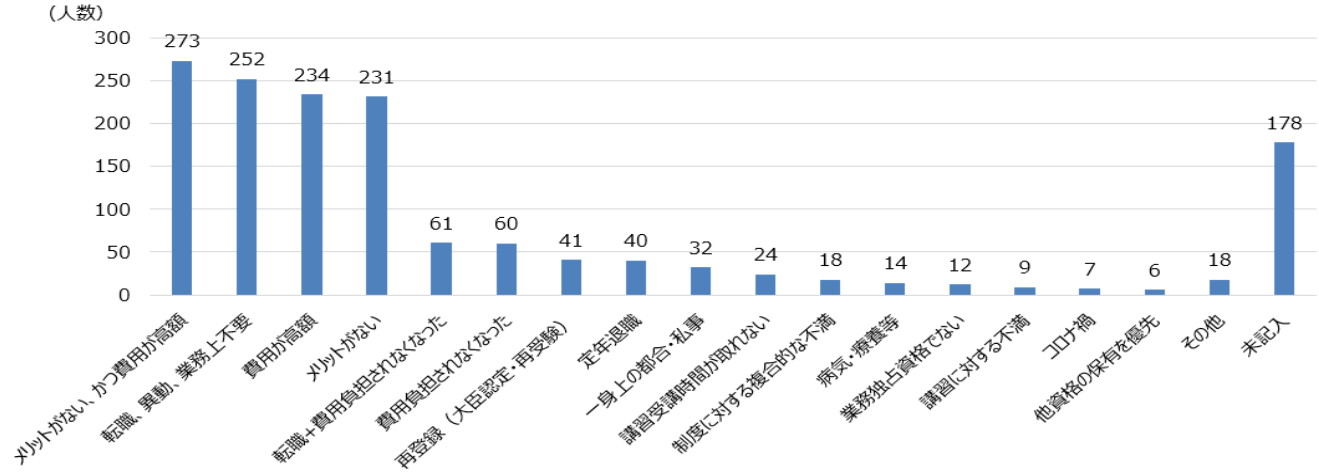
（参考２）登録セキスペの現状

登録者数



出典：https://www.ipa.go.jp/jinzai/riss/reports/data/index.html

消除理由



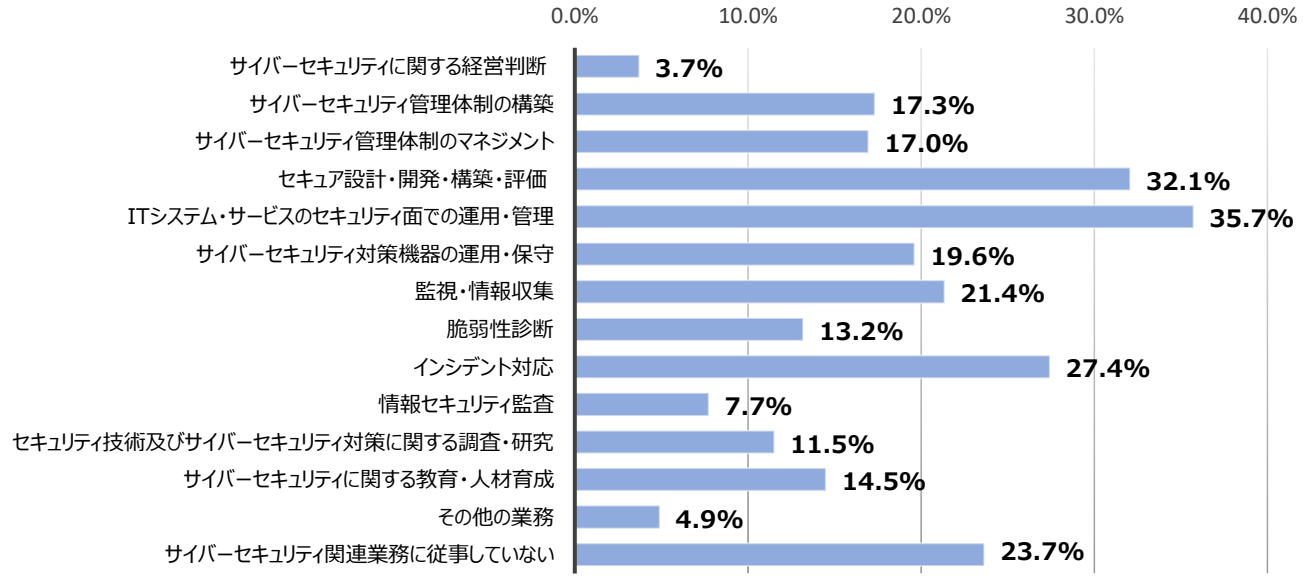
出典：情報処理安全確保支援士登録消除届出書の理由欄（任意記載項目）（2024年5月22日時点） N=1,510

業種別内訳

	人数	割合
情報処理・提供サービス業	7,346名	38.0%
ソフトウェア業	4,399名	22.7%
製造業	1,664名	8.6%
運輸・通信業	1,357名	7.0%
サービス業	878名	4.5%
官公庁、公益団体	853名	4.4%
金融・保険業、不動産業	689名	3.6%
コンピュータ及び周辺機器製造又は販売業	612名	3.2%
建設業	326名	1.7%
教育（学校、研究機関）	266名	1.4%
卸売・小売業、飲食店	213名	1.1%
電気・ガス・熱供給・水道業	180名	0.9%
医療・福祉業	97名	0.5%
調査業、広告業	48名	0.2%
農業、林業、漁業、鉱業	7名	0.0%
その他（学生、未入力など）	403名	2.1%
計	19,338名	100.0%

現状調査票に基づく内訳。回答は任意。
2022/4/1～2024/10/1の登録・更新者の集計（消除者を除く）

業務別内訳



現状調査票に基づく内訳。回答は任意。複数回答可。
2022/4/1～2024/10/1の登録・更新者の集計 N=6,693

２．第２回までの主な御意見（ユーザ企業における活用促進・活躍の場の拡大に関するもの①）

＜登録セキスペの得意分野等の開示＞

- 登録セキスペには、バランスよく各領域のスキルを一定のレベルまで習得している方と、ある領域のスキルが突出している方など様々な方がいらっしゃると理解。**どのタイプの方に対し、どのような業務が向いているかがレーダーチャート等でわかるとよいのではないか。**
- 企業や個社によって事業方針等は異なるため、**セキュリティマネジメント系の業務を担当する企業内部の人材、あるいは外部人材として補い企業内部の人材を補完する人材も必要**ではないか。
- アクティブリストについて、**登録セキスペがサイトを積極的に活用し、企業の方々が参照する仕組みを作る必要がある。**

＜ユーザー企業内部でのセキュリティマネジメント人材の不足＞

- **通常の事業会社では**、技術的な専門職の人材も一定の割合で必要との声もあるが、どちらかというと**セキュリティマネジメント系の人材の方が求められている**印象がある。
- 特定講習は技術よりのものが多く、監査やマネジメントに関するものは少数である。**技術系の講習とマネジメント系の講習のバランスが是正されるのであれば、企業での活用につながり得る。**

2．第２回までの主な御意見（ユーザ企業における活用促進・活躍の場の拡大に関するもの②）

＜サイバーセキュリティ対策促進制度との連動＞

- **企業類型によって登録セキスペの使い方や役割が異なる**。大企業や重要インフラ事業者等であれば社内で登録セキスペを抱えた方がよいし、中小企業や小規模企業では外部から登録セキスペを調達することになるであろう。
- 登録セキスペ相当の技術があれば資格自体は不要、ユーザー企業にとって有資格者が不可欠でない限り登録セキスペを活用しないとの指摘もあったところ。そうした点を踏まえ、登録セキスペの更なる登録者数拡大に向けて、**「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」と連携**するよう検討いただけるとよい。
- 重要インフラを扱うような事業者については、セキュリティ対策の中身等についても理解している必要があるので、登録セキスペが企業内部に一人以上は置かれるべきという位置づけは納得感がある。

＜中小企業の外部アドバイザーとしての活躍＞

- 中小企業等では登録セキスペを社内で抱えきれないため、**外部のアドバイザーとして活用することも想定**される。
- 中小企業の方々がガイドラインだけで自ら対策を実施するのは現実的には難しいため、**何をどのように実施するかなどを登録セキスペがサポートできるような仕組みが必要**であり、政府としても強くメッセージを出していくことが重要である。
- DX を推進している部署や団体を巻き込み、第１回検討会の資料 4の**「登録セキスペと中小企業等とのマッチング事業」**にあるような活動を推進されたい。

２．第２回までの主な御意見（資格維持コストの低減に関するもの）

＜資格維持メリット強化の重要性＞

- 登録セキスペ資格を更新しない理由として、**特にメリットがないとされている点が重要**であり、資格の登録にも影響していると考えられる。
- 費用が高いから継続しないということと、費用を安くすれば継続するということは必ずしもイコールではない。施策として安全な方法は、**メリットを増進することが重要**に思われる。

＜更新講習の「みなし受講」制度の導入＞

- 大学の社会人向け講座を受講している登録セキスペの方からは、普段から勉強していることが認められないのは残念とのご意見をいただくことがある。実際に、大学の社会人向け講座には実践的な要素も含まれており、そうした講座を受講されている方は普段からサイバーセキュリティ関連情報を収集しているが、資格継続の役に立っていない。**そのような経験が資格継続に認められる制度があるとよい**。
- 更新について他の制度と比較すると、セキュリティプロフェッショナル認定資格制度（CISSP） や公認内部監査人（CIA） の場合は、更新する上での選択肢が多く、外部のイベントで有資格者の仲間に出会う。そうした**外部のイベントでは、学習の場があり知識の維持向上がなされ**、コミュニティも形成されており、メリットになっている。
- 登録セキスペ義務講習の免除対象を、セキュリティに関する実務要件を課している他の資格にも拡大してはどうかとの意見の中で、CISSPのポイント利用について言及があったが、国家資格である登録セキスペ制度が他国の民間の枠組みに乗るのは適切ではないのではないか。
- 基準をどうするかという点が重要である。例えば、実務経験に基づく更新については、実務経歴書等を提出させて終わりとするのではなく、それらを事務局でチェックする形になるのではないか。

3．登録セキスペに係る施策の分類・整理

主な課題

- 実態を伴う活躍イメージの提示が不十分
- 社会からの評価が不十分
- 活躍の場の確保が不十分（活躍の場が限定）

- 中小企業等ではセキュリティ人材が不足しており、人材のミスマッチが発生

- 資格更新時のコストが高額

市場への働きかけ

登録セキスペの能力向上、スキル・実績の見える化

- 登録セキスペアクティブリスト整備
- デジタル人材育成・DX推進プラットフォームの整備
- 戦略マネジメント層向け講習の拡大
- 監査スキル強化機会の提供

連携・反映　活用

企業と登録セキスペのマッチング促進

（※）令和６年度予算事業にて実証中

活用　紹介　動機付け

- 各種専門家派遣策 中小企業向け支援策
- 中堅・中小企業が実施する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（β版）

更新コストの低減

- 更新講習（一部）のみなし受講制度の創設
- オンライン講習の一部簡素化

企業側（活用側）への働きかけ

ユーザー企業における登録セキスペの活用

- 公的機関・重要インフラ事業者等における配置促進
- 各種投資促進施策における要件化（●）
- 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）
- サイバーセキュリティ対策促進制度における活用（サプライチェーン対策評価制度、IoTセキュリティ適合性評価制度 等）

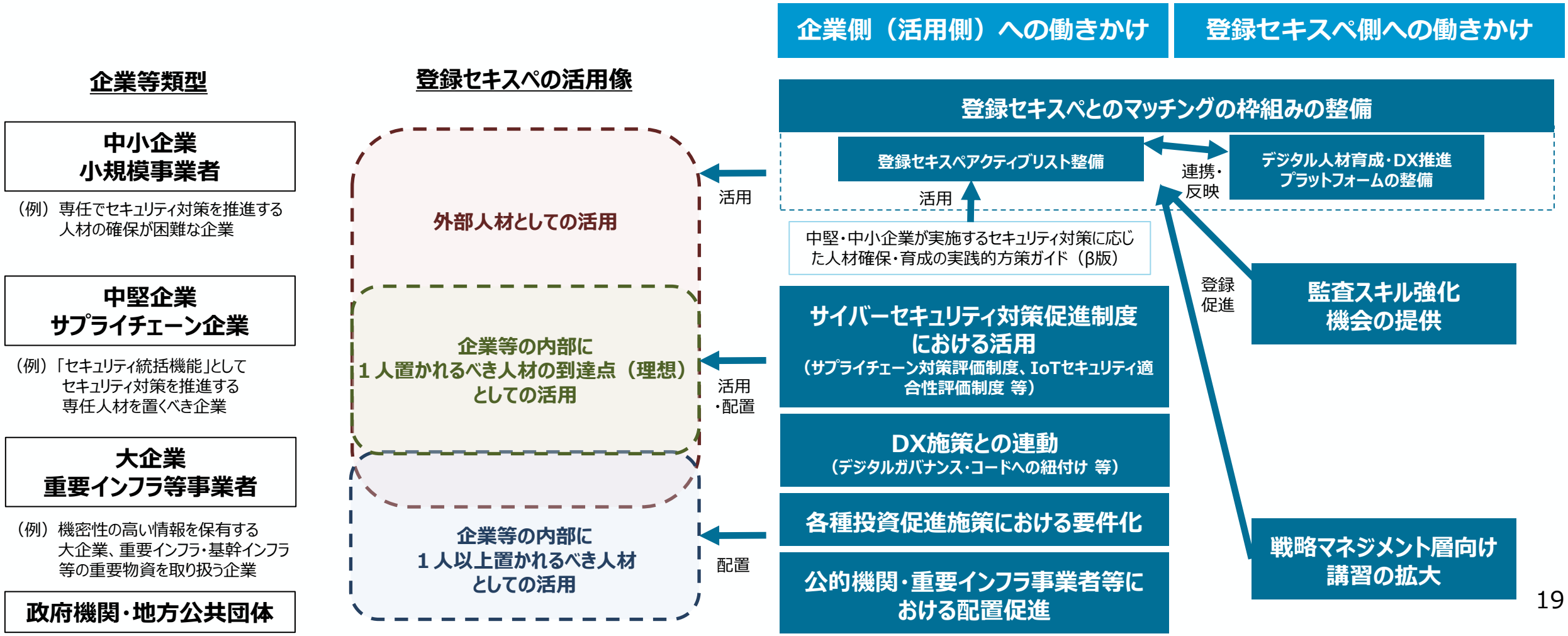
（●）：既に取り組んでおり今後も継続的に実施するもの

施策により期待される効果

- 企業等（特にユーザー企業）における**登録セキスペの活用が促進**され、その**スキル・実績が社会的に評価**されるようになる。
- そうした**評価に見合った報酬**を期待しつつ、**負担コストも低減**させる（2030年までに登録セキスペ登録者数５万人を達成）。
- 上記のほか、登録セキスペの能力向上等に伴い、セキュリティビジネス振興にも寄与。

4．登録セキスペの活用促進・活躍の場の拡大（施策の全体像）

- **企業等の類型によって登録セキスペに求められる役割は異なる**という点に鑑み、**中小企業等向けにはアクティブリストの整備を通じたマッチング枠組みの整備、中堅企業～大企業向けには各種対策促進制度との連動**、をそれぞれ検討。
- アクティブリストの活性化に向け、**登録セキスペに対するスキル強化・多様化につながる機会**を検討。



４．登録セキスペの活用促進・活躍の場の拡大

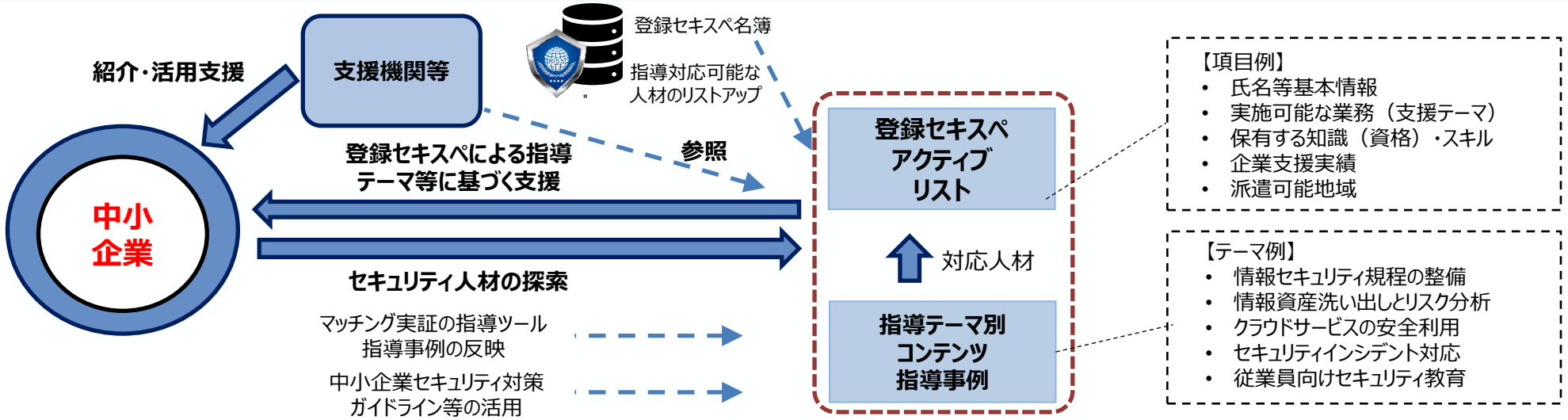
４－１．アクティブリスト・中小企業等とのマッチングの枠組みの整備

- 令和７年度に、**登録セキスペの得意分野・専門領域を可視化**するため、**登録セキスペのリスト（アクティブリスト）整備**を行う。

※令和５年度補正予算事業において、特定の地域で商工会議所等と連携した中小企業等へのマネジメント指導を実施。どのような項目を可視化することが効果的か、中小企業とのマッチングを促すためにどのような働きかけが必要か、自走化の（予算支援を必要としない）ためにどのような仕組みが必要か等について実証事業を通じて知見を蓄積し、上記アクティブリストの整備に活かす。

※本枠組みの活用促進に向けて、商工会議所等の中小企業支援機関や（一社）情報処理安全確保支援士会等の関係団体と連携し、アクティブリストの活用・管理手法について検討を実施。その他、各種中小企業向け支援策との連携や、「中堅・中小企業が実施する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（β版）」での参照等も検討。

- これにより、人材不足に悩む**中小企業等が、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アクティブリストに掲載の**登録セキスペを外部人材として活用することができる**と同時に、**登録セキスペにとっても活躍の機会が確保**されることが期待。

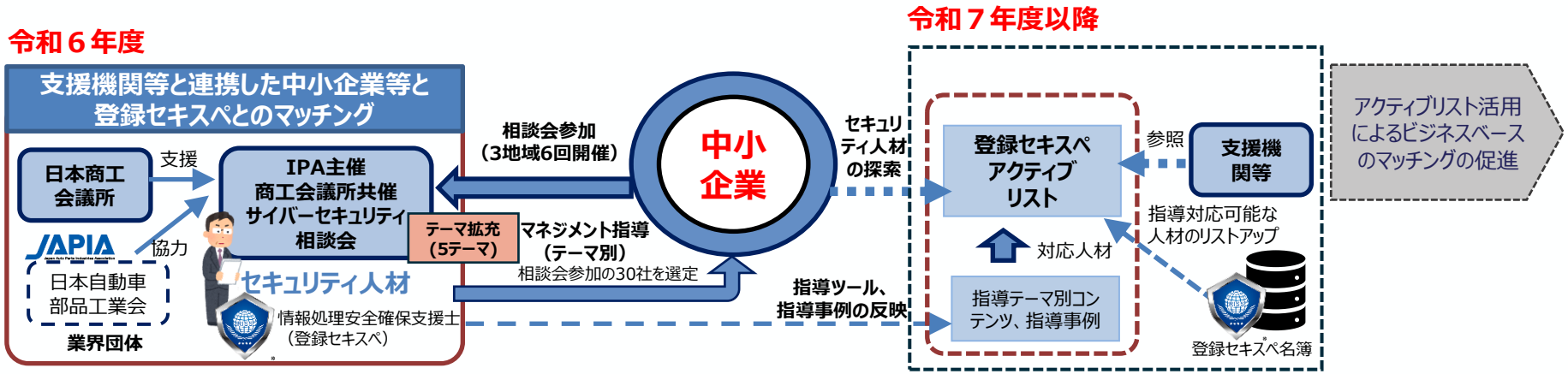


（参考１）令和５年度補正予算事業（セキュリティ人材活用促進事業）

- 商工会議所等の**支援機関等を通じた効果的な登録セキスペの広報周知の方法**や、**中小企業と登録セキスペの効率的なマッチング方法**について検証。
- 全国各地の多様な**支援機関等が当該場の提供を国費に頼らず自前で実施できるような**（＝支援機関等がマッチング裨益者から対価を得られる）**方策**についても模索。

事業概要

- 支援機関（商工会議所）等と連携した中小企業向けサイバーセキュリティ相談会を３地域計６回開催。
- 相談会参加の中小企業等30社程度に対して、登録セキスペによるマネジメント指導を実施。
- 中小企業等のセキュリティコンサルが対応可能な登録セキスペのリスト（アクティブリスト）について検討。



（参考２）登録セキスペのマネジメント指導テーマ

※令和５年度補正予算事業における実証事業にて検証中

指導テーマ	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
どういった企業に受けてもらいたいか	**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。
マネジメント指導により期待される効果	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。

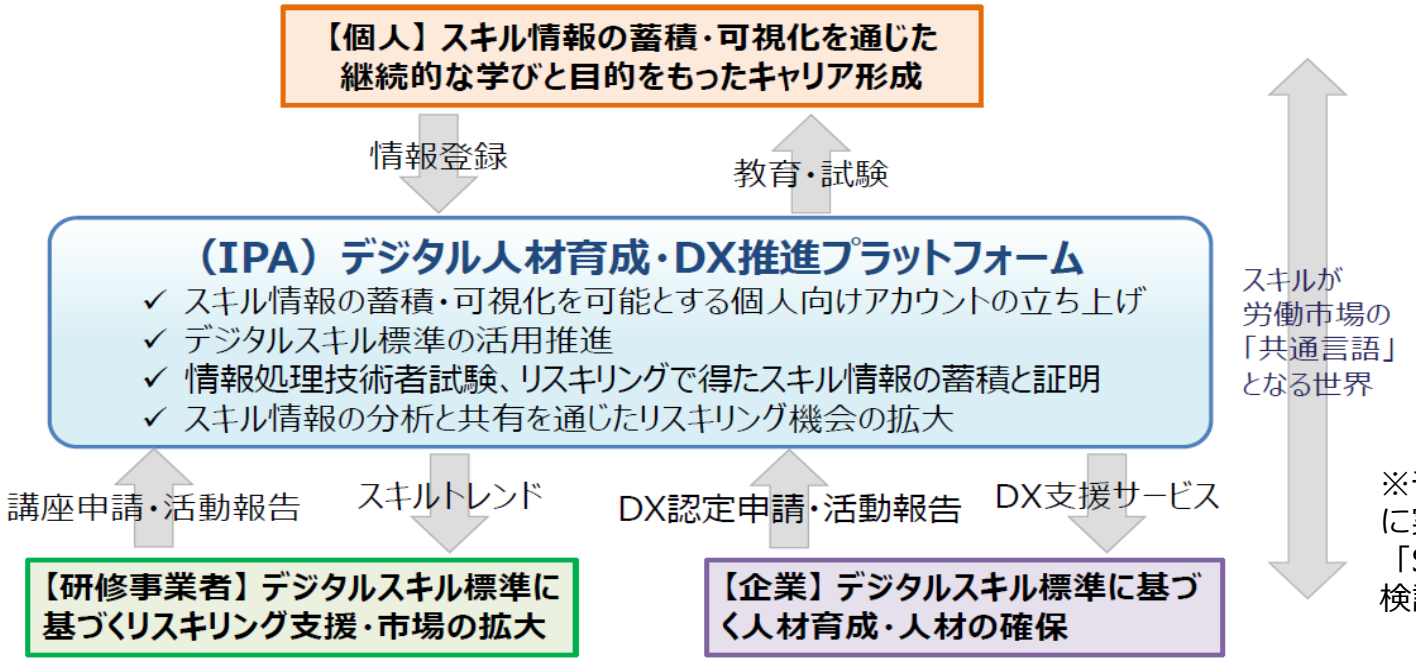
4．登録セキスペの活用促進・活躍の場の拡大

4－2．登録セキスペ側への働きかけ

①デジタル人材育成・DX推進プラットフォームの整備

- 登録セキスペ自身が、現状の知識やスキルの修得度合いを把握し、自分の希望するキャリアパスに対して、何が不足しているのかが可視化され、その不足分を補うような講習や実務経験等を選ぶことができるよう、**IPAに実装されるデジタル人材育成・DX推進プラットフォームと連動する取組**を検討。前述の**アクティブリストとの連携**も想定。
- これにより、**登録セキスペの能力向上及びスキル・実績の見える化が促進**され、そうしたスキル情報等がアクティブリストに反映されることにより、同リストの改善ひいては中小企業等による活用の促進につながることが期待される。

<参考：デジタル人材育成・DX推進プラットフォームのイメージ>



※デジタル人材育成・DX推進プラットフォームに実装される具体的機能については、「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、別途議論予定。

４．登録セキスペの活用促進・活躍の場の拡大

４－２．登録セキスペ側への働きかけ

②監査スキル強化機会の提供

- 令和７年度に、登録セキスペに対して**セキュリティ監査スキルの向上に向けた研修機会を提供**する。　※研修受講履歴は、アクティブリストへの反映も想定。
- **取引企業先に信頼性を示していく必要があるサプライチェーン上の企業の情報セキュリティ監査に対するニーズの増加が予想される**中、この取組により、当該**ニーズに応えることができる登録セキスペの供給力を強化**することで、より幅広い企業との**マッチングが促進**され、登録セキスペの活躍機会の拡大が期待される。

③戦略マネジメント層向け講習の拡大

- **企業内のセキュリティ専門家＊の養成につながる講習を増加**させるための方策を検討。　※講習受講履歴は、アクティブリストへの反映も想定。

  ＊ ①セキュリティガバナンスの確保（国内外・同業他社のインシデント把握等の情報収集・リスク分析・提案を含む）②社内のセキュリティ対策の推進（方針策定、教育・インシデント対応等の実務）等の役割を担い、経営層と担当者（情報システム部門、事業部門、管理部門等）をつなぐ者（戦略マネジメント層）。

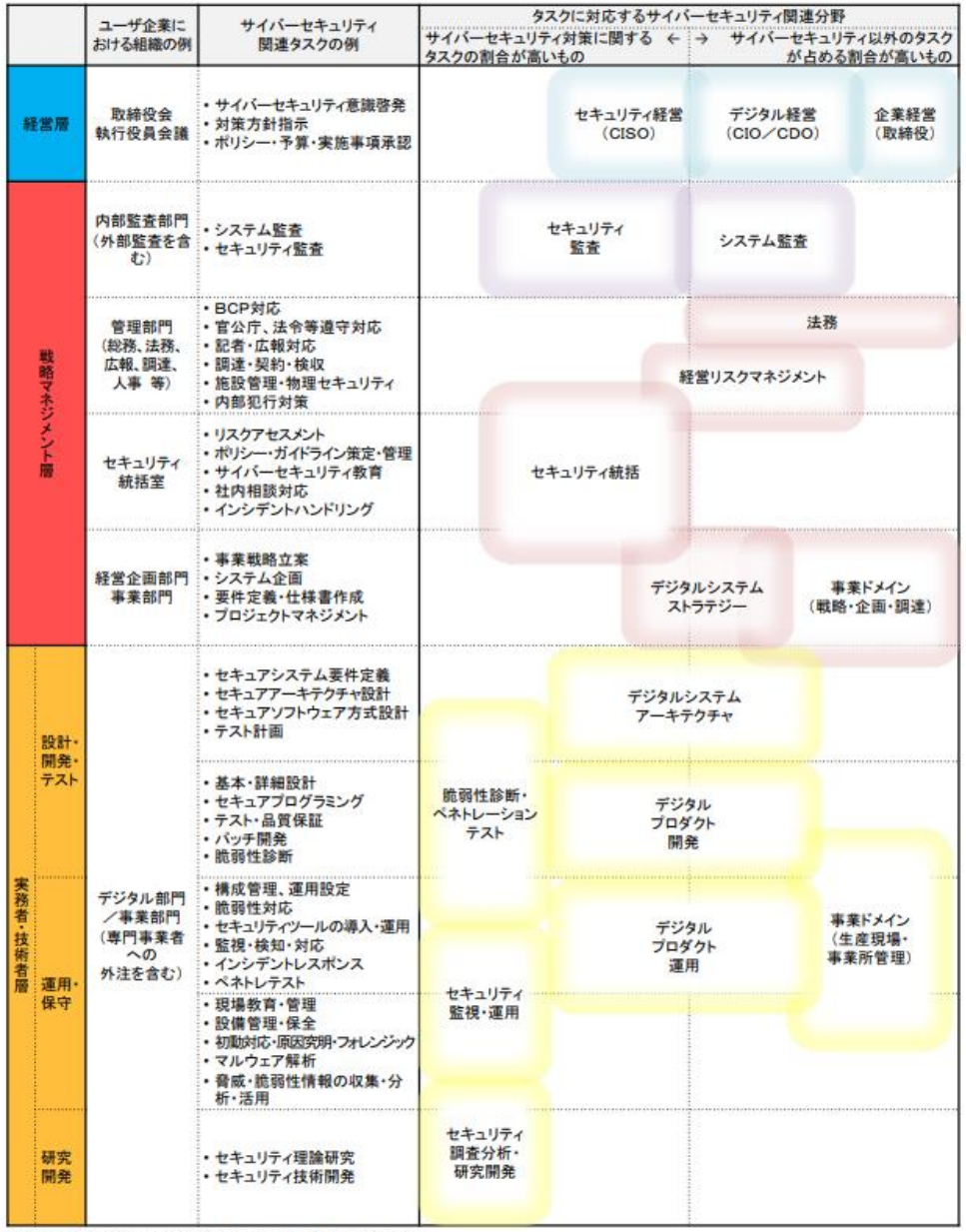
- **ユーザー企業内部において**、企業におけるリスクマネジメント活動の一部として、自社のサイバーセキュリティリスクを把握し必要な意思決定や管理を行い、対策を推進する**登録セキスペの増加・活用促進**を進める。

＜参考：現在提供されている特定講習の分類＞

ITSS＋（セキュリティ領域）	講習数
セキュリティ監視・運用 • 監視・検知・初動対応・原因究明、インシデントレスポンス	20
セキュリティ調査分析・研究開発 • 脅威情報の収集・分析、デジタルフォレンジック、セキュリティ技術開発	19
脆弱性診断・ペネトレーションテスト • 脆弱性診断の実施、ペネトレーションテストの実施	6
セキュリティ統括 • リスクアセスメント、ポリシー・ガイドライン策定・管理、サイバーセキュリティ教育・社内相談対応、インシデントハンドリング	2

（参考）ITSS＋（セキュリティ領域）

図表6 ITSS＋（セキュリティ分野）で定義されている17分野



※クラウド、アジャイル、DevSecOps等により境界は曖昧化の傾向
※チップ/IoT・組み込み/制御システム/OS/サーバ/NW/ソフト/Web等の取扱う技術の種類や事業分野によりタスクやスキルは大きく異なる

図表7 ITSS＋（セキュリティ分野）で定義されている17分野毎のタスク例

	分野名	サイバーセキュリティ関連タスクの例
経営層	セキュリティ経営（CISO） デジタル経営（CIO/CDO） 企業経営（取締役）	● サイバーセキュリティ意識啓発 ● 対策方針の指示 ● セキュリティポリシー・予算・対策実施事項の承認 等
戦略マネジメント層	セキュリティ監査	● 情報セキュリティ監査、報告・助言 等
	システム監査	● システム監査、報告・助言 等
	セキュリティ統括	● サイバーセキュリティ教育・普及啓発 ● サイバーセキュリティ関連の講義・講演 ● サイバーセキュリティリスクアセスメント ● セキュリティポリシー・ガイドラインの策定・管理・周知 ● 警察・官公庁等対応 ● 社内相談対応 ● インシデントハンドリング 等
	デジタルシステムストラテジー	● デジタル事業戦略立案 ● システム企画 ● 要件定義・仕様書作成 ● プロジェクトマネジメント 等
	経営リスクマネジメント	● 経営リスクマネジメント ● BCP／危機管理対応 ● サイバーセキュリティ保険検討 ● 記者・広報対応 ● 施設管理・物理セキュリティ ● 内部犯行対策 等
	法務	● デジタル関連法令対応 ● コンプライアンス対応 ● 契約管理 等
	事業ドメイン（戦略・企画・調達）	● 事業特有のリスクの洗い出し ● 事業特性に応じたサイバーセキュリティ対応 ● サプライチェーン管理 等
実務者・技術者層	脆弱性診断・ペネトレーションテスト	● 脆弱性診断、ペネトレーションテスト 等
	セキュリティ監視・運用	● セキュリティ製品・サービスの導入・運用 ● セキュリティ監視・検知・対応 ● インシデントレスポンス ● 連絡受付 等
	セキュリティ調査分析・研究開発	● サイバー攻撃捜査、原因究明・フォレンジック ● マルウェア解析、脅威・脆弱性情報の収集・分析・活用 ● セキュリティ理論・技術の研究開発 ● セキュリティ市場動向調査 等
	デジタルシステムアーキテクチャ	● セキュアシステム要件定義 ● セキュアシステムアーキテクチャ設計 ● セキュアソフトウェア方式設計 ● テスト計画 等
	デジタルプロダクト開発	● 基本設計、詳細設計 ● セキュアプログラミング ● テスト・品質保証 ● パッチ開発 等
	デジタルプロダクト運用	● 構成管理 ● 運用設定 ● 利用者管理 ● サポート・ヘルプデスク ● 脆弱性対策・対応 ● インシデントレスポンス 等
	事業ドメイン（生産現場・事業所管理）	● 現場教育・管理、設備管理・保全、QC活動 ● 初動対応 等

4．登録セキスペの活用促進・活躍の場の拡大

4－3．企業側（活用側）への働きかけ

①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での活用

- サプライチェーン上の中堅・中小企業（受注者）が取引先（調達者）からの要請に応えるために、将来、本制度を活用して一定水準（例：三つ星（★３））のサイバーセキュリティ対策を満たす旨を自己宣言する際、必要に応じて外部のセキュリティ専門家の助言や検証を受けることを想定。その際、**外部の専門家として、登録セキスペが積極的に活用される**よう、本制度の設計に当たって（登録セキスペの位置付けを明確化するなど）配意する方向で検討する。
  ※当該中堅・中小企業への支援が可能な旨や実績等については、アクティブリストに反映も想定。
- これにより、**サプライチェーンに属する中堅・中小企業におけるセキュリティ対策を支援する専門家として**の、**登録セキスペの活躍機会の確保**が期待される。

<参考：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イメージ>

成熟度の定義	三つ星（★３）	四つ星（★４）	五つ星（★５）
レベル感の説明	サプライチェーン形成企業として最低限満たすべき基準	サプライチェーン形成企業として標準的に満たすべき基準	重要インフラ事業者、経済安全保障上、特に重要なインフラ事業者、関連サプライヤーが満たすべき基準
ガイドラインの相当性を認定	・IPA「中小企業の情報セキュリティ対策ガイドライン」	・○○業界ガイドライン ・・・・	・重要インフラ行動計画 ・・・・
ガイドライン準拠を確認する方法を定義	自己宣言型	第三者認証型	第三者認証型

（出典）第８回 産業サイバーセキュリティ研究会　資料３より抜粋・加工

政府調達・補助施策等への要件化

取引先からの対策要請による活用促進

利害関係者への情報開示による対話の促進

4．登録セキスペの活用促進・活躍の場の拡大

4－3．企業側（活用側）への働きかけ

②IoTセキュリティ適合性評価制度での活用

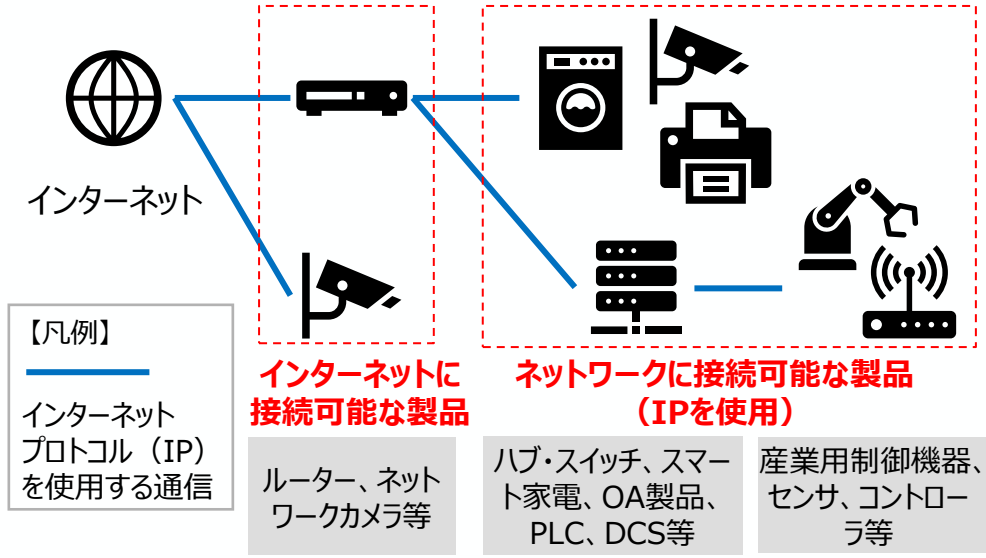
- 本制度の運用設計に当たり、IoT製品に求められるセキュリティ水準に応じた複数の**適合性評価レベルの評価を行う指定資格者として登録セキスペを活用**していく方向で検討。※当該評価が可能な旨や実績等については、アクティブリストに反映も想定。
- これにより、 **IoT製品の評価レベルの評価を行う専門家としての登録セキスペの活躍機会**を確保。

＜参考：IoT製品に対するセキュリティ適合性評価制度の概要（制度名称・ロゴ・ラベル／対象製品の概要／制度の概要（イメージ））＞

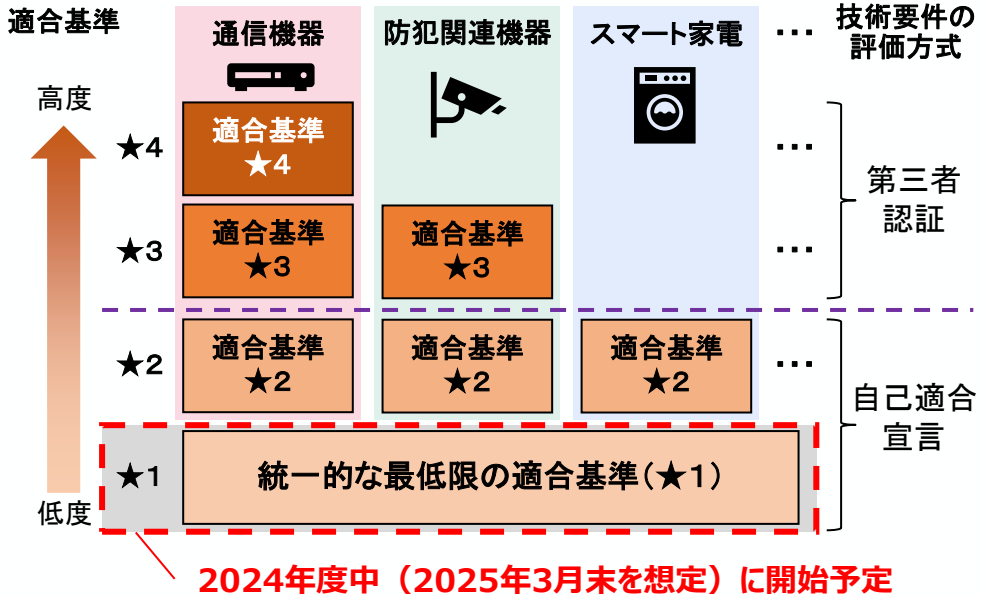
セキュリティ要件適合評価
及びラベリング制度
JC-STAR
(Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements)

JC-STAR

JAPAN CYBERSECURITY LABEL
ジャパン・サイバーセキュリティ・ラベル
★★★★
JC-STAR
Registered ID: 01234567890123456
Information-technology Promotion Agency, JAPAN (IPA)



※ 国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的なIT製品（パソコン、タブレット端末、スマートフォン等）は対象外とする。



4．登録セキスペの活用促進・活躍の場の拡大

4－3．企業側（活用側）への働きかけ

③DX施策との連携

- **企業のDX推進に関連する各種文書に登録セキスペの活用・配置を紐づけていく**。既に、例えば、**デジタルガバナンス・コード**の最新の改訂において、サイバーセキュリティ対策の体制構築に向けた取組として、**情報処理安全確保支援士（登録セキスペ）の取得を明記**。本コードを踏まえて、DX銘柄やDX認定の基準も設定される。
- これにより、**DXを促進する企業の内部で、サイバーセキュリティリスクに対応できる体制の構築に向けた取組を推進する人材として**登録セキスペの活躍機会が拡大することが期待される。

○デジタルガバナンス･コード3.0 ～DX経営による企業価値向上に向けて～（2024年９月19日改訂）（抜粋）

３－３．ITシステム・サイバーセキュリティ
（２）望ましい方向性

- 経営者がサイバーセキュリティリスクを経営リスクの一つとして認識し、CISO等の責任者を任命するなど管理体制を構築するとともに、サイバーセキュリティ対策のためのリソース（予算、人材）を確保している。
- サイバーセキュリティリスクとして守るべき情報を特定し、リスクに対応するための計画（システム的・人的）を策定するとともに、防御のための仕組み・体制を構築している。
- 自社のサイバーセキュリティリスクを評価するために、システム監査やセキュリティ監査など第三者監査を実施している。
- サイバーセキュリティリスクに対応できる体制の構築に向けた取組として、**情報処理安全確保支援士（登録セキスペ）の取得や外部人材の活用、社員への教育等を企業として進めている**。
- サイバー攻撃による被害を受けた場合の事業継続計画（BCP）を策定するとともに、経営陣も含めて緊急対応に関する演習・訓練を実施している。
- サプライチェーンの保護に向けて、取引先や調達するITサービス等提供事業者のサイバーセキュリティ対策の強化を促しつつ、サプライチェーン全体での付加価値の向上に取り組んでいる。

（参考）デジタルガバナンス・コード3.0の全体像

- 経営者が**DXによる企業価値向上の推進のために実践することが必要な事項**をとりまとめ。
- 改訂版では、**①DX経営による企業価値向上に焦点を当てた経営者へのメッセージとDX経営に求められる３つの視点を追加**するとともに、②データ活用・連携、デジタル人材の育成・確保、サイバーセキュリティ等の論点を反映しつつ、**柱立ての名称・構成を大幅に見直し**。

柱立て	柱となる考え方（概要）
1. 経営ビジョン・ビジネスモデルの策定	➢ データ活用やデジタル技術の進化による社会及び競争環境の変化が自社にもたらす影響も踏まえて、経営ビジョン及び経営ビジョンの実現に向けたビジネスモデルを策定する。
2. DX戦略の策定	➢ データ活用やデジタル技術の進化による社会及び競争環境の変化も踏まえて目指すビジネスモデルを実現するための方策としてDX戦略を策定する。
3. DX戦略の推進	
3-1. 組織づくり	➢ DX戦略の推進に必要な体制を構築するとともに、外部組織との関係構築・協業も含め、組織設計・運営の在り方を定める。
3-2. デジタル人材の育成・確保	➢ DX戦略の推進に必要なデジタル人材の育成・確保の方策を定める。
3-3. ITシステム・サイバーセキュリティ	➢ DX戦略の推進に必要なITシステム環境の整備に向けたプロジェクト等を明確化する。 ➢ 事業実施の前提となるサイバーセキュリティリスクに対して適切な対応を行う。
4. 成果指標の設定・DX戦略の見直し	➢ DX戦略の達成度を測る指標を定め、指標に基づく成果についての自己評価を行う。 ➢ 事業部門や ITシステム部門等とも協力し、デジタル技術に係る動向や自社のITシステムの現状を踏まえた課題を把握・分析し、DX戦略の見直しに反映する。
5. ステークホルダーとの対話	➢ 経営ビジョンやビジネスモデル、DX戦略等について、「価値創造ストーリー」として投資家をはじめとした適切なステークホルダーに示す。 ➢ DX戦略の実施に当たり、ステークホルダーへの情報発信を含め、リーダーシップを発揮する。

4．登録セキスペの活用促進・活躍の場の拡大

4－3．企業側（活用側）への働きかけ

④各種投資促進施策への紐付け（補助施策における登録セキスペの要件化）

- **経済産業省の各種補助施策において登録セキスペの配置を要件化**していく。例えば、既に、直近の投資促進施策（以下）においても登録セキスペの配置を要件としている。
- これにより、規模拡大や新事業創出など積極的な投資を行う大企業等において、当該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ペの活用促進**を図る。

● 令和５年度補正グローバルサウス未来志向型共創等事業費補助金におけるサイバーセキュリティ要件（抜粋）

- ２．補助対象事業が工場に係るものについて、サイバーセキュリティの対処（※）が適当か
  ※サイバーセキュリティの対処とは、「**サイバーセキュリティの確保に関する運用を的確に行うに足りる知識及び技能を有する者として、情報処理安全確保支援士又はこれと同等以上の知識及び技能を有すると認められる者を配置又は活用していること**及び①サイバーセキュリティの確保のための管理体制について、第三者認証（ISO 27001）を取得し、維持していること、もしくは②定期的に、サイバーセキュリティに関する外部監査等（当該監査を受けられないやむを得ない事情がある場合は、外部監査に準じた措置として組織内において講じるものを含む。）を実施するとともに、当該外部監査等の結果に基づき、サイバーセキュリティ対策の改善を行っていること。」を指す。

● 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けるサイバーセキュリティ要件（抜粋）

- サイバーセキュリティの確保に関する運用を的確に行うに足りる知識及び技能を有する者として、**情報処理安全確保支援士又はこれと同等以上の知識及び技能を有すると認められる者を配置していること**【配置している資格等保有者のリスト】

４．登録セキスペの活用促進・活躍の場の拡大

４－３．企業側（活用側）への働きかけ

⑤公的機関・重要インフラ事業者における配置促進

- 今後、政府機関等の対策基準策定のためのガイドラインにおける記載ぶりを参考としつつ、**政府機関、地方自治体、重要インフラ等における登録セキスペの活用を促していくための方策を検討**。
- これにより、政府機関、地方自治体公的機関、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、登録セキスペの活躍機会の確保を目指す。

○政府機関等の対策基準策定のためのガイドライン（令和５年度版）（抜粋）

- 遵守事項 2.1.1(5)(a)「最高情報セキュリティアドバイザー」について
  - ✓ 最高情報セキュリティ責任者は、情報セキュリティに関する技術的事項等について自ら及び最高情報セキュリティ副責任者への助言等を含む機関等の情報セキュリティ対策への助言、支援等を行う者として最高情報セキュリティアドバイザーを置く。最高情報セキュリティアドバイザーは、機関等における情報システムに関する技術的事項、情報セキュリティインシデントへの対処その他の情報セキュリティ対策に対する助言・支援を担うため専門的な知識及び経験を有した者、すなわち**情報セキュリティに関する資格（情報処理安全確保支援士等）及び実務経験を有する者**である必要がある。

- 遵守事項 4.1.2 情報システムに係る業務委託
  - ✓ 情報システムセキュリティ責任者は、以下の内容を全て含む情報セキュリティ対策を実施することを情報システムに関する業務委託の委託先の選定条件に加え、仕様にも含めること。
    - A) 委託先企業若しくはその従業員、再委託先又はその他の者によって、情報システムに機関等の意図せざる変更が加えられないための管理体制
    - B) 委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（**情報セキュリティに係る資格（情報処理安全確保支援士等）**・研修実績等）・実績及び国籍に関する情報提供

5．資格の更新コストの低減（施策の全体像）

①更新講習（一部）のみなし受講制度の創設

- 令和８年度を目途に、実際に企業等においてサイバーセキュリティ関連業務に従事している等、**所定の実務に当たっている登録セキスペについて**は、資格更新のために同様の内容の講習を受ける負担を軽減させるべく、本人の申請により、**更新講習の一部の受講を免除**することを検討。

※情報処理の促進に関する法律施行規則（平成28年経済産業省令第102号）の改正により対応することも想定。

- これにより、更新時の負担軽減に加えて、前述の**「登録セキスペの活用促進・活躍の場の拡大」に掲げる各種制度や企業内部におけるセキュリティ実務等に携わる登録セキスペが増加する**ことも期待。

②オンライン講習の一部簡素化

- 上記①の創設と並行して、更新講習の一部である**「オンライン講習」の一部簡素化**を進め、すべての登録セキスペにとって、更新のために必要となる**講習の受講費用を一定程度低減**させることを検討。

※具体的な簡素化の方策（一部内容の省略、回数の減等）については、今後、IPAによる講習の提供のために必要なコストも踏まえながら検討。

５－１．更新講習（一部）のみなし受講制度の創設

（１）更新制度・講習の趣旨

- サイバーセキュリティ分野で必要とされる知識及び技能は、技術進歩や社会情勢の変化により時々刻々と変化していることを踏まえ、登録セキスペの**試験合格後においても、試験合格時の知識及び技能を維持することを目的として**、登録セキスペには、**講習の受講義務が設けられている**。
- また、登録セキスペは、公的機関、民間事業者等の情報処理の安全性及び信頼性の確保を支援するため、そのシステムの設計・開発・管理や人的体制の整備・管理に深く関わる業務を行うことが想定されているところ、**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、**登録セキスペの資質を担保するために講習を受講することが資格更新の要件とされている**。

○情報処理の促進に関する法律（昭和45年法律第90号）
（受講義務）
第二十六条　情報処理安全確保支援士は、経済産業省令で定めるところにより、機構の行うサイバーセキュリティに関する講習（第二十八条において「機構の講習」という。）又はこれと同等以上の効果を有すると認められる講習として経済産業省令で定めるもの（同条において「特定講習」という。）を受けなければならない。

○情報処理の促進に関する法律施行規則（平成28年経済産業省令第102号）
（登録の更新）
第十九条の二　法第十五条第二項の更新（以下単に「更新」という。）を受けようとする情報処理安全確保支援士は、更新の期限の日の六十日前までに、法第二十六条に基づいて機構の講習又は特定講習を修了し、様式第八による登録更新申請書を経済産業大臣に提出しなければならない。
２～３（略）

5－1．更新講習（一部）のみなし受講制度の創設

（2）オンライン講習と実践・特定講習それぞれの意義

オンライン講習

登録セキスペとして必要とされる倫理面・最新知識等を身に付けるための講習

- セキュリティの国家資格として有すべき責務や倫理について学ぶことができる
- 設計・開発・運用の各段階において、セキュリティを組み込むために行うべき内容がわかる
- セキュリティの提案・指導・助言する際にその根拠となるガイドライン、事例を示すことができる
- IT環境、技術、法令の変化に対応してどのようなセキュリティ対策をすればよいか学ぶことができる

最新知識の習得のみならず、国家資格としての登録セキスペのあるべき姿や果たすべき役割について提示するものであることから、**すべての登録セキスペが共通的に受講する必要**がある

実践・特定講習

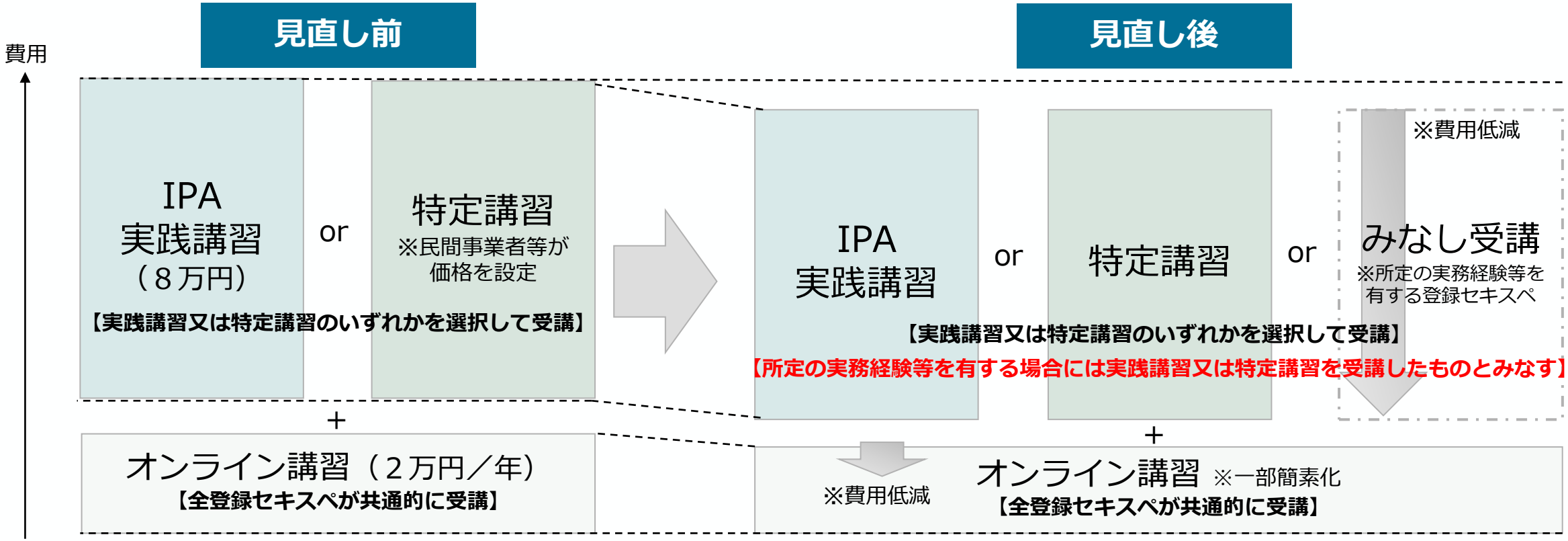
登録セキスペとして必要とされる実践的な能力を身に付けるための講習

- インシデント発生時の対応や予防策、新規事業企画の際のセキュリティリスク洗い出しや対策に関する検討、助言など、実践的な対応方法を学ぶことができる
- 「教科書的な判断」だけでは対応できない、実際に起こり得る課題に対しての対処方法を学べる
- 様々な地域や所属組織、異なる立場の登録セキスペの意見交換により新たな気づきを得ることができる

提供されている講習の内容と同等以上の内容の実務をより実践的な形式で行っている登録セキスペにとって、実践・特定講習の受講義務は、必要以上の負担となっていると評価されることから、**そうした者について受講を免除することは相当**である

5－2．資格の更新コストの低減（見直し前後のイメージ）

- 登録セキスペに関する政策課題の一つとして、更新に係る費用負担の高さが挙げられる。具体的には、資格を更新するに際して、講習の受講が義務付けられているところ、これらの**講習の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、その金額は少なくない。**
- 所定の実務経験等を有する場合において、講習を受講したものとみなす措置（みなし受講）、講習の一部簡素化等による講習費用低減により、**登録セキスペの資格維持にかかる負担を軽減していく。**



６．登録セキスペに関する継続的な検討事項（詳細は次頁以降参照）

（１）登録セキスペアクティブリストの在り方・活用促進ついて御議論いただきたい。

- （中小企業や、仲介者である支援機関等の視点に即した）アクティブリストに掲載されるべき登録セキスペに関する情報項目
- （中小企業、支援機関等、登録セキスペに）アクティブリストが活用されるための方策
- 仲介者である支援機関等が自主事業としてアクティブリストを活用するための環境整備　等

（２）更新講習の「みなし受講」の対象とする実務経験の範囲や判断方法について御議論いただきたい。

- 企業内外でのサイバーセキュリティ関連業務（実践的業務）の内容を評価する方策
- 実践的業務に当たらない活動（論文執筆、セミナー参加、大学での講義等）の許容範囲
- 客観性を担保して事務負担を抑制することができる「みなし受講」の該当性を判断する手法　等

（３）登録セキスペの「入口」として情報処理安全確保支援士試験の在り方について御議論いただきたい。

- 情報処理安全確保支援士試験の試験区分・試験科目の見直し（例：試験区分を複数設ける等）の必要性
- 試験内容の見直しの必要性（マネジメント系の出題の比重を増やす等）　等

6．登録セキスペに関する継続的な検討事項

6－1．アクティブリストの完成イメージ

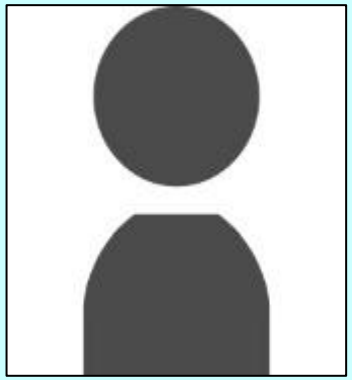
- 登録セキスペの得意分野・専門領域、支援実績等を可視化し、中小企業等のセキュリティコンサルが対応可能な登録セキスペのリスト（アクティブリスト）整備を行い、「どのような支援が受けられるのか」 を明確に提示する。
- 今年度実施する、支援機関と連携したセキュリティ相談会、登録セキスペによるマネジメント指導（テーマ別）、登録セキスペのアンケート調査等をもとに、アクティブリストの項目の内容・構成の検討を行う。

<アクティブリストの項目イメージ>

検索結果一覧

	氏名	地域	支援可能期間	得意とする支援領域	支援実績	経験業種	経験業務	保有資格	専門分野（技術）	一言アピール
①	AAA									
②	BBB									
③	CCC									

氏名をクリックすると、専門家の詳細情報（写真、プロフィール、指導経験等）を表示



氏名：
地域：
支援可能期間：
得意とする支援領域：
支援実績：
経験業種：
経験業務：
保有資格：
専門分野（技術）：
一言アピール：

6．登録セキスペに関する継続的な検討事項

6－1．アクティブリストの完成イメージ

<アクティブリストの検索イメージ>

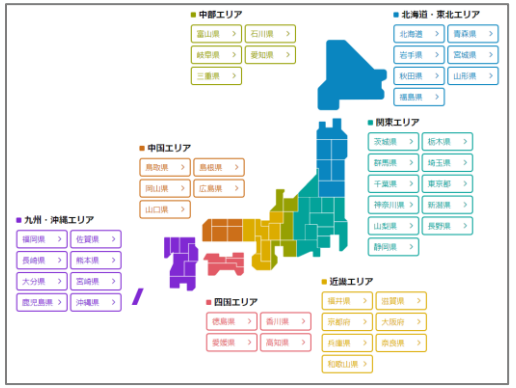
■ キーワード

検索

■ 支援領域

○ 1. セキュリティ対策のルール作り、体制構築、教育、管理について （管理・統制）
　□情報セキュリティ規程の整備
○ 2. 社内のリスクの洗い出しについて （識別）
　□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
○ 3. セキュリティ対策の実践、運用の構築について（防御）
　□アクセス管理 □ソフトウェア更新 □データバックアップ □従業員向け教育
○ 4. サイバー攻撃の検知と監視、検知後の運用策定（検知）
○ 5. サイバー攻撃発生時の対応について（反応）
　□セキュリティインシデント対応
○ 6.インシデントからの復旧とコミュニケーションについて（復旧）

■ 支援地域



(*中小企業庁　認定経営革新等支援機関検索システムより)

■ 支援業種

○自動車産業 ○半導体産業 ○防衛産業 ○建設業 ○電力産業 ○運輸・交通産業 ○その他製造 ○小売業 ○卸売業 ○サービス業 ○金融・・・

■ 支援業務

○財務・経理 ○生産管理 ○受発注 ○在庫管理 ○販売管理 ○社員教育 ○社内のセキュリティ体制構築 ○HP・ウェブページ
○インシデント対応 ○インシデント分析 ○ネットワーク構築

■ 支援期間

○スポット ○1か月程度 ○1か月～6か月 ○ 半年以上 ○長期（顧問契約含む）

■ 支援形態

○訪問でのコンサルティング ○オンラインコンサルティング ○従業員向け研修の開催 ○インシデント発生時の対応支援 ○その他

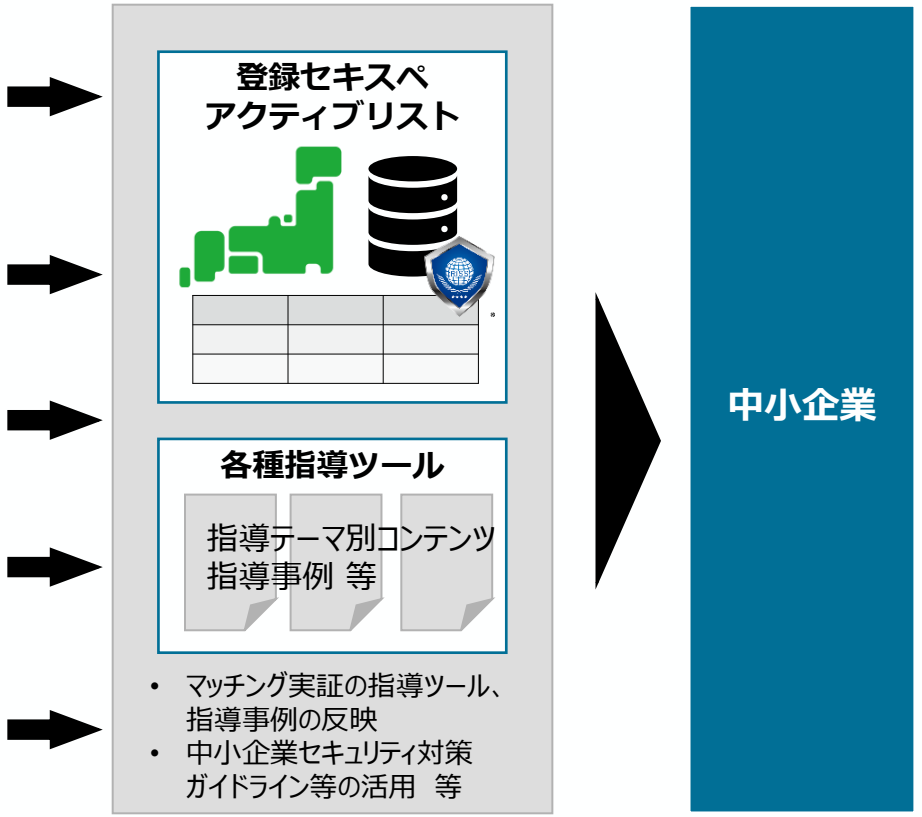
6．登録セキスペに関する継続的な検討事項

6－2．支援機関等におけるアクティブリストの活用イメージ

- 人材不足に悩む中小企業が、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アクティブリストに掲載の登録セキスペを外部人材として活用できるよう、検討を進めていく。

＜支援機関等におけるイメージ＞

支援機関等	アクティブリストの活用イメージ（例示）
中小企業支援機関（中小機構・商工会議所、商工会等）	• セキュリティ対策相談・相談会・セミナー・ワークショップ参加者に対する、セキュリティ専門家の紹介＆マッチング • お助け隊サービスと組み合わせた、セキュリティ専門家の導入支援付パッケージの提供
情報処理安全確保支援士会	• IPA指導ツールを用いた、中小企業対策に関する勉強会の開催 • 税理士会、社会保険労務士会、行政書士会等との合同セミナーの開催や人材紹介プログラムの策定
金融機関	• 補助金制度申請時や融資時におけるセキュリティ専門家の紹介 • セキュリティ専門家による診断・助言を融資条件とした中小企業向け金融支援プログラムの策定
ITベンダー	• セキュリティ専門家活用による中小企業向けセキュリティ製品・サービスの導入時支援、運用サポートの提供 • セキュリティインシデント発生時の運用・復旧支援の提供
業界団体	• サプライチェーンセキュリティ対策の推進を目的とした、業界団体とセキュリティ専門家による合同セミナーの開催 • セキュリティ対策の実践を希望する企業に対するセキュリティ専門家の紹介＆マッチング



6．登録セキスペに関する継続的な検討事項

6－3．みなし受講制度の対象とする実務経験等の考え方

- ①講習代替性を充足することを前提に、②～⑤を総合的に考慮した上で、みなし受講の対象とする実務経験等を決定する必要。

①講習代替性

- 講習受講を義務としている法律の趣旨から逸脱しないものであり、登録セキスペの資質を担保できるものである必要

②本制度の効果

- 実践・特定講習の内容よりもより実践的なサイバーセキュリティ関連業務に従事する登録セキスペの二重負担を解消する必要
- 併せて、資格ホルダーとしての資格の取得・維持ではなく、サイバーセキュリティの実務（「登録セキスペの活用促進・活躍の場の拡大」に掲げる各種制度や企業内部におけるセキュリティ実務等）に携わる登録セキスペを増加させる効果も期待

③客観的判断

- 実務経験等の証跡として客観的に判断が可能である必要

④事務負担

- みなし受講の審査コストや持続可能性を考慮する必要

⑤その他

- 法令に規定できるものである必要

6．登録セキスペに関する継続的な検討事項

6－4．情報処理安全確保支援士試験の在り方について

- サイバー攻撃は今後ますます増加するとともに高度化・複雑化していくおそれがある中、一定規模以上の企業においては、サイバーセキュリティ対策に外部委託を積極活用しつつも、企業におけるリスクマネジメント活動の一部として、自社のサイバーセキュリティリスクを把握し、必要な意思決定や管理を行い、対策を推進する立場の人材を割り当てる必要がある。登録セキスペについても、「企業等の外部から専門的なセキュリティ対策を実施できる人材」としてのみならず、**「企業等の内部に置かれるべき人材」としての活躍が期待**される。

- 登録セキスペの活動領域は様々であるところ、**情報処理安全確保支援士試験の試験区分・試験科目の見直し**（例：試験区分を複数設ける等）**は必要であるか。試験自体は共通としつつ、更新体系に選択肢を設けることで対応すべきか。**また、**試験内容について、マネジメント系の出題の比重を増やすべきか。**

※試験に関する論点は、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も、別途議論予定。

＜これまで頂いた御意見＞

- 試験の見直しという観点では、情報処理安全確保支援士試験ではテクニカル寄りの出題が中心になっており、マネジメント寄りの出題は少ない。**ITSS レベル 4 においてマネジメント寄りの出題は難しい**ため、継続的な更新講習でカバーしていくことが必要と考えられる。
- **制度自体が複雑になることはできるだけ避けるべき**と考える。また、登録セキスペが企業の内外どちらで活躍するかは各人のキャリアパスの結果であるため、**それぞれが別資格でなければならないということではない**と理解している。試験自体は同じであっても、「企業等の外部から専門的なセキュリティ対策を実施できる人材」と「企業等の内部に置かれるべき人材」とで更新（２階部分の講習）のオプションを作るのはどうか。
- 登録セキスペがどちらの人材としても活躍できるためのベースをどうするかについては、試験の側で考えていく必要があるが、**資格更新については、多様性を持たせることが重要**なのではないか。

（参考）ITSS＋（プラス）セキュリティ領域と情報処理安全確保支援士試験シラバスの関連知識・スキルとの対比表

■分野とセキュリティ関連知識・スキルとの対応

→　セキュリティ関連知識・スキルの内容は、情報処理安全確保支援士試験シラバス（https://www.jitec.ipa.go.jp/1_13download/syllabus_sc_ver2_0.pdf）を参照する

【注釈】

※1 「◎」は主導できるレベル（情報処理安全確保支援士試験レベル）、「○」はコミュニケーションが取れるレベル（情報セキュリティマネジメント試験レベル）を想定。

※2 企業等によって、「◎」、「○」の付し方の変更や、知識・スキル項目の追加・削除・詳細化が必要。

※3 分野に固有のタスクを実施するための知識・スキルについては含まれていない。

	分野	セキュリティ関連知識・スキル（大項目）		
		セキュリティマネジメント	システムセキュリティ	セキュリティオペレーション
戦略マネジメント層	システム監査	○		
	経営リスクマネジメント			
	法務			
	事業ドメイン（戦略・企画）			
	セキュリティ監査	◎	○	○
	セキュリティ統括			
	デジタルシステムストラテジー			
実務者・技術者層	脆弱性診断・ペネトレーションテスト	○	◎	◎
	セキュリティ監視・運用			
	セキュリティ調査分析･研究開発			
	デジタルシステムアーキテクチャ	○	◎	○
	デジタルプロダクト開発			
	デジタルプロダクト運用		○	○
	事業ドメイン（生産現場・店舗管理）			○

大項目	セキュリティマネジメント	システムセキュリティ	セキュリティオペレーション
大項目の概要	経営層の下で組織の特性に応じた適切なセキュリティ体制・ポリシーの構築・運用が行える	セキュアなシステムの企画・設計・開発が行える	セキュリティインシデントへの事前対策・事後対応が適切に行える
情報処理安全確保支援士試験シラバス大項目との対応	(1)情報セキュリティマネジメントの推進又は支援に関すること	(2)情報システムの企画・設計・開発・運用でのセキュリティ確保の推進又は支援に関すること	(3)情報及び情報システムの利用におけるセキュリティ対策の適用の推進又は支援に関すること (4)情報セキュリティインシデント管理の推進又は支援に関すること

Ⅳ　中堅・中小企業等の内部でセキュリティ対策を推進する者の育成・確保に向けた施策の検討

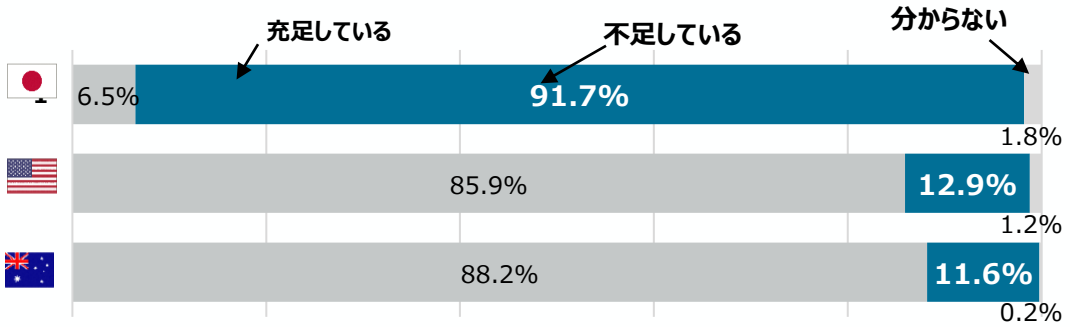
１．中堅・中小企業のセキュリティ人材の現状・課題
２．第２回までの主な御意見
３．中堅・中小企業等の内部でセキュリティ対策を推進する者の育成・確保に向けた施策の検討の方向性
４．実践的方策の提示の全体像
５．継続的な検討事項

1．中堅・中小企業のセキュリティ人材の現状・課題

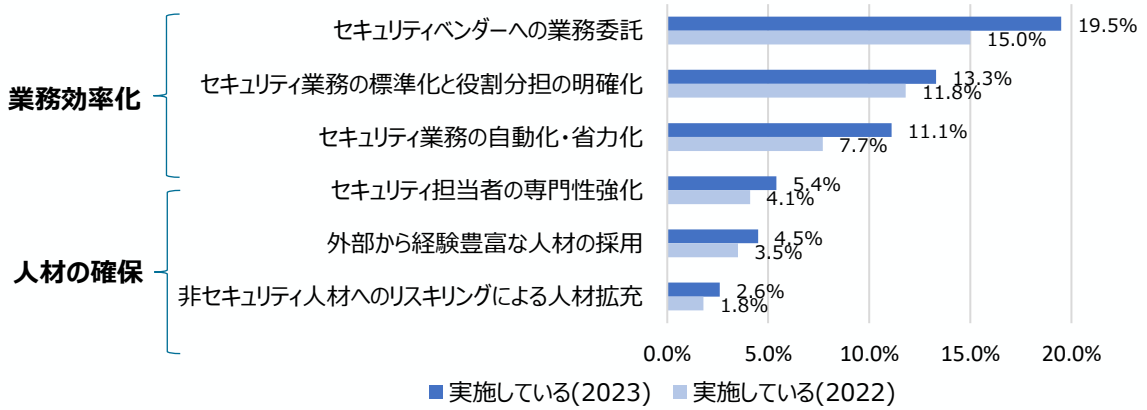
- 民間調査によると、我が国では企業の規模に関わらず、９割の企業がセキュリティ人材が不足していると回答。また、社内のセキュリティ人材不足を補う施策として、人材確保の取組を実施している企業は少ない。
- 経済産業省が実施した企業へのヒアリングでは、社内でのセキュリティ人材の確保と育成が困難であるとの声がある。
- 経済産業省およびIPAでは、企業のセキュリティ人材の確保・育成に資するガイドライン等を策定してきたが、多くの中堅・中小企業においてはセキュリティ人材の確保・育成の取組が実践されていない状況。

→ **中堅・中小企業等の内部でセキュリティ対策を推進する者の育成・確保に向けた施策を検討**

セキュリティ人材の不足状況



セキュリティ人材不足を補う施策の実施状況



企業へのヒアリング結果

- 社内においてセキュリティの教育をする立場にある人材が不足している。もしくは、知識の偏りがあり内部でのセキュリティ人材育成が困難である。
- 担当者がどのようなスキル・知識をどのレベルで有していることが必要か分からない。適切な外部の研修が、ない/分からない/探すことができない。
- ユーザー側企業においては、広く浅くゼネラリスト的な知識が求められる。ベンダー企業のような高い専門知識は必要とされていない。
- 単に知識だけでなく、現場ではトラブルシューティングなど実践的スキルが重要。実践的スキルの習得には、現場やそれに近い環境で学ぶ必要がある。

出典：NRI セキュア 企業における情報セキュリティ実態調査2023

２．第２回までの主な御意見

- 中堅・中小企業にとって課題である、内部のサイバーセキュリティ人材の確保・育成に資するよう、既存施策の見直し等、サイバーセキュリティ人材の拡充に向けた施策の方向性を検討する。
- 中堅・中小企業と言っても、規模、業種等が様々であり、幅が広く、**①専任で推進する人材の確保が可能な企業・目指すべき企業と②兼任であっても推進する人材の確保を目指すべき企業に分けて、効果的なActionが異なりそれぞれ検討する**。
- 人材確保・育成のためのガイドは整備されてきているが、人材不足が解消されていない実態。**既存ガイドを整理しつつ、企業におけるセキュリティ人材の確保・育成の取組を分かりやすく提示する**ことが有効である。
- 中堅・中小企業にとって、自社がどの程度のセキュリティ人材を確保、育成することが適切であるか判断をすることは困難。参考となる他企業の事例が有効だが、現状では数が少ない。**事例を増やすことが必要**である。

3．中堅・中小企業等の内部でセキュリティ対策を推進する者の育成・確保に向けた施策の検討の方向性

基本的考え方

（1）中堅・中小企業を含むサイバーセキュリティ対策を推進する人材の確保については、既に、経済産業省・IPA作成の「サイバーセキュリティ経営ガイドライン Ver2.0 付録Fサイバーセキュリティ体制構築・人材確保の手引き第２版」(2022年6月公開　以下**「人材確保の手引き」)など既存のガイドラインが公表**されているところである。

（2）他方で、中堅・中小企業と言っても幅が広く、現実的には実践が困難な状況であることから、
「①専任のセキュリティ人材の確保が可能な企業」「②兼任であってもセキュリティ人材の確保を目指す企業」の一応の分類を念頭に、企業が実施すべきセキュリティ対策を提示し、各対策に応じた人材の確保・育成方策を講じることができるよう整理することは、サイバーセキュリティ対策が十分でない企業にとって有益なものと考えられる。

（3）そこで、企業が実施すべきセキュリティ対策と「人材確保の手引き」等の既存ガイドの内容を紐付け、検討会として、中堅・中小企業が実施する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（以下、「**実践的方策ガイド**」とする）のβ版を提示することとしたい。

（4）なお、中堅・中小企業においては、特に経営者によるセキュリティ対策への理解とリーダーシップが重要であることから、「実践的方策ガイド」では**経営者向けのメッセージを収録**することとしたい。また、セキュリティ対策の実施に当たっては、特に専門技術的な事項について外部委託が必要となってくることに鑑み、**自社実施と外部委託との切分けや適切な外部委託についても視野**に入れることとしたい。

（5）中堅・中小企業を含むサイバーセキュリティ対策を推進する人材の確保に関する内容を含むガイドライン等は既に存在することから、読者にとって資料の位置付けが明確になるよう、既存のガイドライン等の付属文書との位置付けとしたい。

「実践的方策ガイド」の位置付け

（1）ITサービス等の提供自体を事業内容とする企業や攻めのセキュリティというより、むしろ、セキュリティ対策に十分取り組むに至っていない企業が、順を追って取り組めるような内容を想定。

（2）人材確保・育成の前提となるセキュリティ対策の内容については、IPA作成の「中小企業の情報セキュリティ対策ガイドライン」を参照（SECURITY ACTION（☆１、☆２）など）。また、検討中のサプライチェーン対策評価制度等との関係については、セキュリティ人材が担う取組内容の明確化の観点から、将来的に参照することを視野。

（3） IT、DX人材の育成や採用の際に参考となるスキル標準には、ITSSやDSSがあるところ、スキルの詳細に踏み込むことなく、サイバーセキュリティへの認知が低く、対策が十分でない中堅・中小企業の行動変容につながる分かりやすい取組を提示することを想定。

（参考）人材育成・確保の関連要素（既存のガイドより）①

- 「人材確保の手引き」においては、企業が実施すべきサイバーセキュリティ関連タスクを提示し、自社実施と外部委託の切り分けを提示。また、サイバーセキュリティ関連タスクを担う人材の確保・育成の方策について記載。

セキュリティ統括機能や自社実施・外部委託の切分けの明確化

ⅰ）企業が実施すべきサイバーセキュリティに関するタスク17分野（ITSS＋セキュリティ領域）を紹介

「**セキュリティ統括機能**」を定義（p10～12）

ⅱ）「**セキュリティ統括機能**」とは、サイバーセキュリティ対策やインシデント対応について、専門的な知見・経験によって、経営層による意思決定等をサポートする機能。主に「戦略マネジメント層」と「実務者・技術者層」の２層で組織横断的に関係部署と連携し、組織的なサイバーセキュリティ対策を統括する。（p12）

ⅲ）**自社実施と外部委託の切り分け**を提示（p19～20）

→　**自社：経営判断に直結する分野**

※管理部門が担当すべき分野、事業のリスクマネジメントに相当する分野の外部委託は不適切であり、少なくとも意思決定や管理は自社の要員で対応することが望ましい。（p19）

→　他社：システムアーキテクチャ開発、セキュリティ調査分析、脆弱性診断・ペネトレーションテスト等

※専門性が求められるタスクについては、外部委託可能だが、**委託仕様の策定や委託先からの報告への対応を担う体制が社内に必要**（p20）

（参考）人材育成・確保の関連要素（既存のガイドより）②

サイバーセキュリティ関連タスクを担う人材とその確保・育成

ⅰ）　**サイバーセキュリティ対策を主たる目的とする業務に従事する人材**と、サイバーセキュリティ以外を主目的とする業務を遂行する中でサイバーセキュリティ対策に関わる人材（ p26ではプラス・セキュリティの取組）について、**ITSS＋における対象分野を特定**（p22～23）

ⅱ）　**「サイバーセキュリティ対策を主たる業務とする人材」が担う分野として、「セキュリティ統括」分野を提示**、セキュリティ対策業務を担う人材が専任である必要はないものの**インシデントの際には司令塔としての役割に専念できるようにする必要**（p24）

ⅲ）　「サイバーセキュリティ対策を主たる業務とする人材」の確保策としては、①**隣接分野（RM・IT等）の業務経験を有する人材の配置転換・育成**、②**セキュリティ対策関連の業務経験を有する人材の中途採用**、③**セキュリティを専門とする教育機関（大学院・大学・高専・専門学校など）を修了した人材の新卒採用**、④（他企業との）**兼業・副業で従事する人材の活用**を提示（p25）。

ⅳ）　**教育プログラム・試験・資格等の活用と人材育成計画の検討**として、①**教育プログラム等の活用**（中核人材育成プログラム：IPA、サイバーセキュリティ企画演習：IPA、キャリアアップMOTサイバーセキュリティ経営戦略コース：東工大、CYDER：NICT）（p29）、②**試験・資格の活用**（登録セキスペ、情報セキュリティマネジメント試験）を提示（ｐ30）（※p38には、ITパスポート試験など30以上の資格・試験を提示）

４．（１）「実践的方策ガイド」の内容・提示方法（イメージ）

① **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・育成の方策を分かりやすく整理**。

② 読者として、経営層、セキュリティ人材本人、中堅・中小企業を支援する立場の人材を想定。

③ 人材の確保状況に応じて実施すべきセキュリティ対策についても合わせて提示するとともに、自社のセキュリティ対策における現在の立ち位置、**目指すべき姿の参考となる事例等を提示**。

④ 具体的取組については、**人材の「確保」と「育成」の観点**から、**実施すべきセキュリティ対策と合わせて分かりやすく整理**。

⑤ 各取組は、**既存ガイド等と紐づけ**を行い、考え方・具体的な実践方法（How-to）を参照可能にするとともに、人材を「育成」する際に参照できる**実際のセミナー・資格等を提示**。

⑥ 経営者向けに、セキュリティ対策の重要性、全体像が分かるチラシ、担当者向けに取組を分かりやすく示した小冊子、動画コンテンツ等で提示。

4．（２）経営者へのメッセージ

- **「実践的方策を示したガイド」**を中小企業等に提示するに当たっては、経営者のリーダーシップが特に重要と考えられることから、人材の確保・育成以前に、サイバーセキュリティ対策自体の必要性を改めて、経営者向けに発信する方向で検討。

既存ガイド※1を参考にした経営者へのメッセージ（イメージ）

（１）中堅・中小の企業においても、**「自社の事業特性に応じたセキュリティ対策の実行」が必要不可欠であり**、サイバーセキュリティリスクを組織の経営リスクの一環として捉え、把握・評価した上でセキュリティ対策の実施を通じて、**サイバーセキュリティリスクを自社が許容可能とする水準まで低減させることは、企業として果たすべき社会的責任であり、その実践は経営者としての責務※2。**

（２）具体的には、セキュリティ対策を疎かにしたために**システム障害が発生した場合、自社の事業活動が停止する恐れがある。また、情報漏えいが発生した場合は、顧客や取引先からの信用失墜につながる。さらには、自社の事業停止はサプライチェーン全体にも広く影響を与える**ことから、業務を受託する中小企業もサプライチェーンを構成する一員であることを自覚し、セキュリティ対策に取り組むことが不可欠。

※2：消費者・従業員の個人情報や企業が取り扱う機密情報の保護、自社事業停止に伴うサプライチェーン全体への影響等への社会的責任への対応

企業の中には、サイバーセキュリティ対策の必要性を理解したとしても、どうしても人材の確保・育成に踏み出せない企業も存在し得る。登録セキスペ等セキュリティ専門家への相談、SECURITY ACTION（☆１、☆２）やサイバーセキュリティお助け隊サービスを経営者主導で実践・導入することも考えられる。

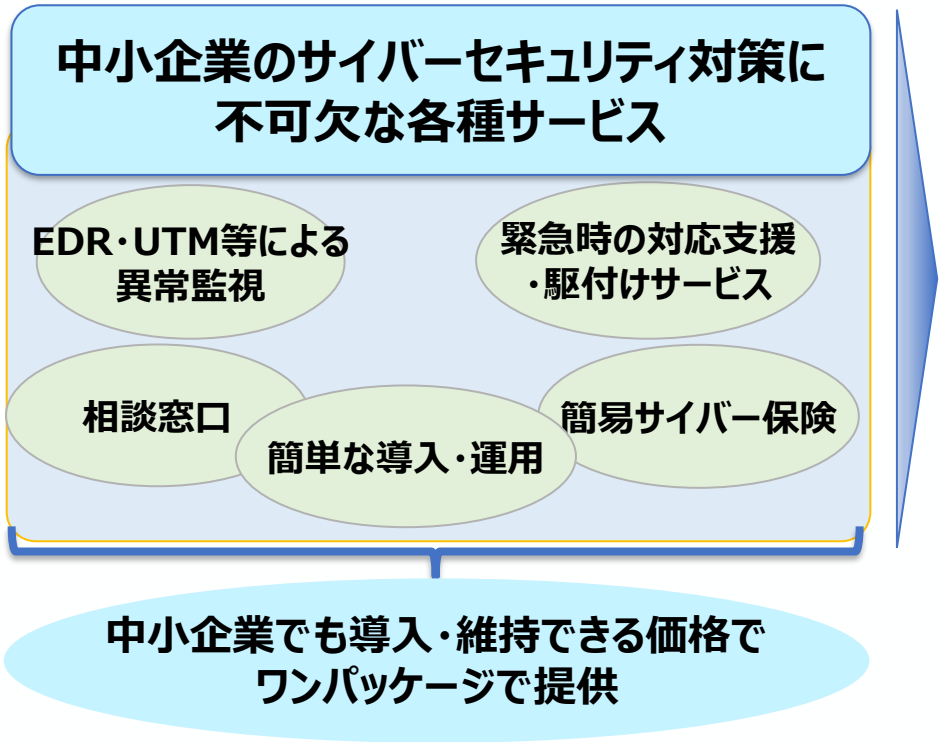
他方で、①サイバーセキュリティ対策に外部人材を活用するとしても、委託仕様の策定や委託先からの報告への対応など、専門事業者とのコミュニケーションを図る人材が社内に必要と考えられること、②社内で経営者の意向を反映させたセキュリティルールを策定し、従業員に対して周知する役割を担う人材が必要と考えられることなどから、サイバーセキュリティ人材を企業内部で確保・育成することは重要。

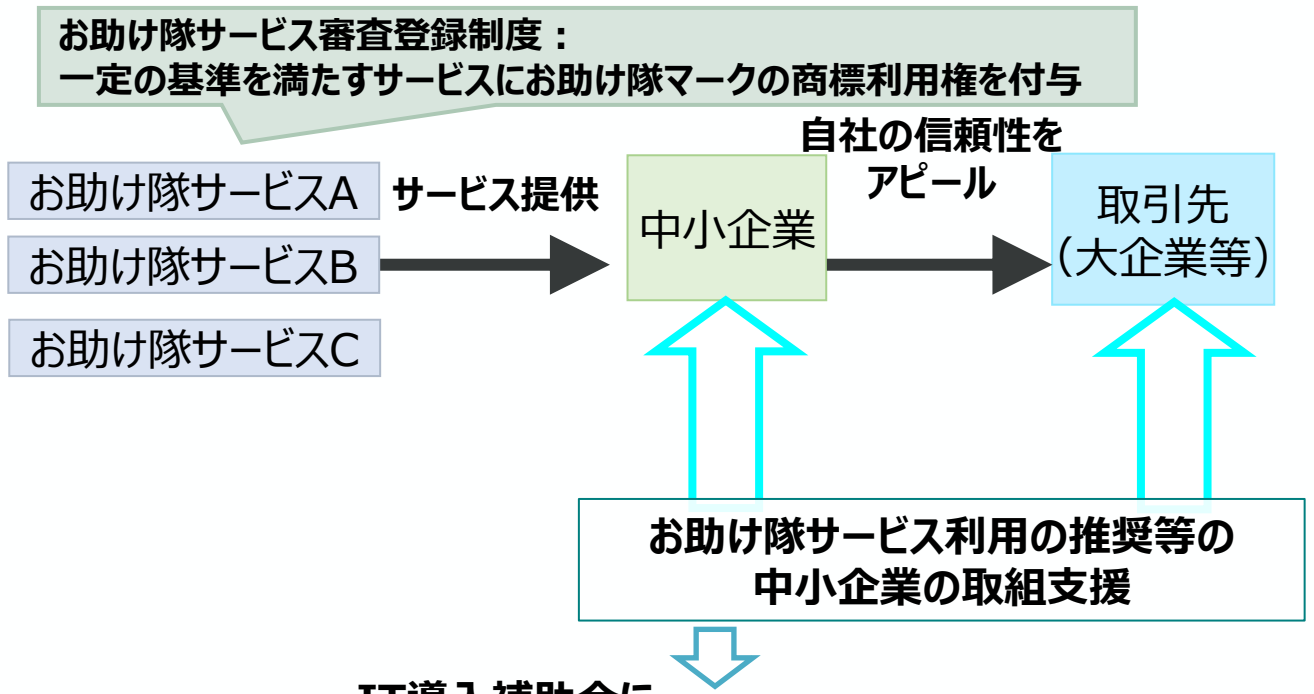
また、社内のサイバーセキュリティ人材の確保のためには、処遇の改善やキャリアパスの検討が必要。

※1サイバーセキュリティ経営ガイドラインVer3.0(2023年3月 経済産業省)、中小企業の情報セキュリティ対策ガイドライン第3.1版(2023年4月 IPA)

（参考）サイバーセキュリティお助け隊サービス

- 中小企業に対するサイバー攻撃への対処として不可欠なサービス（見守り、駆付け、保険）をまとめた、民間の事業者から提供されるサービス。**中小企業が利用しやすい安価で提供。**
- IT導入補助金「セキュリティ推進枠」でお助け隊サービス**導入費用を補助**（補助率：1/2）。





4．（3）企業が実施するセキュリティ対策の状況に応じた人材確保・育成の方策

～「実践的方策ガイド」の作成に向けた全体像～

		実施するセキュリティ対策 （中小企業ガイドラインを参考に整理）	必要なセキュリティ人材	（想定される人材状況）	人材の確保・育成の方策	
（兼任でのみ確保可能）	Step1 「取組の開始」	基本的なセキュリティ対策を開始 ・情報セキュリティ5か条を実施	基本的対策（情報セキュリティ５か条）を社内に周知・実践させるための人材を最低１人以上確保	サイバーセキュリティ対策を推進する者が自社に存在しない状況	A 隣接分野（リスクマネジメント・ITなど）の業務経験を有する社内人材の配置転換 A 希望する社員の社内公募による配置転換	どうしても自社の人材の確保・育成に踏み出せない状況にある企業においては、 登録セキスペ等の外部のセキュリティ専門家への相談から開始。
	Step2 「組織的な取組」	担当者の下で、組織的な取組を開始 ・社内の情報セキュリティに関するルールを規定 ・従業員へのセキュリティルールの周知、注意喚起、教育の検討	特に、従業員としての対策、組織としての対策（情報セキュリティ対策のルール化を含む）を社内に周知・実践させるための人材を確保	サイバーセキュリティ対策を他業務との兼任で推進する人材は選定されているものの、組織的な取組を行うには不十分な状況	（上記方策に加え、） A 社内人材の配置転換による兼任人材の増員 E 「中小企業ガイドライン」を参照 E IPA映像コンテンツの視聴	
（兼任又は専任で確保可能）	Step3 「本格的な取組」	セキュリティ体制を構築し、対応すべきリスクに応じたセキュリティ対策を開始 ・平時、有時の対応体制を構築 ・外部専門家(セキスペ等)を活用した資産の洗い出し、リスク分析の実施 ・必要なセキュリティ対策の検討、導入、運用を実施 ・外部委託範囲の適切な決定、契約書・覚書などへのセキュリティ対策の明記	自社の情報資産の管理、対応すべきリスクの特定、実施すべき対策（IT機器利用、IT基盤運用管理、システム開発及び保守、委託管理、情報セキュリティインシデント対応ならびに事業継続管理、委託時の対策における対策等）を決定する人材を確保	多岐にわたるセキュリティ対策を実施するために、人材の増員に加え、人材の質の面で、対策推進のための知識・経験・スキルの更なる向上が必要な状況	A 専任の人材の任命 A 社内人材の配置転換による兼任人材の増員 E IPAセキュリティ関連セミナーの受講 E マナビDX　セキュリティ関連講座の受講	左記人材を全て自社内で確保することは困難であると考えられることから、**自社で実施する業務と外部委託が可能な業務を切り分け**、自社に必要な人材の確保・育成を実施。 登録セキスペアクティブリスト等を活用し、**外部専門人材への相談**も有効。
	Step4 「継続的な改善」	より強固なサイバーセキュリティ対策に取り組む ・システム・ソフトウェアの脆弱性管理 ・インシデントの検知	自社が利用するシステム・ソフトウェアにおける脆弱性の管理、インシデントが疑われる兆候や実際の発生の検知のための人材を確保	多岐にわたるセキュリティ対策を高度なレベルで実施するために、人材の質の面で、高度な対策推進のための知識・経験・スキルの更なる向上が必要な状況	より強固なセキュリティ対策に取り組む人材について、上記方策に加えて、取組を強化 （取組例） B セキュリティ対策関連の業務経験を有する人材の中途採用 C サイバーセキュリティを専門とする教育機関を修了した直後の人材の新卒採用 D 専任の人材による兼任人材への指導 E 教育プログラムの受講(IPA:サイバーセキュリティ企画演習、NICT：CYDER、大学によるリカレント教育)	

※Step1・2においては、セキュリティ人材を「兼任でのみ確保可能な企業」、Step3・4においては「兼任又は専任で確保可能な企業」を念頭に置いており、全ての企業が等しくStep4を目指すというより、**経営者は、自社の事業特性に応じた実施すべきセキュリティ対策に必要なセキュリティ人材の確保・育成を検討することが重要。**
※SECURITY ACTION（☆１、☆２）の実践やサイバーセキュリティお助け隊サービスの導入等を経営者主導で実施することも考えられる。

（参考）企業が実施すべきセキュリティ対策（中小企業情報セキュリティガイドライン　3.1版）

P４（本ガイドラインの活用方法）の記載（ポイント）		P４でリンクされている各頁の記載（ポイント）
Step1 まず始めましょう	これまで情報セキュリティ対策を特に意識していない場合は「２.できるところから始める」（P.19）を参照して、**「情報セキュリティ５か条」を実行**。	【p19】 情報セキュリティ５か条は、共通する基本的な対策をまとめたものなので、必ず実行
Step2 現状を知り改善しましょう	Step1 は実施できていて次に進める場合は「3.組織的な取り組みを開始する」（P.20）を参照して、**「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、できていない対策の実行に努める**。 【進め方】 ・「情報セキュリティ基本方針（サンプル）」を参考に**基本方針を作成**。 ・「5 分でできる！情報セキュリティ自社診断」で**現状の対策を把握し、実施すべき対策を検討**。 ・**「情報セキュリティハンドブック（ひな形）」を参考に具体的な対策を定めて従業員に周知**。	【p20】 （１）情報セキュリティ基本方針の作成と周知 （２）実施状況の把握 ※「５分でできる！情報セキュリティ自社診断」（付録３）を利用 （３）対策の決定と周知 **※自社診断には、あまり費用をかけず、効果があると考えられる対策例が示されている**ので、診断結果に基づき、実施すべき対策を検討
Step3 本格的に取り組みましょう	Step2 までは実施できていて次に進める場合は「４.本格的に取り組む」（P.24）を参照して、自社のリスクに応じた**対策規程を作成**し、**運用後は点検して改善**。 【進め方】 ・情報セキュリティ**管理の体制を構築し、対策の予算を確保**。 ・対応すべきリスクと対策を検討し、「情報セキュリティ関連規程（サンプル）」を参考に**規程を作成**。 **・委託時に必要となる対策を検討**するとともに、**点検や改善**に務める。	【p24】 （１）管理体制の構築 ①責任分担と連絡体制の整備 ②緊急時対応体制の整備 （２）デジタルトランスフォーメーション（DX）の推進と情報セキュリティの予算化 ※より有効なセキュリティ対策のために、自社の情報システムについて、インターネットとの接続状況を図にするなどして対策を検討するとともに、**予算を確保**する必要 （３）情報セキュリティ規程の作成 ①対応すべきリスクの特定 ②対策の決定 （組織的対策、人的対策、情報資産管理、アクセス制御及び認証、物理的対策、IT機器利用、IT基盤運用管理、システム開発及び保守、委託管理、情報セキュリティインシデント対応ならびに事業継続管理、テレワークにおける対策） （４）委託時の対策 ※取り扱う情報の種類、委託する業務に適した情報セキュリティ対策を**委託先にも実施してもらう**。 委託先の情報セキュリティ対策が維持されているか、責任をもって管理。
Step4 改善を続けましょう	「５.より強固にするための方策」（P.32）を参照して、**自社に必要な対策を追加実施**してください。Step1 や Step2 に取り組んでいる企業でも、Step4 を参照して必要な対策があれば実行。	【p32】 （1）情報収集と共有（2）ウェブサイトの情報セキュリティ（3）クラウドサービスの情報セキュリティ（4）テレワークの情報セキュリティ（5）セキュリティインシデント対応（6）セキュリティサービス例と活用（7）技術的対策例と活用（8）詳細リスク分析の実施方法

（参考）人材の確保・育成のための方策

人材育成・確保の取組項目※

人材の確保	**A　配置転換 「内部から内部へ」**	隣接分野（リスクマネジメント・ITなど）の業務経験を有する社内人材の配置転換、希望する社員の社内公募による配置転換
	B　中途採用 「外部から内部へ」	セキュリティ対策関連の業務経験を有する人材の採用 ＊ほかに、厳密には内部人材とは言えないが、社内に不足する知識・経験・スキルを外部の副業・兼業人材によって補充する方策も有効と考えられる。
	C　新卒採用 「外部から内部へ」	サイバーセキュリティを専門とする教育機関を修了した直後の人材の採用
人材の育成	**D　OJTによる育成 「内部からのスキル等移転」**	サイバーセキュリティに関する業務経験を有する人材が、サイバーセキュリティ対策推進のための知識・経験・スキルが備わっていない人材に対し、業務遂行の中で指導
	E　OFF-JTによる育成 「外部からのスキル等移転」	サイバーセキュリティ対策推進のための知識・経験・スキルが備わっていない人材が、教育プログラム等の活用

※「中小企業・小規模事業者人材活用ガイドライン」（2023年6月　中小企業庁）を参考に項目を作成

5．中堅・中小企業等の内部でセキュリティ対策を推進する者に関する継続的な検討事項

- 本年度取りまとめる「実践的方策ガイド」β版をブラッシュアップさせるため、来年度、実証の実施を検討。また、特に中小企業においては、セキュリティ対策の実施に当たって外部専門人材の活用も必要となることから、活用のための支援策についても検討。

「実践的方策ガイド」のブラッシュアップのための実証

「実践的方策ガイド」をさらに充実したものにするために、以下のような実証が有効ではないか。

（１）実証の対象

「実践的方策を示したガイド」の各Stepに相当する複数の企業であって、必要なサイバーセキュリティ対策を実施するためのセキュリティ人材の確保・育成に課題を感じている企業

（２）実証の内容、実施者

「実践的方策ガイド」が、中堅・中小企業にとってセキュリティの向上に有効なものとなっているか（有効性）、使い勝手がよいものとなっているか（利便性）、補充すべき内容がないか（網羅性）などについて、登録セキスペ等のセキュリティ専門家が伴走支援をしながら実証（可能な限り取組事例についても収集）。

（３）ガイド普及のための調査

中堅・中小企業が接点を持つ（情報収集している）、支援機関(商工会議所、Web、税理士、中小企業診断士等)はどこなのか等、ガイドの普及に資する情報を合わせて調査。

外部専門人材活用のための方策

外部専門人材の活用のためには、例えば、以下のような支援策が考えられるのではないか。

（１）外部専門人材の支援拠点への配置

（登録セキスペのアクティブリストの普及・活用を促進するとともに、）中堅・中小企業との直接の接点を有する支援機関や相談窓口等に登録セキスペを配置（検討）。

（２）外部専門人材の活用のための導入支援

既存の支援パッケージ（中小企業が利用しやすい安価なセキュリティサービスを普及させるために、見守り・駆け付け・相談窓口・保険をワンパッケージで提供する「サイバーセキュリティお助け隊サービス」）に、外部専門人材の派遣・相談を追加（検討）。