

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

2025年5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 委員等名簿

※敬称略、五十音順

(委員)

- 北野 晴人 デロイトトーマツサイバー合同会社 執行役員
- 小出 洋 九州大学 情報基盤研究開発センター 教授
- 武智 洋 サプライチェーン・サイバーセキュリティ・コンソーシアム (SC3) 企画・調整室長
日本電気株式会社 サイバーセキュリティ戦略統括部 エグゼクティブエキスパート
- 田中 浩之 東京ガス株式会社 監査部
- 長谷川 長一 株式会社ラック 新規事業開発部 主席研究員
- 平山 敏弘 情報経営イノベーション専門職大学 (iU) 教授
- 藤本 礼久 一般社団法人 日本情報システム・ユーザー協会 参与
- 丸山 満彦 PwCコンサルティング合同会社 パートナー
情報セキュリティ大学院大学 客員教授
- 三谷 慶一郎 株式会社NTTデータ経営研究所 主席研究員 エグゼクティブ・コンサルタント【座長】

(オブザーバー)

- 内閣官房 内閣サイバーセキュリティセンター
- 総務省 サイバーセキュリティ統括官室
- 経済産業省 商務情報政策局 情報技術利用促進課
- 独立行政法人情報処理推進機構
- 日本商工会議所
- 一般社団法人情報処理安全確保支援士会

サイバーセキュリティ人材の育成促進に向けた検討会 開催経緯

※各回に記載した内容は、事務局説明資料の項目又はプレゼンテーションいただいた有識者を示す。

- **第1回 令和6年7月3日**
 - セキュリティキャンプの拡充
 - 登録セキスぺの活用及び制度の見直し
 - 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
- **第2回 令和6年8月7日**
 - 登録セキスぺの活用及び制度の見直し
 - 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
- **第3回 令和6年11月22日**
 - これまでの議論の整理と継続的な検討事項
- **第4回 令和7年2月7日**
 - 「登録セキスぺアクティブリストを活用した中小企業支援」「みなし受講制度」
 - 「実践的方策ガイドの位置付け等」「実践的方策ガイドβ版（案）」
 - 有識者プレゼンテーション「大阪商工会議所」
- **第5回 令和7年3月4日**
 - 有識者プレゼンテーション①「情報処理安全確保支援士会」
 - 有識者プレゼンテーション②「グーグル合同会社」
- **第6回 令和7年4月3日**
 - 有識者プレゼンテーション①「東邦ガス情報システム株式会社」
 - 有識者プレゼンテーション②「三井物産セキュアディレクション株式会社」
- **第7回 令和7年5月8日**
 - 最終取りまとめ（案）

- I 検討会における議論の全体像**
- II セキュリティ・キャンプ**
- III 登録セキスペ**
- IV 中堅・中小企業等の内部でセキュリティ対策
を推進する者の確保・育成**

I 検討会における議論の全体像

II セキュリティ・キャンプ

III 登録セキスペ

IV 中堅・中小企業等の内部でセキュリティ対策
を推進する者の確保・育成

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登録セキスペ※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ペのリスト（アクティブリスト）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）

- アクティブリストの整備・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
※アクティブ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

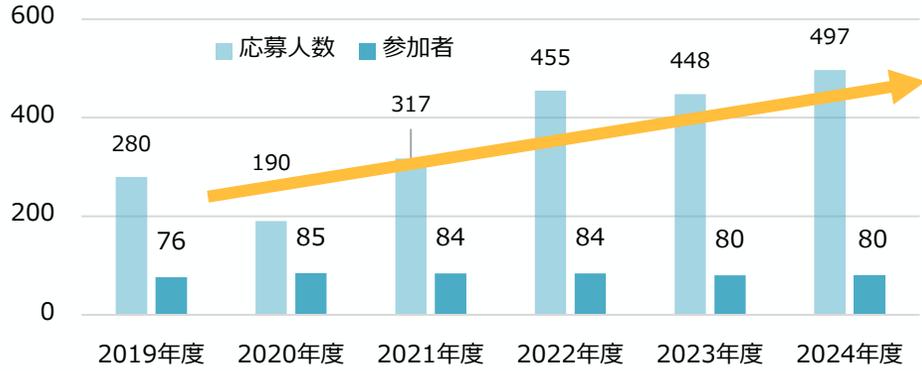
- 「トップガン」人材育成スケール拡大（現状の2倍以上）
- セキュリティ人材のキャリアの魅力化

- 登録セキスペの活躍機会（中小企業のセキュリティ確保等の実務経験機会）増加
- 登録セキスペ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ペ5万人
（2025年4月時点で約2.4万人）を達成

(参考) サイバーセキュリティ人材の育成・確保状況に係るデータ

セキュリティ・キャンプ 全国大会の参加状況



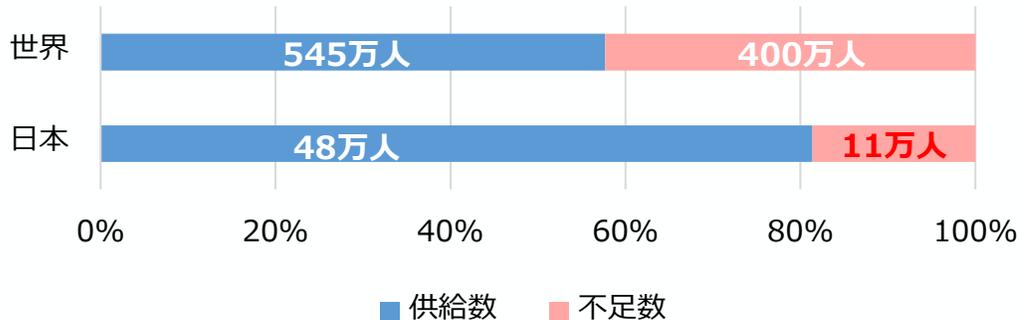
登録セキスペ 登録者数の推移



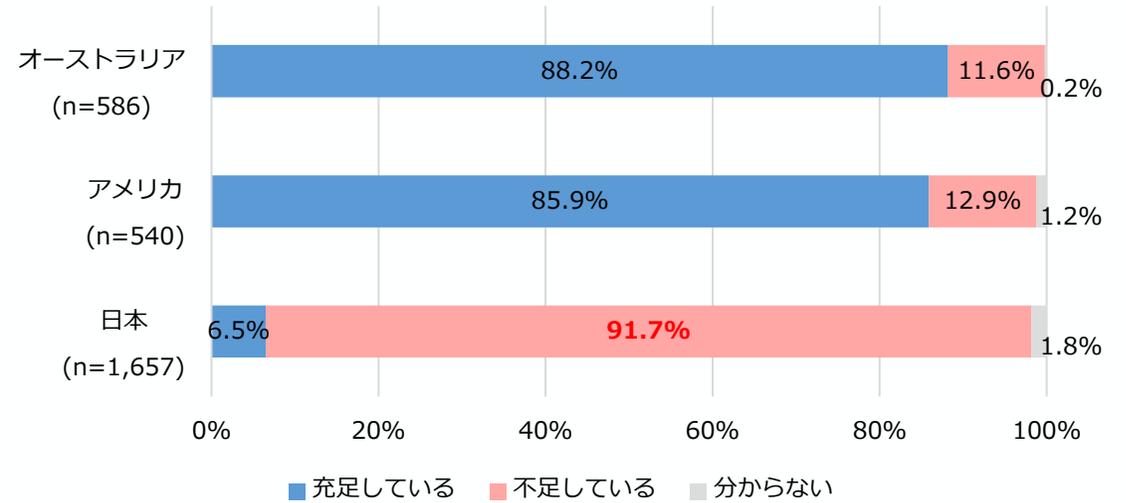
登録セキスペ 消除理由上位5位

- 1位 メリットなし、かつ費用が高額
- 2位 転職、異動、業務上不要
- 3位 費用が高額
- 4位 メリットがない
- 5位 転職+費用負担されなくなった

セキュリティ人材の不足状況①

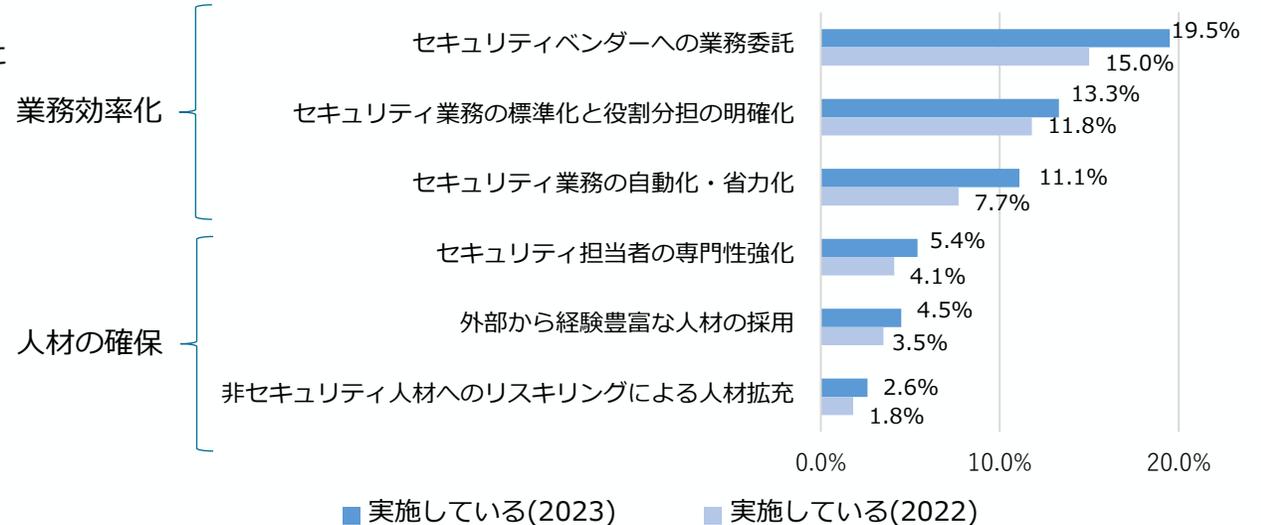


セキュリティ人材の不足状況②



出典：NRI セキユア 企業における情報セキュリティ実態調査2023

セキュリティ人材不足を補う施策の実施状況



出典：NRI セキユア 企業における情報セキュリティ実態調査2023

出典：ISC2 Cybersecurity Workforce Study 2023を基に経済産業省作成

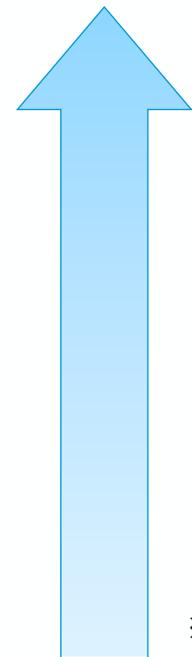
(参考) サイバーセキュリティ人材の育成・確保に係る状況

- 「サイバーセキュリティ人材」について、セキュリティに関する知識・スキル水準の程度に階層別に分解した場合、
 - ① トップ人材の育成・確保については、セキュリティ・キャンプの取組を通じて質的効果はみられるも、**規模が依然として不足**。
 - ② 高度専門人材や専門人材として活躍が期待される「登録セキスペ」については、**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らない（結果として量が不足）。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あり、**ミスマッチも生じている**。
 - ③ 「登録セキスペ」ほど高度かつ網羅的な水準が求められない専門人材のうち、**特に中堅・中小企業等の内部でセキュリティ対策を推進する者**については、企業内部での人材育成に資する効果的な施策も見られず、**圧倒的に人材が不足している状況**。

セキュリティに関する知識
・スキル水準の程度

各層の育成・確保に向けた主な施策

課題



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

セキュリティ・キャンプ

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

中核人材育成プログラム

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、地方ベンダー実務担当者など

登録セキスペ制度

※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。

質よりも量が不足

・・・世界で活躍する人材を輩出するなど、一定の政策効果はある上、参加希望者数は年々増加しているが、スケールしていない。また、サイバーセキュリティ供給側としての起業促進にはつながらない。

活躍の場が限定的・市場のミスマッチ

・・・登録セキスペを必要とする需要側企業（中小企業等）において、①サイバーセキュリティ対策の必要性が理解されていない場合（登録セキスペの活躍の場がない）や、②人材不足が懸念される場合（登録セキスペとのミスマッチが起きている）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。

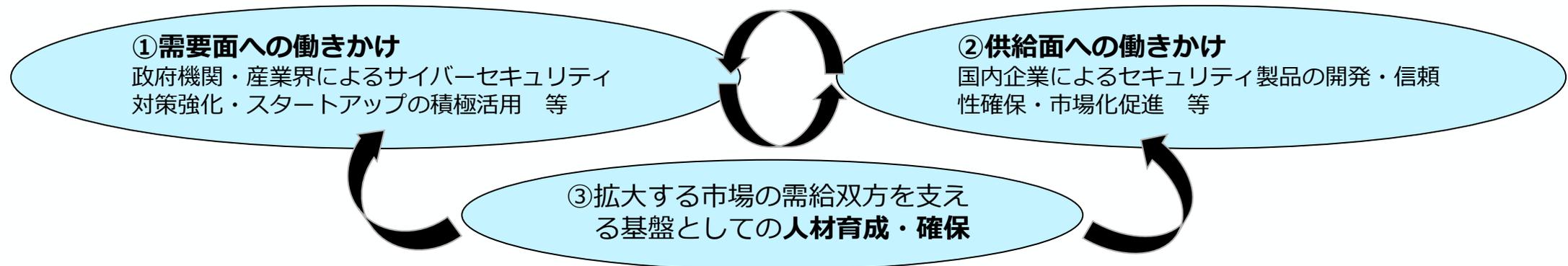
施策の空白地帯

・・・登録セキスペほど高度な知識・スキル水準は求められないが、ある程度の水準を確保した「ちょうど良い」人材が圧倒的に不足。その課題にアドレスする効果的な人材施策もみられない。（試験制度はあるが、実戦的なスキルは測れない。）

(参考) 産業サイバーセキュリティ政策における人材育成・確保施策の位置付け

- 経済産業省では、デジタル時代の社会インフラ（デジタルライフライン）を守り、国民生活や経済活動を守るとの観点から、これまでの施策の一層の普及・啓発などに取り組みながら、政府調達等への要件化を通じた**サイバーセキュリティ対策の実効性強化**や、**セキュリティ市場の拡大に向けたエコシステムを構築**、**官民の状況把握力・対処能力向上**に向けた新たな取組も進めることとしている。
- セキュリティ市場の拡大に向けたエコシステムを構築するためには、産業・技術基盤の維持・発展を支える供給側、セキュリティ対策を実装する需要側、双方の基盤となる人材の育成・確保が重要。
- さらに、NISC改組後の「新たな組織」を含む政府機関等において十分なセキュリティ人材を確保することにより、政府全体でのサイバー安全保障分野での対応能力を向上につなげることも重要。こうしたセキュリティ人材が、産業界に留まることなく、**政府と民間との間でより活発に行き来できるようにすることも必要**。
- こうした視点の下、**セキュリティ人材の裾野を更に拡大していくために必要な施策の在り方を検討する必要**。

<「セキュリティエコノミー」好循環のイメージ>



I - 1 ① 中小企業等の実態を踏まえた人材確保・育成の支援策

- 検討会のテーマ（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）のうち、特に②関係の登録セキスペアクティブリスト・③関係については、**検討会における有識者プレゼン等**（一部個別の意見聴取結果を含む）や令和6年度の予算事業から得られた、**中小企業等の実態を踏まえて検討**。
- 中小企業等がサイバーセキュリティ対策を無理なく実施できる人材面の支援策として、①個社の状況に応じた個別相談・支援が可能な登録セキスペをリスト化した「登録セキスペアクティブリスト」、②セキュリティ対策の内容・人材確保・育成策のエッセンスを段階的に示す「実践的方策ガイド」を活用・普及。

中小企業におけるセキュリティ対策の課題（全般）

「必要性を感じない」

- 回答企業の47%が「対策の必要性を感じたことがない」。
- 中小企業にセキュリティ対策の必要性を提示し、**需要を喚起**する必要。

<中小企業実態調査>

<有識者プレゼン等>

「どこから始めれば良いか分からない」

- 相談会参加者のうち（セキュリティ対策の）「始め方が分からない、相談先が分からない」企業が約8割。
- 各社のセキュリティ課題の**成熟度・領域が多様**で、**サンプル規程もそのまま適用できない**。

<以上セキュリティ人材活用促進実証>

- 自社の**取組の妥当性を第三者的視点で確認**したい、業界別の要求事項を**具体的な対策に落とし込み**たい。

<中小企業実態調査>

「十分なコストをかけられない」

- 「必要性を感じている」企業でも**実施対策はウィルス対策など基本的な対策に限定**。
- 対策を記載した**ガイドラインは長尺で読むことが困難**。

<セキュリティ人材活用促進実証>

<有識者プレゼン等>

社内人材の確保・育成

- 70%が**社内に体制（専門部署等）がなく**、64%が**従業員へのセキュリティ教育を実施していない**。
- 41%が**人材育成のための適切な演習がない・分からない**。

<以上中小企業実態調査>

外部リソースの確保

- 51%の企業が「**困った際の相談先が特にな**い」。
- 情報収集先として、**社外の登録セキスペを活用している企業は2.4%**。

<以上中小企業実態調査>

個社の状況に応じて、セキュリティに関する課題を発見し、対策内容をカスタマイズする個別相談・支援が必要

各所に散らばったセキュリティ対策や人材確保・育成策（教育コンテンツを含む）の標準的なエッセンスを段階的かつコンパクトに示すガイドが必要

相談者のニーズに応じた登録セキスペを探索できる登録セキスペアクティブリスト

（連携）

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

I-1② 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「アクティブリスト」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

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)

<アクティブリストを
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

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

<人材育成・確保の
実践的方策ガイド>

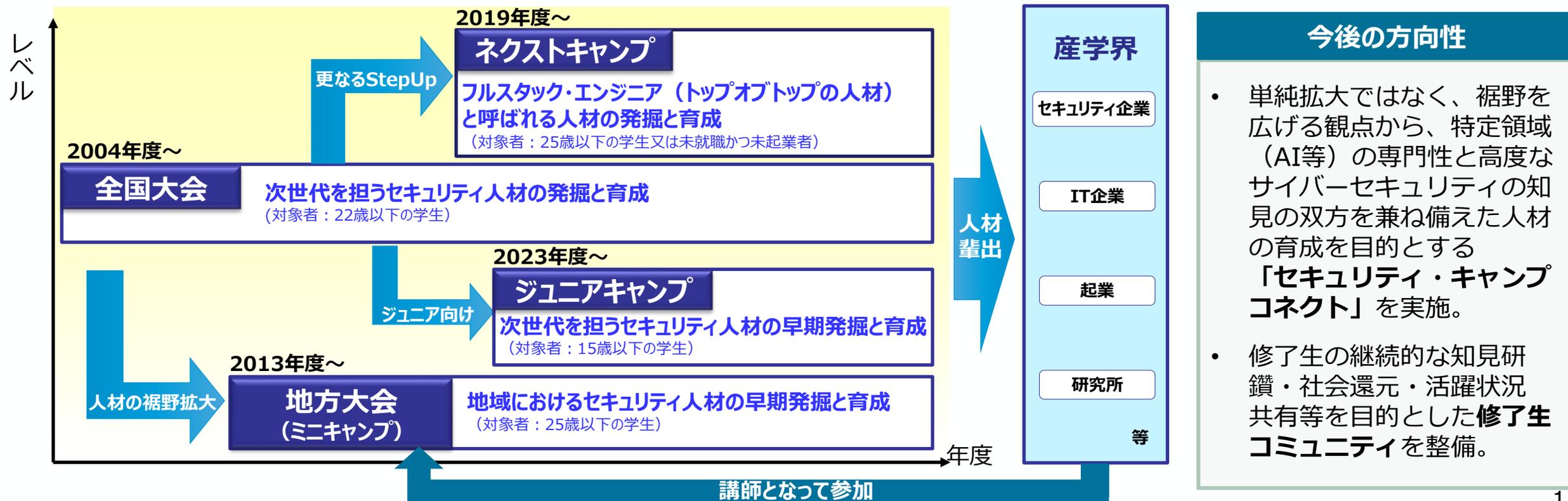
既存ガイドとの
整合確保



(etc.)

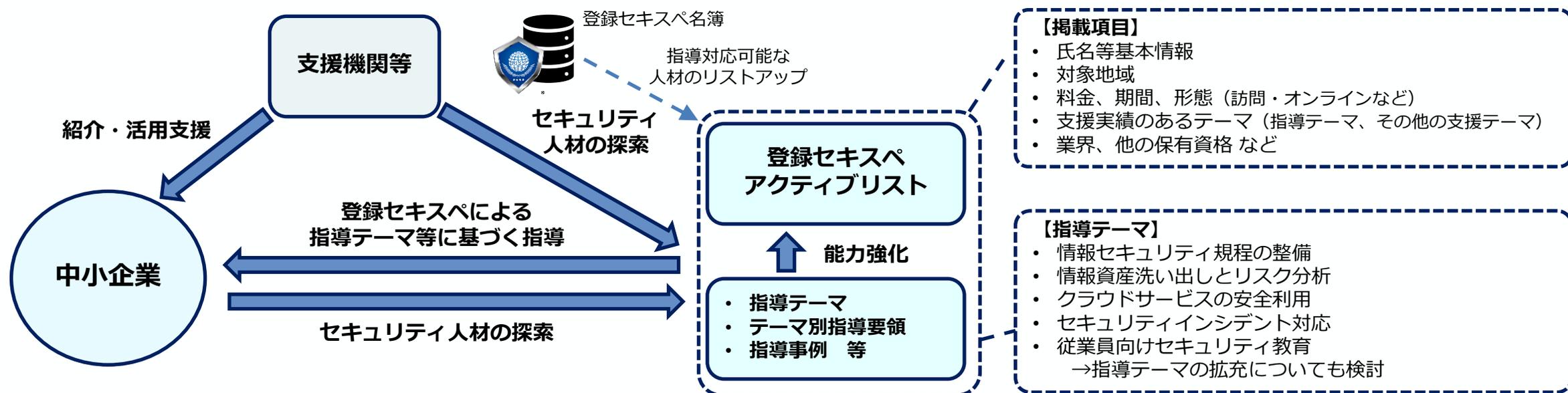
I - 2 セキュリティ・キャンプの拡充

- 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の人材を育成・発掘するため、IPAとセキュリティ・キャンプ協議会が開催。計約1,200名が修了。
- 今後、裾野の拡大に向けた**新たなキャンプ（セキュリティ・キャンプ コネクト）**を実施するとともに、修了生の知見研鑽や活躍状況の共有等を目的とした**修了生コミュニティを整備**。



I - 3 登録セキスペ① (アクティブリストを活用した中小企業支援)

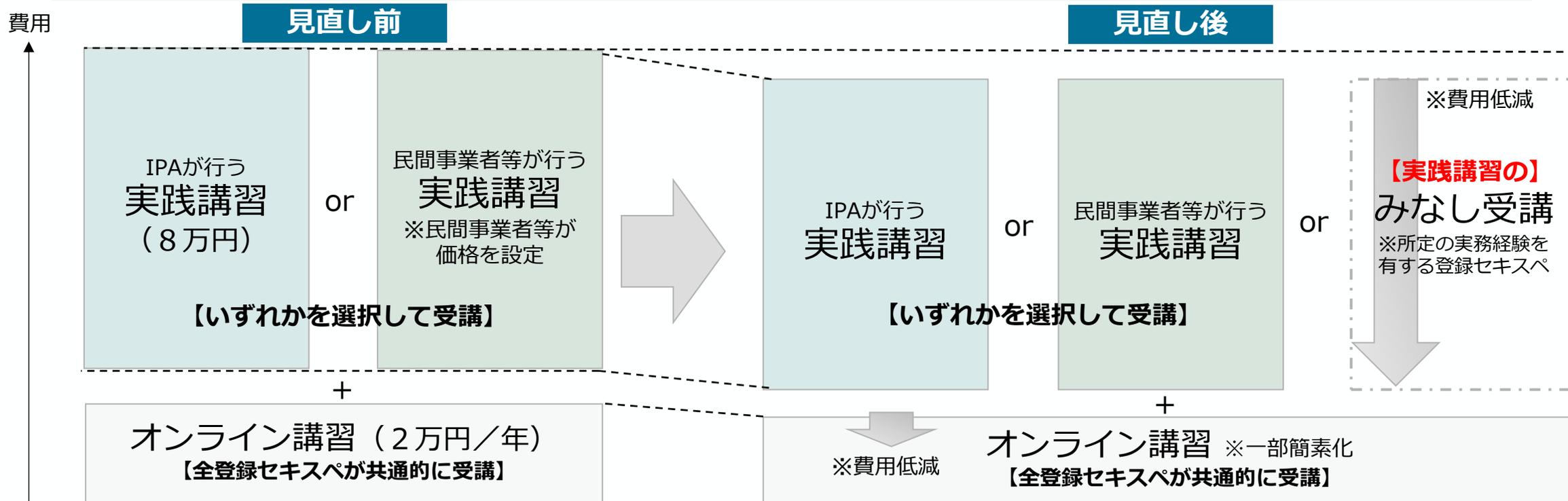
- 令和5年度補正予算事業において、中小企業と登録セキスペのマッチングを促す場を構築し、予め設定した指導テーマに即して、セキュリティの課題を抱える中小企業と登録セキスペの効率的なマッチングについて検証。
- 令和7年度に、検証結果を踏まえ、中小企業等に対するセキュリティコンサルが可能な登録セキスペの得意分野・専門領域を可視化した「登録セキスペアクティブリスト」を整備。
 - リスト掲載項目の一つである指導テーマの拡充など、継続的にリストの掲載内容・運用を改善。
- 「リスト」の活用を通じて、中小企業が多大な探索コストをかけることなく、地域の支援機関等を通じて登録セキスペを活用。登録セキスペにとっても活躍の機会が広がることを期待。



I - 3 登録セキスペ②（みなし受講制度の創設）

- 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、登録セキスペの中には、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ペを実務に向かわせるインセンティブを設定することが、登録セキスペの一層の活用促進、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（令和8年度中に制度開始想定）。



I - 3 登録セキスペ③（その他の登録セキスペ活用促進策等）

登録セキスペの活用促進の取組

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

- 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ペを活用。
- 評価者としての登録セキスペを育成するために、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ペが評価するための指導要領を作成。②併せて、登録セキスペに対して、企業評価のためのスキル（監査スキル）習得機会を提供。

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）

- 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・配置の紐づけを推進（令和6年9月）。
- 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」に登録セキスペの活用を明記（令和7年3月）。

各種投資促進施策における要件化

- 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ペの活用を促進。
- 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、登録セキスペの配置を要件化。

公的機関・重要インフラ事業者等における配置促進

- 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、登録セキスペの活用を推進。
- 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、登録セキスペを明記。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、登録セキスペ制度の紹介及び活用策について周知。

（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ペの活用についても引き続き検討。

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

- 「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。
- 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、登録セキスペの能力向上及びスキル・実績の見える化促進が期待。

情報処理安全確保支援士試験の見直しとの連携

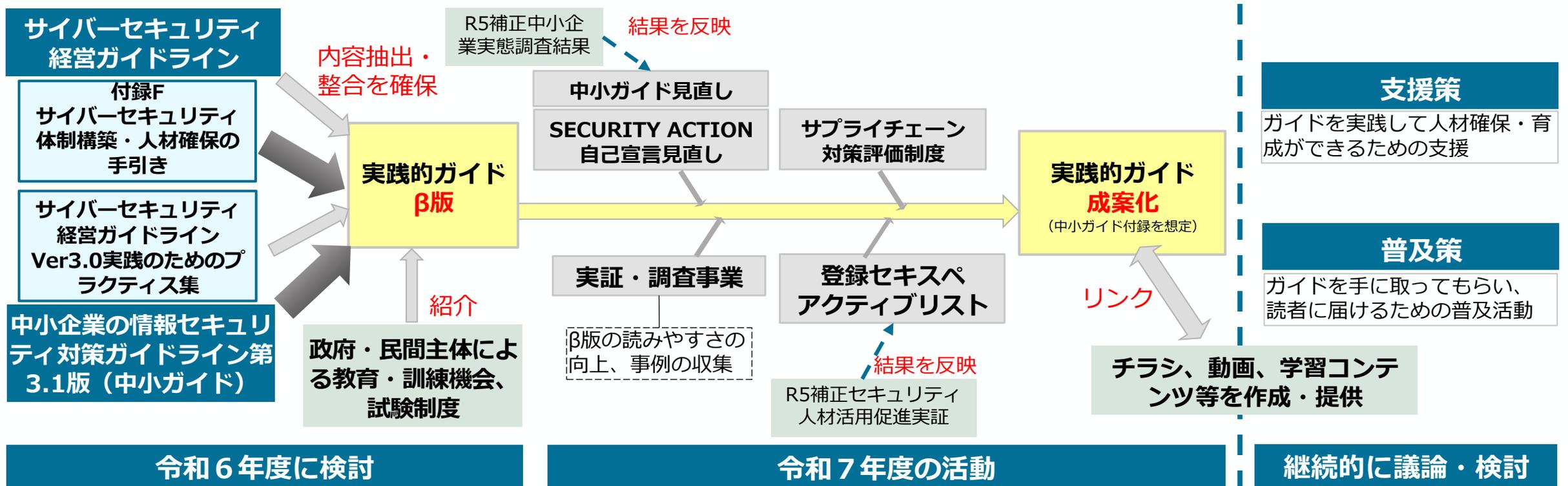
- 「デジタル人材のスキル・学習の在り方ワーキンググループ」において、デジタル人材の類型ごとに求められるスキル習得の考え方・学習の在り方について検討。サイバーセキュリティ分野については、本検討会においても議論。
- 検討会においては、自社内のマネジメント需要への登録セキスペによる対応として、①試験制度自体の複雑化は避けるべきとの考え方とともに、②資格更新時の講習で対応していく考え方や、③試験問題においてマネジメントの要素を増やす考え方を提示。

更新時の義務講習におけるマネジメント要素の習得

- 自社内のマネジメント需要への登録セキスペによる対応として、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。
- 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。

I - 4 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・育成①

- 人材の確保・育成については既に、「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2.0版」等が策定されているところ、使いやすさをより向上させる観点から、**人材確保・育成策の標準的なエッセンスを段階的かつコンパクトに示すガイドを策定**。
- 併せて、セキュリティ対策に関する**経営者へ向けたメッセージ**、**外部人材の活用方策**や**教育・訓練機会**等も提示。
- 既存のガイドライン**等から、具体的なセキュリティ対策や人材の確保策に関する内容を抽出して**整合性を確保**しつつ**充実**を図った上で、「**中小企業の情報セキュリティ対策ガイドライン**」の**付録**とすることを想定。
- 令和7年度、関連施策の進展や実証・調査事業の成果を踏まえ、使いやすさを向上させて成案化。ガイドの普及策やガイドに書かれた方策実行のための支援策は継続的に検討。



I - 4 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・育成②

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) (全体像)

- セキュリティ対策を段階的に4つのStepに分類し、各Stepにおいて、「実施するセキュリティ対策」から「対策実施のためのタスク」、「人材の確保・育成策」に至るまでを提示。
- 自社の状況に応じたStepから、対策実施のためのタスクや人材確保・育成策を参考に取組。



Stepごとに取組を提示

実施するセキュリティ対策

対策実施のためのタスク

人材の確保・育成策

- ▶ 社内人材の確保
- ▶ 外部人材の活用
- ▶ 既存情報・学習コンテンツ・セミナーの活用
- ▶ 試験・資格の活用

サイバーセキュリティお助け隊サービス <https://www.ipa.go.jp/security/otasuketai-pr/>

取組の開始前や各Stepの取組と合わせて、中小企業のサイバーセキュリティ対策に不可欠な各種サービス（見守り、駆付け、保険）をワンパッケージで安価に提供する、国が認定したセキュリティサービスである「サイバーセキュリティお助け隊サービス」の導入が有効。

情報処理安全確保支援士（登録セキスペ） <https://www.ipa.go.jp/jinzai/riss/index.html>

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である情報処理安全確保支援士（登録セキスペ）への相談も有効。サイバーセキュリティに関する相談に応じて、企業の取組に対して分析や評価を行い、その結果に基づいて指導・助言。

(参考) 令和5年度補正予算事業① (セキュリティ人材活用促進実証の概要)

- 物価高や最低賃金引上げ等により中小企業等における資金的余力や人材確保が厳しい状況にある中、セキュリティ専任の部署（担当者）が置かれるケースは少なく、多くは兼務となっており、セキュリティ業務の外部委託も進んでいない。その要因の1つとして、**セキュリティ人材に関する需要と供給の適切なマッチングがされていないことが考えられる。**
- 令和5年度補正予算事業において、**中小企業等と登録セキスペとのマッチング**を促す場を構築する実証事業を実施し、**登録セキスペの社外における活用と、中小企業等がセキュリティ人材を探索しやすくするための環境整備**を検討。
- 具体的には、**商工会議所と連携したサイバーセキュリティ相談会**を実施し、相談会参加企業105社のうち34社が登録セキスペとマッチング。**登録セキスペによる訪問指導**を実施。

〔中小企業等と登録セキスペのマッチングフロー〕

商工会議所と連携したサイバーセキュリティ相談会

- 商工会議所と連携したサイバーセキュリティ相談会を開催。
- 専門家によるセキュリティ対策の必要性等を訴求する基調講演を実施。

登録セキスペによる個別相談

- 相談会参加者のうち希望者に対して登録セキスペによる個別相談を実施。
- 自社のセキュリティ対策の課題を特定・優先づけを実施。

登録セキスペによる訪問指導

- 個別相談参加者のうち希望者に対し、**5つの指導テーマ**の中から選択したテーマについて伴走支援（3回実施し、各回ごとに目標を設定）。

〔相談会・個別相談の実施結果〕

相談会参加者アンケート・個別相談の結果

- セキュリティに対する意識がある社の中で、**どこから始めたらよいか分からない、どこに相談したらよいか分からない社が約8割**存在した。
- セキュリティ専門家を選定するときに重視する点として、「**緊急時の対応力**」「**提案内容の具体性**」「**セキュリティ専門家の技術力・専門性**」「**自社の業界に対する理解度**」「**コスト**」が上位に挙がった。
- 支援を希望する内容**（個別相談の中で明らかになったものを含む）として、「**従業員向けセキュリティ教育の実施支援**」「**取引先から／取引先への要求事項への対応支援**」「**情報セキュリティ規程の作成・改訂支援**」「**現在の社内のセキュリティ対策状況の診断**」が上位に挙がった。
- セキュリティ専門家の探索手法として望ましいと考えるものとして、「**公的機関（IPA等）における専門家リストの利用**」のほか、「**商工会議所等の中小企業支援機関による紹介・マッチング支援サービス**」「**取引のあるITベンダーからの紹介**」が上位に挙がった。

個別相談における具体的な相談内容

- 各社におけるセキュリティ課題は、その**成熟度や課題領域において非常に多様**。
- 「**サンプル規程があることは知っているが、それをどのように使用し、自社用に作り直せばいいのかわからない**」など**具体的なアドバイス**を求める相談が見られた。
- 「**作成した規程の内容が本当に十分か、自社に合っているか**」など、**自社の判断・取組の妥当性を専門家の第三者的な視点から確認したい**というニーズも存在。
- 業界別の対策水準の要求等の確保**を目的としたセキュリティ対策の相談が多く、**要求事項を自社に即した具体的な対策として落とし込む方法**について、実践的な示唆を求める声が複数確認。

(参考) 令和5年度補正予算事業② (セキュリティ人材活用促進実証の概要)

〔訪問指導の実施結果〕

指導実施企業からの声

- アクティブリストの活用（マッチング方法含む）に関するもの
 - 自社の状況や課題について共有する個別相談を経て取るべき対策が明確になり、訪問指導をお願いする事を決めた。いきなり課題解決のための具体的な指導を行う訪問指導に入られるのは抵抗があり、まずはセキュリティ専門家と企業とのマッチング機会があることが重要
 - 商工会議所で開催されるということで安心感がある。商工会議所からの専門家紹介は、中小企業の身の丈にあった支援を行ってくれるという信頼性がある。
 - 商工会議所でリストを使った専門家紹介事業を行うのであれば、十分活用の可能性がある
 - その他、取引先や業界団体からの案内があれば、活用を検討できる。
 - 簡単には有料で専門家の指導を受けることを決められない。一方で、この専門家であれば信頼できると判断できれば、無料指導を経た上で有料指導につながり得るため、「初回お試し無料」のような項目があれば有益である。
 - 他の企業と話す機会があったが、どこもセキュリティ業務が兼務となっており、相談先がないという困りごとは必ず出ていた。ITベンダー等のサービスを利用する手前の段階で、気軽に相談できる先として専門家が可視化されたリストがあれば大変助かる。しかもIPA等信頼できるところからの情報であるとありがたい。
- アクティブリストの項目に関するもの
 - 専門家探索をする際には、まず地域を見るはずである。地元の専門家の方が圧倒的にコミュニケーションを取りやすい。
- アクティブリストの管理運用に関するもの
 - 信頼できる機関が発表しているリストであれば使うだろう。情報の更新頻度が重要な要素。

指導専門家（登録セキスペ）からの声

- アクティブリストの活用（マッチング方法含む）に関するもの
 - 自社の状況や課題について共有する個別相談であらかじめ方向性を整理することで、課題解決のための具体的な指導を行う訪問指導に際して、すぐに本格的な作業に取りかかることができた。指導に入る前に、企業側での取り組みに対する熱量や考えを知ることができるのは、効率的に指導を実施する上で重要。
- アクティブリストの活用（指導テーマ含む）に関するもの
 - 標準的な進め方、スケジュール、達成レベル感を示された企業支援のための指導要領は有効に活用できた。
 - 支援テーマについては、入口ではあまり細かく絞らず、些細な「相談ごと」からでも、専門家にアクセスできるようになればよい。
- アクティブリストの項目・管理運用に関するもの
 - リストのデータ更新は必須。どういう企業でどのような活動をしてきたか実務経験が分かった方がよさそう。
- その他
 - 講習受講はそれなりに負担である。謝金をいただきながら活動した内容が資格維持に活用できるのであればありがたい。

(参考) 令和5年度補正予算事業③ (中小企業実態調査の概要)

- 過去の調査によると、企業によってセキュリティ対策に支出可能な金額は大きく異なっており、また、セキュリティ対策に当たっては「コストや自社のセキュリティ体制とレベルに応じた対策をしたい」と回答した企業は約4割程度存在。企業によってIT依存度も異なり、**セキュリティ対策に支出できる費用や対策を実施できる体制も異なる**。
- そこで、昨年にかけて、令和5年度補正予算事業として、**中小企業等の規模や業種、IT依存度、セキュリティ対策の実施状況の実態**を明らかにするため、調査を実施した。本事業のアンケート調査で得られた結果の概要は以下のとおり。

調査概要

| | |
|------|--|
| 調査手法 | <ul style="list-style-type: none">ウェブアンケート |
| 調査項目 | <ul style="list-style-type: none">企業概要サイバーセキュリティ対策への取組状況、体制、教育等IPA施策の認知度・効果及び利用状況等 |
| 回答数 | <ul style="list-style-type: none">4,000件以上 |

アンケート調査の結果

セキュリティ対策の実施状況等

- 回答企業の47%が「**セキュリティ対策の必要性を感じたことがない**」
 - セキュリティ対策の必要性を感じていると回答した企業についても、**実施している対策はウィルス対策やファイアウォールなど基本的な対策に限られている**
- SECURITY ACTION一つ星に相当する簡易なセキュリティ対策について、4割程度の企業が実施していない
- 回答企業の36%が、情報セキュリティ対策を実施する効果として「**対処すべきリスクの特定**」を期待

社内の知識不足、人材育成等

- 回答企業の70%において**セキュリティ対策に関わる社内体制が無い**（専門部署、兼務担当者の任命がない）
 - 企業のセキュリティ対策向上のために主な必要な事項として「**経営者のリスク意識向上**」「**従業員の意識向上**」「**企業内の体制整備**」「**従業員への実践教育**」
- セキュリティ対策に関して活用したいサービスとして「**経営層向けの手引書**」（29%）「**経営層向けの教育**」（22%）が挙げられており、多くの企業で経営層のセキュリティ対策の知識不足を不安視
- 回答企業の64%が**従業員に対する情報セキュリティ教育を「特に実施していない」**
 - 人材育成のための外部研修を活用していない・活用する意向がない理由としては、「**適切な演習がない・わからない**」（41%）が主

外部リソースの活用状況

- 回答企業の51%にとって、セキュリティに関して「**困った際の相談先が特にない**」
- 情報セキュリティ対策に関する**情報収集先として、社外の登録セキスペを活用している回答企業は2.4%**にとどまる
- 回答企業の70%が**情報セキュリティ業務について外部委託を行っていない**

(参考) 有識者プレゼンにおける主な御意見

(登録セキスペアクティブリスト)

➤ アクティブリストの活用に関するもの

- セキュリティに関しては、中小企業側の需要が小さいからマーケットとして未成熟であり、**中小企業に対してセキュリティ対策の必要性を提示し、需要を喚起することが必要**では。
- 中小企業の支援機関には、セキュリティに特化して相談に乗ることができる職員が殆どいない。セキュリティに関する相談に対応することができる下地を作るため、**支援機関自身がアクティブリストを使用し、指導員への研修などに活用することで、会員企業に対して広く相談対応ができるような人材を育成**するべきでは。
- アクティブリストの活用により、支援機関における**支援項目や企業支援件数の増加**など、これまでになかった**専門家との結節点が増える**ことは、**支援機関としての活動量が拡大に寄与**するためメリットである。
- その他、土業団体、金融機関、業界団体、ITベンダー等に対しても活用を促し、**情報処理安全確保支援士会を中心とした組織的な対応が有効**では。
- **地域SECURITYとアクティブリストに掲載された登録セキスペをつなげる**ことで、相談先の課題解決と伴走支援につながるのでは。
- **地域においては、信用・信頼・顔が見えるということが重要**であり、登録セキスペについても、その実績等を踏まえて自信もって紹介する必要があるのでは。

➤ アクティブリストの項目に関するもの

- 専門家の情報として、**業務形態**（インハウス/独立）、**指導形態**（訪問/オンライン）による**料金区分**、**初回無料の有無**、**他の保有資格**などがあると選びやすい。
- **自己申告の項目と、客観的に検証可能な項目**（例：義務講習の受講状況）は**分けて設定**してはどうか。
- リスト上で、**登録セキスペが自身のステータス**（例：現在対応不可）を設定できることが望ましい。

➤ アクティブリストの管理運用に関するもの

- **検索順位の上位に問合せが集中しないような工夫**も必要ではないか。
- **登録のための一定の能力担保の仕組み**が必要ではないか。
- 支援する人によって**推奨する対策に大きな差異が生じない仕組み**が必要では。

➤ その他

- 副業禁止などの事情によってリストに登録できない人材の登録を促すため、**リスト登録による中小企業等のセキュリティ対策支援は、登録セキスペを擁している企業にとっても、人材育成等の観点から有意義**である旨を**政府から発信**してはどうか。

(参考) 有識者プレゼンにおける主な御意見

(人材確保・育成のための実践的方策ガイド)

➤ 実践的方策ガイドβ版に反映したもの

- セキュリティ対策においては、PDCAサイクルを意識することが重要であることから、**継続的に対策を見直す必要性を訴求する必要**。
- どんなに技術的なセキュリティ対策を取っても、**人の脆弱性**で攻撃を受けてしまうことから、**社内リテラシー、社内教育が必要**。
- ガイドの名称に関しては、**人材の確保・育成に関するものであることが把握可能なものを示す必要**。

➤ 令和7年度に調査・実証等するもの

- 大企業や海外ではなく、**国内の中小企業による取組事例を生々しく発信すべき**。そして、企業の規模や産業別に事例を収集できると良い。
- 多忙な中で、**長いガイドを読むことは難しく、映像コンテンツによる訴求が有効**では。
- 実践的方策ガイドを踏まえて、**中小企業に受け取ってもらいやすいコンテンツを提供し、ユーザに届ける役割を**（民間企業として）担うことが考えられる。

- I 検討会における議論の全体像
- II セキュリティ・キャンプ**
- III 登録セキスペ
- IV 中堅・中小企業等の内部でセキュリティ対策
を推進する者の確保・育成

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 新たなキャンプ（セキュリティ・キャンプ コネクト）
 - ①基本的な考え方
 - ②令和7年度の実施概要
- 3 修了生コミュニティ
 - ①整備内容
 - ②令和7年度の活動概要

Ⅱ-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。

(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。



(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。



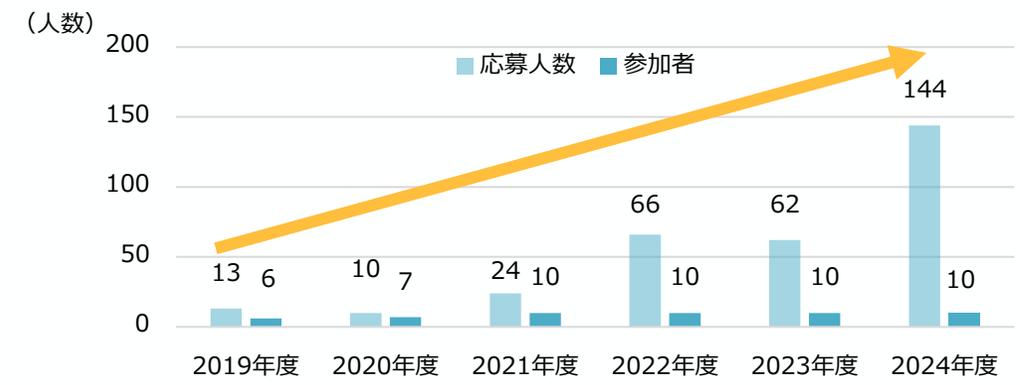
(1) **新たなキャンプの実施**

(2) **修了生コミュニティの整備**

全国大会の参加状況

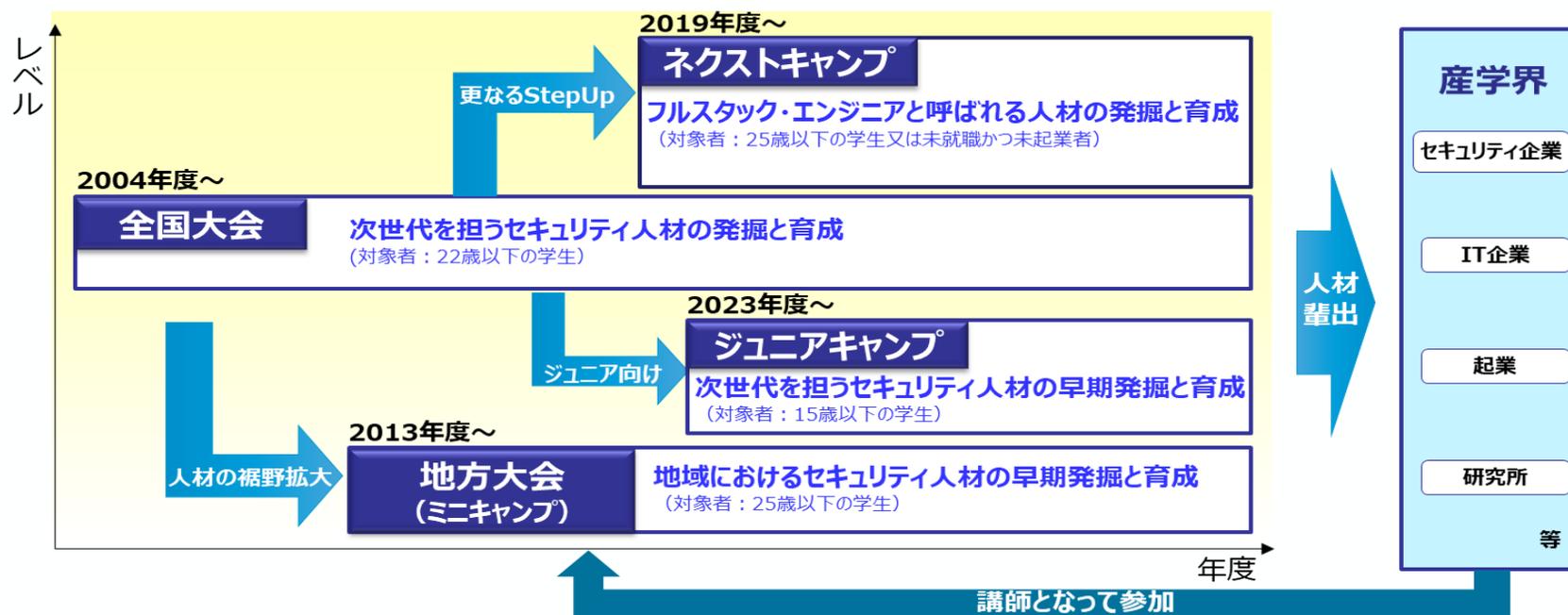


ネクストキャンプの参加状況



(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。



Ⅱ - 2 新たなキャンプ（セキュリティ・キャンプ コネクト）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。

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）**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、産業界とも連携しつつ検討。

(参考) 新たなキャンプに関する第3回までの主な御意見

取組

- 「特定の専門領域における高度な知見・技能を有するもの」として、裾野を広げられるかが課題。サイバーセキュリティは総合力が必要となるため、様々な分野と結びつく必要があり方向性は非常に良い。育成する人数を増やすことが重要。現状の枠組みでは、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。
- 学生に広めやすくなるような工夫が必要。(経済産業省側から公的なものとアナウンスいただく、セキュリティ・キャンプが大学の単位として認められるようにする等)

講師

- 企業内において問題解決に取り組んでいる(実践的に取り組んでいる)人材が講師を受け持つことは、受講生にとっても魅力的にみえると考えられる。
- 講師の自主性に頼らず、講師の輪を広げていくことが課題。

専門領域の選定方法

- 産業分野(例：自動車、宇宙、電力)とのコラボレーションや技術分野(例：AI・IoT・量子コンピュータ)とのコラボレーションがある。
 - 産業要素で領域を特定し、業界ごとの固有の考え方を考慮する場合、制度の設計が難しくなる可能性。
 - 汎用的な技術領域と特定事業領域があるが、DXを進めるユーザ企業では、汎用的技術領域よりも特定事業領域のセキュリティエキスパートが即戦力として求められている。
- 「デジタルスキル標準」に示されたロールごとに、今までの施策と整合をとりながら対象分野を整理。
- ニーズのある分野から始め、徐々に対象分野を広げる。最終的には、産学連携で自走する形が望ましい。

Ⅱ - 2 新たなキャンブ (セキュリティ・キャンブ コネクト) の実施

② 令和7年度の実施概要

- セキュリティ以外の特定の専門領域分野をテーマとして取り扱う初の試みであるため、**令和7年度はプレ開催と本開催の2段階で展開**し、事業のブラッシュアップを図る（プレ開催における受講者の反応や議論の進行状況を踏まえ、その結果を本開催の設計に反映させて内容を改善する予定）。

1. 実施概要

| | プレ開催 | 本開催 |
|------|--|--------|
| 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） | |
| 人数 | 15名程度 | 50名程度 |
| 開催時期 | 令和7年9月 | 令和8年3月 |
| 開催方法 | 対面 もしくは オンライン | |
| 構成 | <ul style="list-style-type: none"> プレ開催は本開催のテーマの一部で実施することを想定。 令和7年度は、本開催に先立ちプレ開催を行い、本開催の募集事項にプレ開催の結果を掲載することで、具体的なイメージを持ってもらえるような形で募集を進める予定。 セキュリティ以外の専門領域については、受講生は、複数のテーマから一つを選択。また、倫理等の共通講義を設けることを想定。 キャンブはゼミ形式で実施し、受講生同士の相互作用やつながりを大切に、グループワークを積極的に行うことを想定。 | |

2. セキュリティ以外の専門領域の選定方法

- セキュリティ以外の専門領域について、**産業分野別、技術分野別、社会科学などの観点を軸**として、複数のテーマを選定。
- 選定したセキュリティ以外の専門領域については、その時々**の産業界のニーズ等を踏まえ、継続的に見直し**。
- 協賛企業を募り、規模を拡大するために、**発表会や協賛プログラムの実施について産業界と連携しながら検討**。

3. 令和7年度のスケジュール

| | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 1 | 2 | 3 | 4 |
|--------|---|---|---|-----------|---|----------------|-------|----|----------|---|---|---|------|
| コネクト | | | | | | | ★プレ開催 | | | | | | ★本開催 |
| | | | | ●プレ開催募集開始 | | | | | ●本開催募集開始 | | | | |
| 既存キャンブ | | | | | | ★全国大会、ネクストキャンブ | | | | | | | |
| | ← | | | | | ミニキャンブ | | | | | | | → |

II - 3 修了生コミュニティ ① 整備内容

- 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の連携・協力)
- ※修了生による社外での社会貢献活動の意義を経営者に向けて発信することを検討
- 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年度中の修了生コミュニティの開始に向けて準備を実施する。**

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 | <ul style="list-style-type: none"> ・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 | <ul style="list-style-type: none"> ・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 |
| | 修了生が活動状況/研究成果を発表する機会を得る | <ul style="list-style-type: none"> ・キャンプフォーラムへの参加 |
| 情報発信・情報交換 機会の提供 | 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 | <ul style="list-style-type: none"> ・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 | <ul style="list-style-type: none"> ・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 |

II - 3 修了生コミュニティ ②令和7年度の活動概要

- 今年度は、セキュリティ・キャンプ修了生同士の情報共有及び教育機関・公共機関等への情報発信のためのプラットフォーム（SNSツール）を整備。総会、ジュニア支援（修了生ゼミ）などの修了年次を超えた人脈形成、情報交換・人材交流の場イベント開催を行うとともに、修了生活躍状況の可視化による産業界へのアピール、裾野拡大支援等のセキュリティ・キャンプの価値向上に向けた後方支援も合わせて実施。

1. 令和7年度の活動内容

- ① セキュリティ・キャンプ修了生同士の情報共有及び教育機関・公共機関等への情報発信のためのSNSツールを整備。そして、セキュリティインシデントが発生した場合における修了生同士の対処に向けた協力等、特定の目的に応じたグループを組成し、その中での情報共有や課題解決を行う場を提供。
- ② 年1回の総会を開催し、セキュリティ・キャンプの修了年次を超えた人脈形成、情報交換・人材交流の場を提供。
- ③ 修了生からのニーズを踏まえ、(1)セキュリティ・キャンプ全国大会で好評であった講義の受講（ワークショップ）や、(2)セキュリティ・キャンプで習得した知識・スキルを用いた研究の成果発表（成果発表会）等の機会を設け、修了生の知識・技能の研鑽の場を提供するとともに、修了生の知見やノウハウを社会に還元。具体的には、修了生のアンケート結果で特に好評であったセキュリティ・キャンプ全国大会中の講義（例：『プロダクト開発を攻撃者の視点で捉える』『マルウェア解析の基礎と応用』等）をテーマとして実施。
- ④ 修了生が講師となり、潜在的なセキュリティ・キャンプ参加者の発掘に向けた小中高生を対象とした講座開催等（若年層講座）を実施し、セキュリティ・キャンプの裾野拡大を図る。
- ⑤ こうした取組に加え、修了生コミュニティへの参加レポートや修了生の職業上の活躍状況の広報周知を実施。

2. 令和7年度のスケジュール

| | 8月 | 9月 | 10月 | 11月 | 12月 | 1月 | 2月 | 3月 |
|----------------|-----------------------------|----|------------|-----|-----|------------|-----|----|
| ①SNSツール整備 | ●サービスイン→ | | | | | | | |
| ②総会 | | | | | | | ●実施 | |
| ③ワークショップ・成果発表会 | | | ←●実施（1回目）→ | | | ←●実施（2回目）→ | | |
| ④若年層講座 | | | | | ●実施 | | | |
| ⑤活躍状況の広報周知 | ●webページ/コミュニティサイト等での紹介（逐次）→ | | | | | | | |

- I 検討会における議論の全体像
- II セキュリティ・キャンプ
- III 登録セキスペ**
- 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確保・育成

Ⅲ 登録セキスペ

- 1 登録セキスペの現状・課題・方向性
- 2 登録セキスペに係る施策の分類・整理
 - ①登録セキスペの能力向上、スキル・実績の見える化
 - ②ユーザー企業における登録セキスペの活用
 - ③更新コストの低減

Ⅲ - 1 登録セキスへの現状・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。

(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げていない。

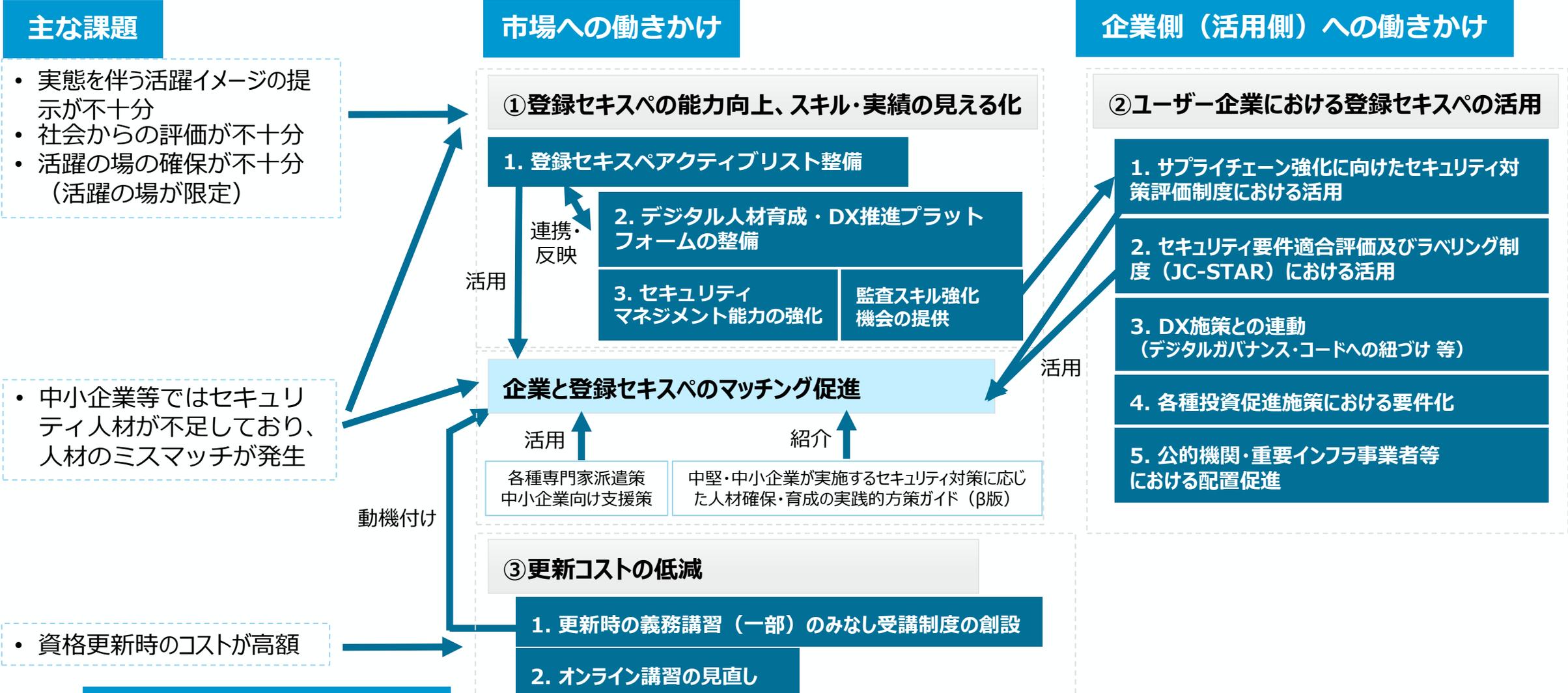
活躍の場がないとする登録セキスがいる一方、人材不足を課題に上げる中小企業等もあり、ミスマッチも発生。

(2) 資格更新時の高額なコストの見直しが必要。

(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

Ⅲ - 2 登録セキスペに係る施策の分類・整理

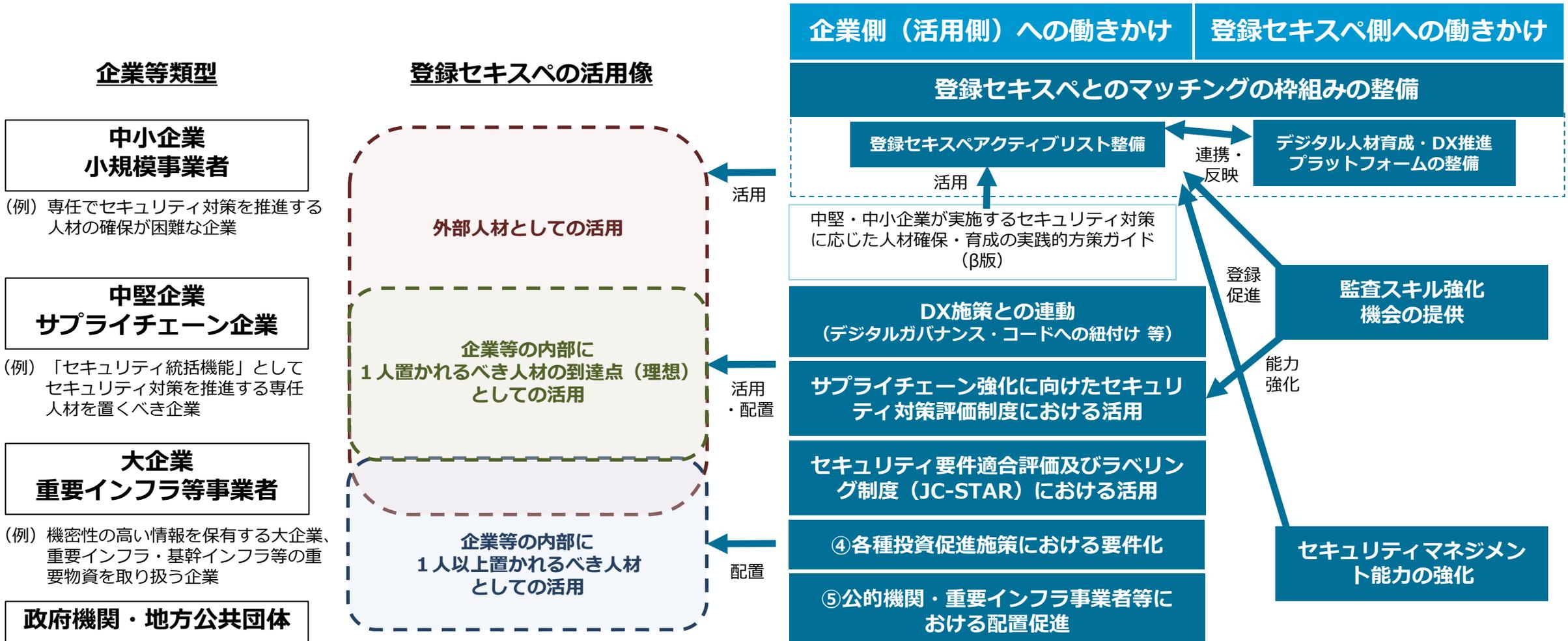


施策により期待される効果

- 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ことで、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。

(参考) 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。

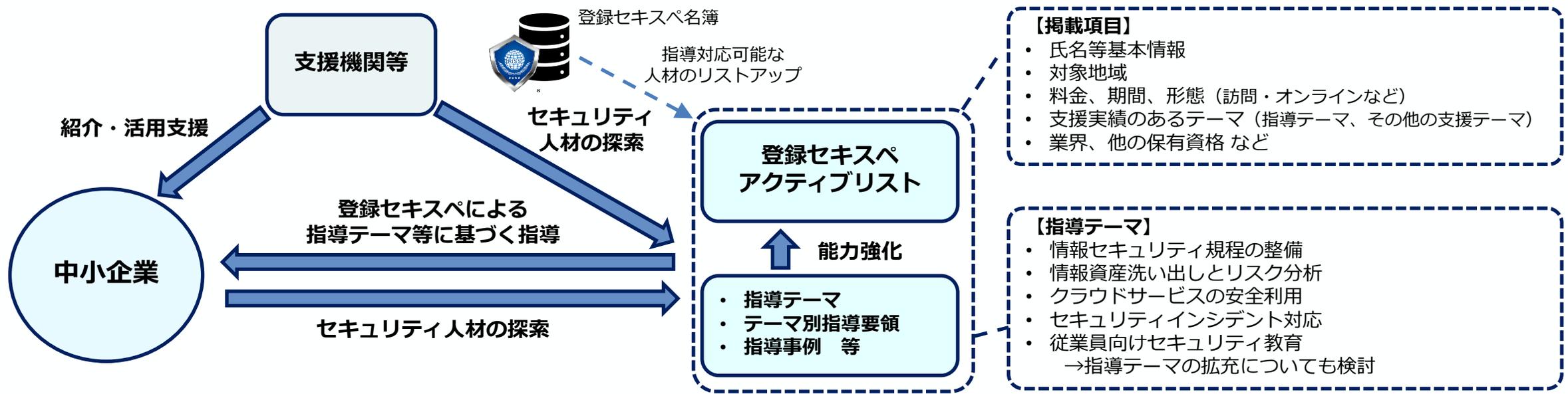


Ⅲ - 2 登録セキスペに係る施策の分類・整理

① 登録セキスペの能力向上、スキル・実績の見える化

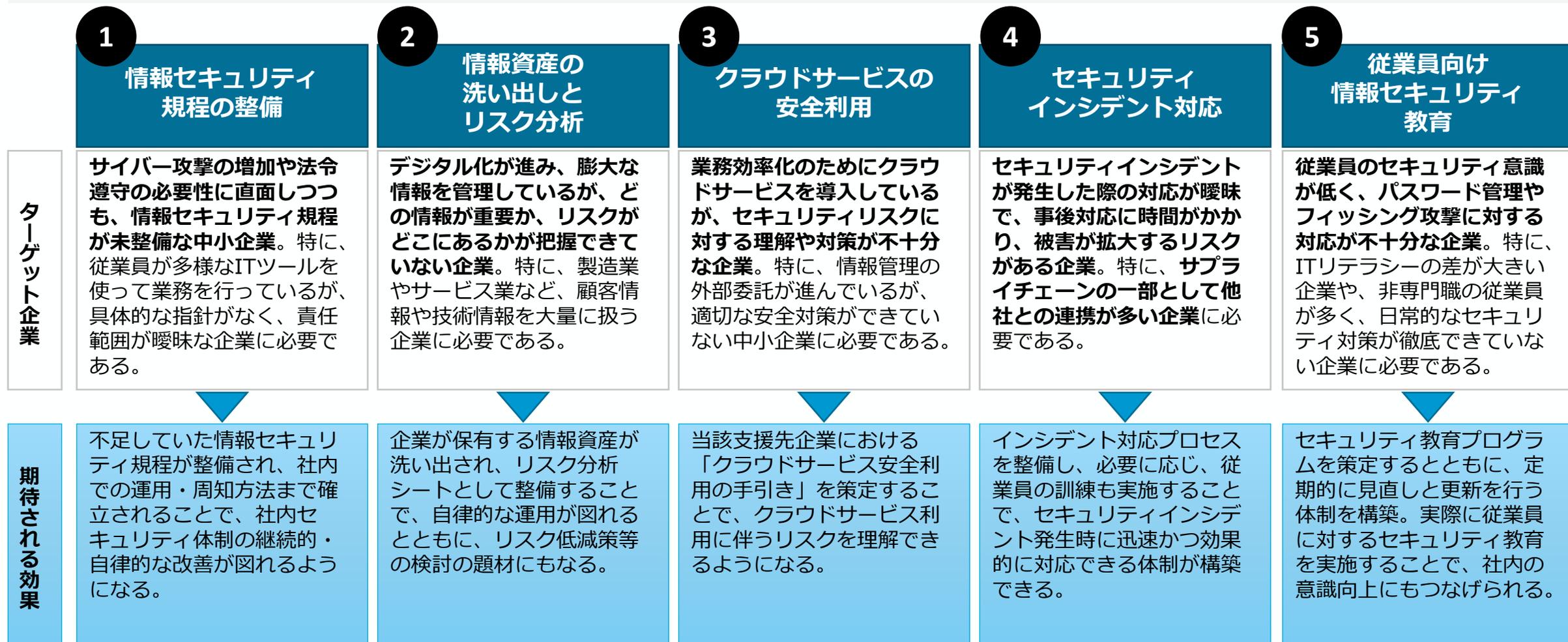
1. アクティブリストを活用した中小企業支援（再掲）

- 令和5年度補正予算事業において、中小企業と登録セキスペのマッチングを促す場を構築し、予め設定した指導テーマに即して、セキュリティの課題を抱える中小企業と登録セキスペの効率的なマッチングについて検証。
- 令和7年度に、検証結果を踏まえ、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・専門領域を可視化した「登録セキスペアクティブリスト」を整備。
 - 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) セキュリティ人材活用促進実証 (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。



(参考) 指導テーマと情報処理安全確保支援士試験シラバスの関係

- 令和5年度補正予算事業（セキュリティ人材活用促進実証）において設定した指導テーマは、情報処理安全確保支援士試験（レベル4）シラバスとの対応関係を意識して設定。

| 指導内容 | | 情報処理安全確保支援士試験（レベル4）シラバスとの対応 | |
|--------------------------|--|---|--|
| 指導テーマ | 指導テーマの達成目標 | シラバス大項目 | シラバス小項目 |
| 指導テーマ① 情報セキュリティ規程の整備 | 【達成目標1】現状における自社の情報セキュリティリスクの洗い出し 【達成目標2】情報セキュリティ基本方針の作成及び既存規程のチェック 【達成目標3】情報セキュリティ関連規程（案）の策定 | 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 | 1-1 情報セキュリティ方針の策定 1-4 情報セキュリティ諸規程の策定 1-6 情報セキュリティに関する動向・事例の収集と分析 |
| | | 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 | 3-1 暗号利用及び鍵管理 3-2 マルウェア対策 3-6 脆弱性への対応 3-9 人的管理 3-11 コンプライアンス管理 |
| | | 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 | 4-1 情報セキュリティインシデントの管理体制の構築 |
| | | | |
| 指導テーマ② 情報資産の洗い出しとリスク分析 | 【達成目標1】現状における自社の情報セキュリティリスクの洗い出し 【達成目標2】自社における情報資産の洗い出し 【達成目標3】抽出した情報資産リストに対するリスク分析の実施 | 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 | 1-2 情報セキュリティリスクアセスメント 1-3 情報セキュリティリスク対応 1-6 情報セキュリティに関する動向・事例の収集と分析 |
| | | | |
| 指導テーマ③ クラウドサービスの安全利用 | 【達成目標1】現状における自社の情報セキュリティリスクの洗い出し 【達成目標2】自社における現状導入済み/利用予定クラウドサービスの洗い出し 【達成目標3】抽出したクラウドサービスに対する安全利用チェック | 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 | 1-4 情報セキュリティ諸規程の策定 1-6 情報セキュリティに関する動向・事例の収集と分析 |
| | | 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 | 2-2 製品・サービスのセキュアな導入 |
| | | 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 | 3-3 バックアップ 3-8 アカウント管理及びアクセス管理 |
| 指導テーマ④ セキュリティインシデント対応 | 【達成目標1】現状における自社の情報セキュリティリスクの洗い出し 【達成目標2】インシデント対応手順書の作成 【達成目標3】作成したインシデント対応手順書に基づく机上演習の実施 | 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 | 1-6 情報セキュリティに関する動向・事例の収集と分析 |
| | | 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 | 3-2 マルウェア対策 3-4 セキュリティ監視並びにログの取得及び分析 3-7 物理的セキュリティ管理 |
| | | 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 | 4-1 情報セキュリティインシデントの管理体制の構築 4-2 情報セキュリティ事象の評価 4-3 情報セキュリティインシデントへの対応 4-4 証拠の収集及び分析 |
| | | | |
| 指導テーマ⑤ 従業員向け情報セキュリティ教育 | 【達成目標1】現状における自社の情報セキュリティリスクの洗い出し 【達成目標2】サイバーセキュリティに関する従業員教育の実施 【達成目標3】教育実施結果のレビューと、以後の継続実施に向けた教育計画の策定 | 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 | 1-6 情報セキュリティに関する動向・事例の収集と分析 |
| | | 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 | 2-7 運用・保守（セキュリティの観点） |
| | | 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 | 3-9 人的管理 |
| | | 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 | 4-3 情報セキュリティインシデントへの対応 |

登録セキスペアクティブリストの基本設計（案）

- 令和5年度補正予算事業を踏まえ、登録セキスペアクティブリストの基本設計について、以下のとおり整理。
- 令和7年度において、登録セキスペアクティブリストを整備し、運用開始を目指すとともに、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。

1. リストの内容

| | |
|-------|---|
| 掲載対象者 | <ul style="list-style-type: none">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が掲載対象。 ※ 登録セキスペとしての専門的知識・技能を所属組織のセキュリティ対策のために発揮することが予定されている者で副業・兼業ができないものは、掲載の対象外と想定（所属組織が中小企業等に対するセキュリティコンサルを行っている場合は、掲載の対象と想定）。 |
| 掲載項目 | <ul style="list-style-type: none">企業・支援機関等に対して、「どのような支援を行うことができるか」を示す項目を提示。具体的な項目としては、氏名・連絡先・対象地域、料金・期間・形態（訪問・オンラインなど）のほか、支援実績のあるテーマ（指導テーマその他の支援テーマ）・業界・他の保有資格などを想定。 |

2. リストの管理運用

| | |
|--------|--|
| 管理運用主体 | <ul style="list-style-type: none">指導テーマの管理と併せてIPAとすることを想定。 ※ 掲載項目のブラッシュアップ等に当たっては、関係団体と連携することも想定。 |
| 登録方法 | <ul style="list-style-type: none">既存の登録セキスペについては、リスト登録を案内し、登録申請を受けることを想定。また、新規登録・更新時にもリスト更新を案内することを想定。 ※ 令和5年度補正予算事業の成果物としてのリストにおいては、同事業の訪問指導の実績がある者を中心に掲載。令和7年度以降は、対象者を拡充することを想定。 |

2. リストの管理運用（続き）

| | |
|------|---|
| 更新方法 | <ul style="list-style-type: none">登録者自らによる更新を想定。確実に更新いただくため、更新等の機会を捕まえて、管理主体から更新依頼をすることも一案。後述のみなし受講制度の対象となる実務経験等に「指導テーマ」の実務を得出しして位置付け、情報更新の誘因とすることも一案。 |
| 活用方法 | <ul style="list-style-type: none">リストは公開し、企業側の発意による利用が可能。セキュリティ対策をどこから始めたらよいかわからない、どこに相談したらよいかわからない企業や、具体的なセキュリティ対策を実施したい企業が直接利用することを想定。他方で、実証事業の結果を踏まえ、商工会議所等の支援機関（※1）や、ITベンダー（※2）等の中小企業の相談先を介した活用も想定。 （※1）令和5年度補正予算事業の中小企業と登録セキスペのマッチング事業において、支援機関を介したマッチングを検証。 （※2）令和5年度補正予算事業において素案を作成した地域ベンダー向け手引書の成案化にあたり、登録セキスペの活用についても紐づけを検討中。上記のほか、①支援機関の無料相談窓口リスト掲載者を配置すること、②支援機関による専門家派遣事業で専門家を選定する際に、リストを活用いただくことを検討。 |

3. その他

- 現在IPAが管理運用している「情報処理安全確保支援士 検索サービス」は、全登録セキスペを管理番号ベースで対象としているものの、氏名・連絡先・保有スキル等が任意項目となっているところ、同サービスの扱いについては「登録セキスペアクティブリスト」の具体化の中で引き続き検討。

(参考) アクティブリストの完成イメージ (案)

- アクティブリストの掲載項目について、現時点案としては以下のとおり。
- 中小企業や支援機関等が登録セキスぺを選定する際に必要となる基礎情報に加えて、詳細情報（登録セキスぺの登録年数、更新時の義務講習の受講状況等）の掲載項目についても引き続き検討。

検索結果一覧（基礎情報）

| | 氏名 | 支援実績のある指導テーマ | 支援実績のある業務 (指導テーマ以外) ※支援士試験シラバスの小項目で定型化 | 支援実績のある業界 | 支援地域 | 支援可能期間 | 支援料金 初回無料 | 支援可能形態（1回あたりの支援料金） | 他資格の保有状況 | 所属形態 |
|---|-----|---|--|-------------------|------------------------|-------------------------------------|--------------|--|--------------------------------------|--------------|
| ① | AAA | 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 ④セキュリティインシデント対応 ⑤従業員向けセキュリティ教育 | 〇〇〇 | 製造業 建設業 | 大阪、奈良、 京都、兵庫 | スポット、 3か月～半年 | あり | 訪問コンサルティング (××円) オンラインコンサルティング (●●円) 講習・研修 (△△円) | ITコーディネータ 中小企業診断士 CISSP 税理士 | 個人事業主 |
| ② | BBB | 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 | ▼▼▼ | 自動車産業 | 奈良、滋賀、 京都、三重、 岐阜 | スポット、 1～3か月、 3か月～半年、 半年～1年 | あり | 訪問コンサルティング (××円) オンラインコンサルティング (●●円) 講習・研修 (△△円) セキュリティ製品の選定・ 導入支援 (■●円) | ITコーディネータ 公認情報セキュリティ 監査人 | ◇◇株式会社所 属 |
| ③ | CCC | 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 ⑤従業員向けセキュリティ教育 | □□□ | 金融業 小売業 卸売業 | 大阪、奈良、 和歌山 | スポット、 1年以上 | なし | 訪問コンサルティング (××円) オンラインコンサルティング (●●円) 講習・研修 (△△円) | 公認会計士 中小企業診断士 | 個人事業主 |

※氏名をクリックすると、専門家の詳細情報（具体的な支援実績、連絡先等）が表示されることを想定。

(参考) 支援機関等におけるアクティブリスト活用シナリオ

活用シナリオ①

(利用者) 中小企業支援機関

(利用目的) 中小企業のニーズに合ったセキュリティ対策の実装を支援する登録セキスペを抽出する

登録セキスペが中小企業に対して担う役割

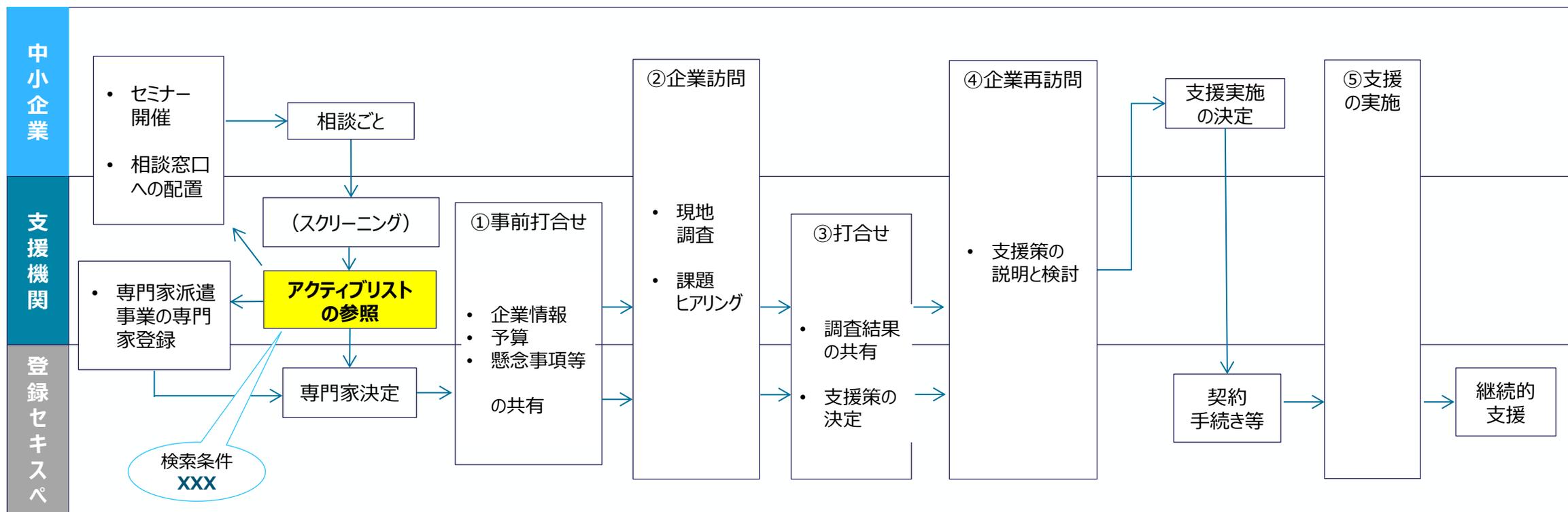
社内ITリソースの補完者としての役割、経営者への説得者としての役割、包括的なセキュリティ戦略の立案と実施者の役割、セキュリティ製品導入後の品質担保者としての役割、効果的なIT投資実現のためのパートナーとしての役割

登録セキスペが支援機関に対して担う役割

支援プログラム実施のための専門的・戦略的パートナーとしての役割

支援機関が中小企業に対して担う役割

中小企業のセキュリティ対策のロードマップ策定、中小企業とセキュリティ専門家・関係者とのネットワーク構築を支援する役割



(参考) 支援機関等におけるアクティブリスト活用シナリオ

活用シナリオ②

(利用者) ITベンダー

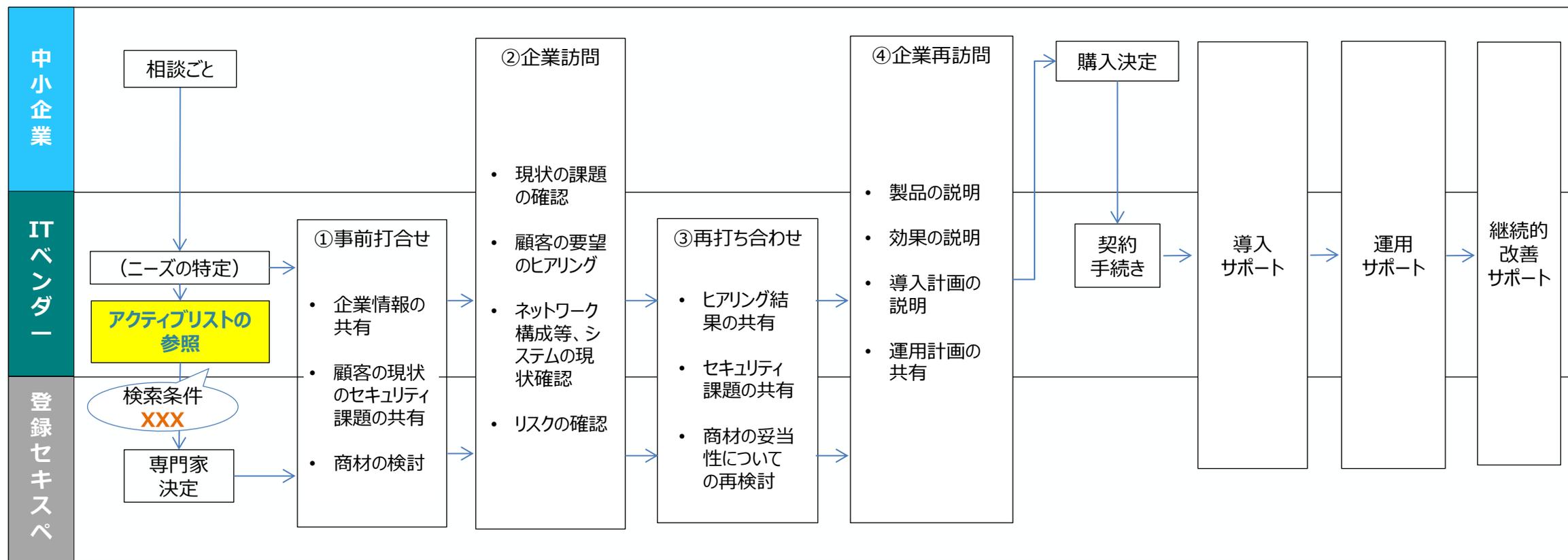
(利用目的) 顧客の中小企業へセキュリティ商材を導入をサポートする登録セキスぺを選定する

登録セキスぺが中小企業に対して担う役割

中小企業の立場からのITベンダーからの提案に対する目利き役としての役割、ITベンダーと経営との橋渡し役としての役割、導入後のサポート等を通じた品質の保証者としての役割、効果的なIT投資実現のためのパートナーとしての役割

登録セキスぺがITベンダーに対して担う役割

知識・経験の共有者としての役割、経営者との橋渡し役としての役割、品質管理・監督者としての役割



令和7年度の取組（登録セキスペアクティブリスト）

リストの掲載メニューについて

- リストの掲載メニューについては、商工会議所、情報処理安全確保支援士会、予算事業に参画した中小企業・登録セキスペ等から広く意見を聴取。令和7年度は、以下の事項について検討。
 - ✓ 対策をどこから始めたらよいか分からない中小企業や、支援機関にも使いやすい**リストのユーザ・インターフェースを整備**するとともに、「支援実績テーマ/得意な業界/所属形態/指導形態（対面/リモート）による料金区分/初回無料の有無/登録セキスペ以外の保有資格/支援地域」などの**リストの掲載メニューを具体化**。
 - ✓ 自己申告の項目と検証可能な項目の別について検討。
 - ✓ セキュリティ**対策支援を求める企業**のため、**支援の選択肢を示す**こととし、**指導テーマ**（規程整備、情報資産の洗出し、セキュリティ教育など）をリストの掲載メニューとして設定。
- また、**指導テーマ**は、標準的な進め方、スケジュール、達成レベル等を指導要領で整備したことから、**指導を行う登録セキスペにとって有意義**であった。また、**支援を受ける企業側**としては、**自社の取組等を第三者的な視点で確認したいニーズも存在**。そこで、令和7年度は、以下の取組を実施。※詳細はスライド51参照
 - ✓ **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、同制度の★3の対策が実施されているかを評価するための**指導要領を作成**。
 - ✓ 登録セキスペに対して、情報セキュリティ監査の観点を踏まえ、指導要領を活用して、**同制度の★3の対策が実施されているかどうかを評価するためのスキル習得の機会を提供**。

令和7年度の取組（登録セキスペアクティブリスト）

リストの管理について

- リストの適切な管理と、セキュリティ対策の支援に携わるアクティブリスト登録者の拡大に向けて、令和7年度は、以下の事項について検討。
 - ✓ 適切な結果表示を含む**検索の品質向上**、登録申請の受付方法（登録者自らによる更新）や能力担保のための**掲載基準**など、必要な検討を進める。
 - ✓ アクティブリストの裾野の拡大（支援実務に携わる登録セキスペの充実）に向けて、**支援の意義の経営者に向けた発信**を検討。

支援機関等と連携したリストの活用について

- 令和6年度は3地域（大阪・名古屋・埼玉）の**商工会議所と連携したサイバーセキュリティ相談会**を実施し、支援機関を介した登録セキスペと中小企業のマッチング機会を提供することは、**中小企業、支援機関、登録セキスペにとって有意義**であった。**令和7年度はその取組を全国に拡大**していく必要があるため、以下の活動を実施。
 - ✓ 令和6年度予算事業（実証事業）に参画した商工会議所を中心に、セミナー開催に併せて企業と登録セキスペの相談会を開催する際に、アクティブリスト（令和6年度の事業成果）の活用を促すため、**活用事例の整理・横展開**を行う。その他、①**支援機関の無料相談窓口への配置**の際の活用、②**専門家派遣事業による派遣**の際の活用など、**活用シナリオを拡充**。
 - ✓ 活用事例の横展開の手段として、「登録セキスペとは?」「登録セキスペが支援できる内容（指導テーマ）」「登録セキスペ（アクティブリスト）の活用シナリオ」「令和6年度予算事業（実証事業）における登録セキスペの活用事例」等を分かりやすく解説した**広報資材を作成し、支援機関、SC3（業界団体）、地域SECURITY、経済産業局等が行うセミナー等で拡散**。
 - ✓ 支援機関等がリストを有効に活用できるよう、支援機関等がセミナー開催に併せて企業と登録セキスペの相談会を開催する際には、**情報処理安全確保支援士会が、ネットワーク（地域支部）を活用し、各地域へアンバサダーを派遣**することで、**セミナー講師としての登壇や相談会等を実施し、支援機関等と連携した取組を拡大**することを期待。

(参考) 有識者プレゼン等を踏まえた登録セキスペアクトイブリストに関する対応の方向性

〔有識者プレゼン等での声〕

リストの掲載メニュー

- ・ **業務形態**（インハウス/独立）、**指導形態**（訪問/オンライン）による**料金区分**、**初回無料**の有無、他の**保有資格**などの情報があれば専門家を選びやすい。
- ・ **自己申告**の項目と**客観的に検証可能**な項目（義務講習の受講状況等）の別の明示も検討すべき。
＜以上有識者プレゼン等＞
- ・ 専門家選定の観点として「**緊急時の対応力**」「**提案内容の具体性**」「**技術力・専門性**」「**自社の業界に対する理解度**」「**コスト**」が上位。
- ・ 地元の専門家の方がコミュニケーションを取りやすいので、**まず地域**を見るはず。
- ・ 相談会参加者のうち「**セキュリティの意識があるものの始め方が分からない**」などと回答した企業は約8割。（再掲）
- ・ 自社の判断・取組の妥当性を専門家の**第三者的な視点から確認したい**。（再掲）
＜以上セキュリティ人材活用促進実証＞
- ・ 依頼したい支援内容は「**セキュリティ教育の実施**」「**規程作成・改訂**」が上位＜中小企業実態調査＞

リストの管理

- ・ 検索順位の上位に問合せが集中しない工夫、リスト登録に際しての一定の能力担保が必要では。
- ・ 現状では副業禁止などによって中小企業等のセキュリティ対策支援に携われない人材の登録を促す観点から、**セキュリティ対策支援は、登録セキスペを擁している企業にとっても、人材育成等の観点から有意義である旨を政府から発信してはどうか**。
＜以上有識者プレゼン等＞

支援機関等と連携したリストの活用

- ・ 専門家の探索方法として、「**公的機関（IPA等）におけるリストの利用**」のほか「**商工会議所等の支援機関による紹介・マッチング**」「**取引のあるITベンダからの紹介**」が上位。
- ・ いきなり専門家が訪問指導に入るのは抵抗があり、**まずは（相談会等の場で、）専門家と企業のマッチング機会**があることが重要。
＜以上セキュリティ人材活用促進実証＞
- ・ **支援機関**としては、アクティブリストによって支援項目・件数、専門家との結節点が増えることは**メリット**。
- ・ 地域ではセキュリティ対策の**支援者が不足**しており、**支援可能な専門家の見える化**ができていない。
- ・ 地域では、**信用・信頼・顔が見える**ということが重要。また、**地域SECURITYとアクティブリストに掲載された登録セキスペをつなげる**ことで、相談先の課題解決と伴走支援につながるのでは。
- ・ 土業団体、金融機関、業界団体、ITベンダー等に対しても活用を促し、**情報処理安全確保支援士会を中心とした組織的な対応が有効**では。
＜以上有識者プレゼン等＞

〔令和7年度以降における対応の方向性〕

- ✓ 対策をどこから始めたらよいか分からない中小企業や、支援機関にも使いやすい**リストのユーザ・インターフェースを整備**するとともに、支援実績テーマ/得意な業界/所属形態/指導形態（対面/リモート）による料金区分/初回無料の有無/登録セキスペ以外の保有資格/支援地域などの**リストの掲載メニューを具体化**。
- ✓ 自己申告の項目と検証可能な項目の別について検討。
- ✓ **セキュリティ対策支援を求める企業のため、支援の選択肢を示すこととし、指導テーマ（規程整備、情報資産の洗出し、セキュリティ教育など）をリストの掲載メニューとして設定**。
- ✓ さらに、自社の取組等を**第三者的な視点で確認したい企業のため、①サブ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、当該テーマの指導要領を作成**するとともに、②登録セキスペに対して、**企業評価のためのスキル（監査スキル）の習得機会を提供**。

- ✓ 適切な結果表示を含む検索の品質向上、登録申請の受付方法（登録者自らによる更新）や能力担保のための掲載基準などについて検討。
- ✓ アクティブリストの裾野の拡大（支援実務に携わる登録セキスペの充実）に向けて、**支援の意義の経営者に向けた発信を検討**。

- ✓ 地域の支援機関等を介した登録セキスペによる中小企業支援を促進するため、**支援可能な登録セキスペの見える化・支援者の裾野拡大のためにアクティブリストを活用**。
- ✓ 対策をどこから始めたらよいか分からない中小企業が、**支援機関等の取組を介して、自社の課題や取るべき対策が明確になることを期待**。
 - ・ R6年度の予算事業（実証事業）に参画した**商工会議所**を中心に、セミナー開催に併せて企業と登録セキスペの**相談会を開催**（自社の状況や課題について共有）する際に、**アクティブリスト（R6年度の事業成果）の活用を促進し、活用事例を整理して横展開**。（セミナーへの情報処理安全確保支援士会による講師派遣等にも期待）
 - ・ 上記のほか、①支援機関の**無料相談窓口への配置**の際の活用、②**専門家派遣事業**による派遣の際の活用についても、支援機関等と連携。

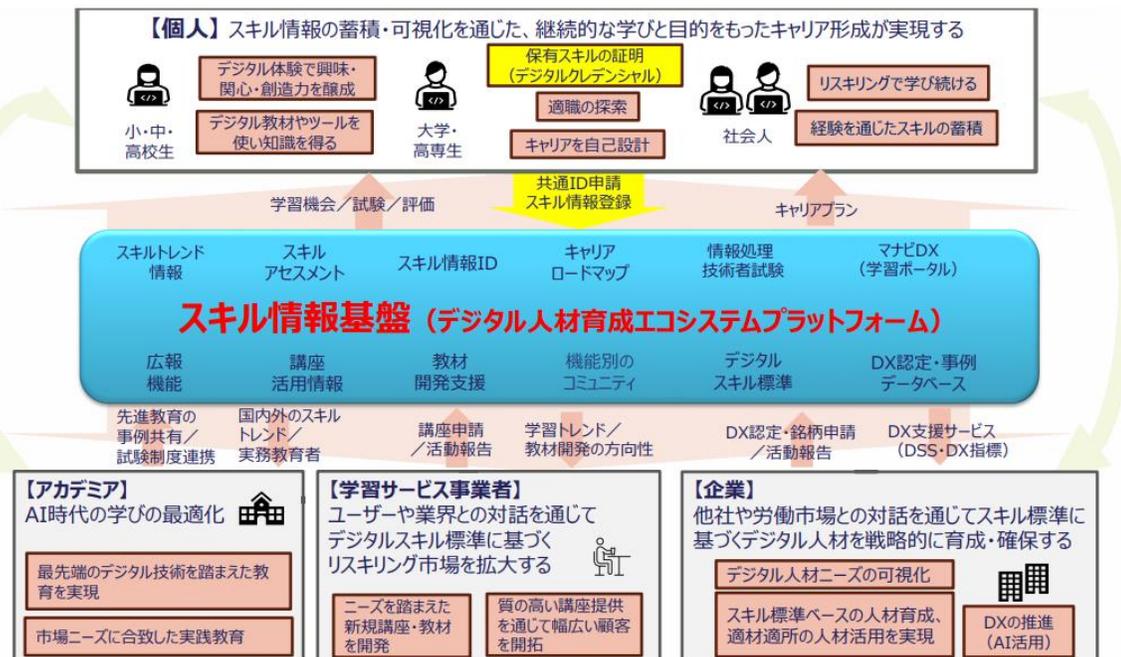
Ⅲ - 2 登録セキスぺに係る施策の分類・整理

① 登録セキスぺの能力向上、スキル・実績の見える化

2. デジタル人材育成・DX推進プラットフォームの整備

- 「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。
- 令和8年下期のリリースを予定しているデジタル人材育成・DX推進プラットフォームが具体化されれば、登録セキスぺの能力向上及びスキル・実績の見える化が促進され、登録セキスぺ自身が、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を理解し、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になることが期待。

<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>



<参考：今後のスケジュール>



(出典) 「Society 5.0 時代のデジタル人材育成に関する検討会」第4回 資料3より抜粋

Ⅲ - 2 登録セキスぺに係る施策の分類・整理

①登録セキスぺの能力向上、スキル・実績の見える化

3. セキュリティマネジメント能力の強化（情報処理安全確保支援士試験の見直し）

- 「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、その学習の在り方（情報処理技術者試験の見直し）について検討がなされていたところ、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。
- 具体的には、サイバー攻撃が今後ますます増加・高度化・複雑化するおそれがある中で、一定規模以上の企業では、サイバーセキュリティ対策の外部委託を積極活用しつつも、**リスクマネジメントの一環として、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ことを踏まえ、以下の論点について検討。
 - 登録セキスぺ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**必要か**。試験自体は共通としつつ更新時に**選択肢**を設けて対応すべきか。
 - **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。

- 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**考え方が提示された。

- 今後、情報処理安全確保支援士試験の見直しについては、別途IPA等の関係者と検討。

Ⅲ - 2 登録セキスペに係る施策の分類・整理

①登録セキスペの能力向上、スキル・実績の見える化

3. セキュリティマネジメント能力の強化（更新時の義務講習におけるマネジメント要素の習得）

- ・ 自社内のマネジメント需要への登録セキスペによる対応として、資格更新時の講習で対応していくことも必要。IPAの実践講習では、企業内での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、現時点においても、**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しており、引き続き取組を継続。**
- ・ また、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。
 - * 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）。
- ・ **マネジメント要素を強化した講習の充実**によって、**マネジメント能力を備えた登録セキスペの増加**が期待。

<参考：IPAで提供されている実践講習>

| 講習の種類 | 講習概要 |
|---------------------------------|--|
| 実践講習A | インシデント対応を題材としたグループ演習を通じ、登録セキスペとして求められる情報セキュリティ実践のための具体的な対応技術やマネジメント手法を習得。 |
| 実践講習B | 新規事業の立ち上げを題材にして、サイバーセキュリティの確保を支援するための一覧の流れ（分析・評価→対策検討→助言）を経験するグループ演習により、業務で利用するための実践的な能力を習得。 |
| 業界別サイバーレジリエンス強化演習（CyberREX） | 企業などの部門責任者層が、業界別の仮想企業におけるシナリオによる演習を通じ、サイバーリスクへの対応力・回復力の強化について学ぶ。 |
| 制御システム向けサイバーセキュリティ演習（CyberSTIX） | 企業等の制御システムに関わる実務者が、模擬システムにおけるサイバー攻撃や防御の演習を通じ、制御システムのセキュリティについてより深く実践的に学ぶ。 |

<参考：民間事業者等で提供されている実践講習の分類>

| 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 | 24 |
| 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 | 20 |
| 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 | 3 |
| 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 | 1 |
| 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 | 1 |
| セキュリティ監査：セキュリティ監査、報告・助言 等 | 1 |

(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

| | ユーザ企業における組織の例 | サイバーセキュリティ関連タスクの例 | タスクに対応するサイバーセキュリティ関連分野 | | |
|-----------|------------------------------|--|-----------------------------|-----------------------------|-------------------------|
| | | | サイバーセキュリティ対策に関するタスクの割合が高いもの | サイバーセキュリティ以外のタスクが占める割合が高いもの | |
| 経営層 | 取締役会 執行役員会議 | <ul style="list-style-type: none"> サイバーセキュリティ意識啓発 対策方針指示 ポリシー・予算・実施事項承認 | セキュリティ経営 (CISO) | デジタル経営 (CIO/CDO) | 企業経営 (取締役) |
| | 内部監査部門 (外部監査を含む) | <ul style="list-style-type: none"> システム監査 セキュリティ監査 | セキュリティ監査 | システム監査 | |
| 戦略マネジメント層 | 管理部門 (総務、法務、広報、調達、人事等) | <ul style="list-style-type: none"> BCP対応 官公庁、法令等遵守対応 記者・広報対応 調達・契約・検収 施設管理・物理セキュリティ 内部犯行対策 | | 法務 | 経営リスクマネジメント |
| | セキュリティ統括室 | <ul style="list-style-type: none"> 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 | セキュリティ統括 | | |
| 設計・開発・テスト | 経営企画部門 事業部門 | <ul style="list-style-type: none"> 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 | | デジタルシステム ストラテジー | 事業ドメイン (戦略・企画・調達) |
| | デジタル部門 / 事業部門 (専門事業者への外注を含む) | <ul style="list-style-type: none"> セキュアシステム要件定義 セキュア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 基本・詳細設計 セキュアプログラミング テスト・品質保証 バッチ開発 脆弱性診断 構成管理、運用設定 脆弱性対応 セキュリティツールの導入・運用 監視・検知・対応 インシデントレスポンス ペネトレーションテスト 現場教育・管理 設備管理・保全 初動対応・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 | 脆弱性診断・ ペネトレーション テスト | デジタル プロダクト 開発 | 事業ドメイン (生産現場・ 事業所管理) |
| 実務者・技術者層 | 運用・ 保守 | | セキュリティ 監視・運用 | | |
| 研究開発 | | <ul style="list-style-type: none"> セキュリティ理論研究 セキュリティ技術開発 | セキュリティ 調査分析・ 研究開発 | | |

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) | <ul style="list-style-type: none"> サイバーセキュリティ意識啓発 |
| | デジタル経営 (CIO/CDO) | <ul style="list-style-type: none"> 対策方針の指示 |
| 戦略マネジメント層 | 企業経営 (取締役) | <ul style="list-style-type: none"> セキュリティポリシー・予算・対策実施事項の承認 等 |
| | セキュリティ監査 システム監査 | <ul style="list-style-type: none"> 情報セキュリティ監査、報告・助言 等 システム監査、報告・助言 等 |
| 戦略マネジメント層 | セキュリティ統括 | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> 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 |
| 戦略マネジメント層 | 経営リスクマネジメント | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> 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 |
| 戦略マネジメント層 | 事業ドメイン (戦略・企画・調達) | <ul style="list-style-type: none"> 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 |
| | 脆弱性診断・ペネトレーションテスト | <ul style="list-style-type: none"> 脆弱性診断、ペネトレーションテスト 等 |
| 実務者・技術者層 | セキュリティ監視・運用 | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> 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 |
| 実務者・技術者層 | デジタルシステムアーキテクチャ | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> 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 バッチ開発 等 |
| 実務者・技術者層 | デジタルプロダクト運用 | <ul style="list-style-type: none"> 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) | <ul style="list-style-type: none"> 現場教育・管理、設備管理・保全、QC活動 初動対応 等 |

※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

Ⅲ - 2 登録セキスぺに係る施策の分類・整理

②ユーザー企業における登録セキスぺの活用（総括表）

- セキュリティ評価制度における評価者としての活用、DX施策との連動、各種投資促進施策における要件化等を通して、企業側（活用側）への働きかけに繋げていく。

| 実施する取組 | 取組の方向性 |
|--|--|
| ②-1. 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における活用 | <ul style="list-style-type: none"> 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。 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。 |
| ②-2. セキュリティ要件適合評価及びラベリング制度（JC-STAR）における活用 | <ul style="list-style-type: none"> 企業がJC-STAR制度の自己適合宣言をする際に、IoT製品のセキュリティ評価を適切に実施できる個人の有資格者として、登録セキスぺを活用することについて引き続き検討。 |
| ②-3. 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"> 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。 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。 |
| ②-4. 各種投資促進施策における要件化 | <ul style="list-style-type: none"> 経済産業省の各種補助施策において登録セキスぺの配置を要件化を進め、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。 取組例として、「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」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。 |
| ②-5. 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"> 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。 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。 |

Ⅲ - 2 登録セキスぺに係る施策の分類・整理

②ユーザー企業における登録セキスぺの活用

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、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を活用して★3のサイバーセキュリティ対策を満たす旨を自己評価する際、専門家がその対策を評価するプロセスを要することを想定。
 - 登録セキスぺは、企業のセキュリティ対策の伴走支援（例：情報セキュリティ規程の整備）のみならず、対策を評価する専門家として積極的に活用されるよう、企業のセキュリティ対策を評価する能力を強化する必要。
 - 令和7年度予算事業において、
 - 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、同制度の★3の対策が実施されているかを評価するための指導要領を作成するとともに、
 - ② 登録セキスぺに対して、情報セキュリティ監査の観点を踏まえ、指導要領を活用して、同制度の★3の対策の実施について評価するためのスキル習得の機会を提供。

(参考) サプライチェーン企業のセキュリティ対策評価制度の構築

- サプライチェーンに起因するインシデントを背景に、企業の取引においてもセキュリティ対策の担保が求められる中、受注企業は異なる取引先から様々な対策水準を要求される、発注企業は外部から各企業等の対策状況を判断することが難しいといった課題が存在。
- こうした課題に対応するため、サプライチェーンにおける重要性を踏まえた上で満たすべき各企業の対策を提示しつつ、その対策状況を可視化する仕組みの検討を進めており、令和7年4月に制度の概要を整理した中間とりまとめを公表。今後、実証事業等を通じた評価スキームの具体化や制度の利用促進のための施策の検討等を進め、令和8年度中の制度開始を目指す。

構築する評価制度（現時点案）

| 成熟度の定義 | 三つ星（★3） | 四つ星（★4） | 五つ星（★5）※ |
|------------|---|---|--|
| 想定される脅威 | <ul style="list-style-type: none"> • 広く認知された脆弱性等を悪用する一般的なサイバー攻撃 | <ul style="list-style-type: none"> • 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃 | <ul style="list-style-type: none"> • 未知の攻撃も含めた、高度なサイバー攻撃 |
| 対策の基本的な考え方 | 全てのサプライチェーン企業が最低限実装すべきセキュリティ対策： <ul style="list-style-type: none"> • 基礎的な組織的対策とシステム防御策を中心に実施 | サプライチェーン企業等が標準的に目指すべきセキュリティ対策： <ul style="list-style-type: none"> • 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を実施 | サプライチェーン企業等が到達点として目指すべき対策： <ul style="list-style-type: none"> • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善プロセスを整備した上で、システムに対しては現時点でのベストプラクティスに基づく対策を実施 |
| 評価スキーム | 自己評価 | 第三者評価 | 第三者評価 |

政府調達や重要インフラ事業者等での活用推進

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

制度実現に向けた検討課題（例）

- 国内外の関連制度・評価制度との整合性確保、相互認証
- 対策推進のための企業への支援の在り方（専門家の活用促進、中小企業支援策との連動、評価機関の支援）
- 下請法や価格転嫁に関する課題の整理
- 実効性の強化に向けた取組（政府機関や重要インフラ事業者等における活用推進、サプライチェーン上の取引先や投資家等のステークホルダとの対話での活用等の促進）

※ISMS適合性評価制度との制度的整合性、★3・4との整合性も踏まえ、対策事項を検討

※サプライチェーン間の結び付きが強固・複雑な自動車、半導体、主要製造業等において、優先的に本制度の利用を促進。

(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★3

<★3の要求事項・評価基準>

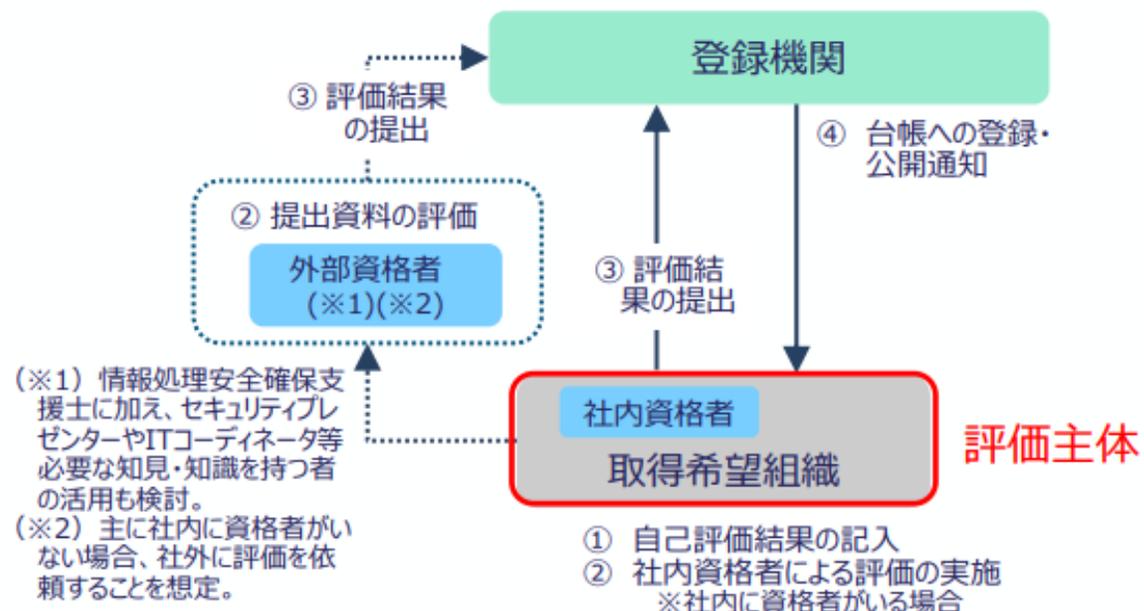
★3 (Basic)

| | |
|-------------|---------------------|
| 経営の責任 | 企業として最低限のリスク管理体制構築 |
| | インシデント発生に備えた対応手順の整備 |
| | 自社IT基盤や資産の現状把握 |
| サプライチェーンの防御 | 取引先等に課す最低限のルールの特化 |
| | 不正アクセスに対する基礎的な防御 |
| IT基盤の防御 | 端末やサーバーの基礎的な保護 |

<★3の要求事項・評価基準>

自己評価：★3

- ① 取得希望組織は、★3要求事項に基づき自己評価を記入（必要に応じ、社内外の資格者の助言を得る）
- ② 社内外の資格者は、記入内容を評価、要求事項に対する合否を判断
- ③ 取得希望組織または社内外の資格者は、登録機関に評価結果を提出
- ④ 登録機関は、申請内容に問題が認められない場合には台帳に登録・公開



Ⅲ - 2 登録セキスぺに係る施策の分類・整理

②ユーザー企業における登録セキスぺの活用

2. セキュリティ要件適合評価及びラベリング制度 (JC-STAR) での活用

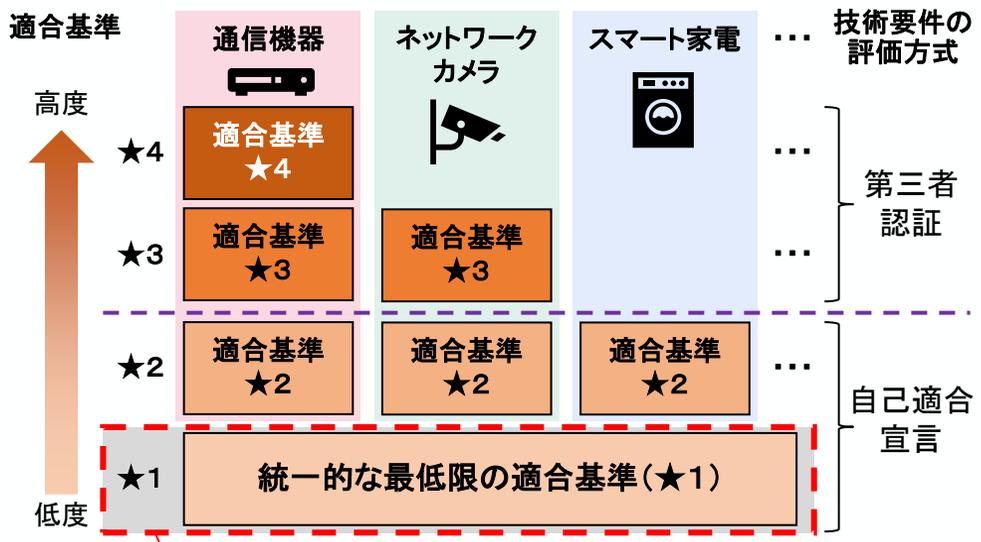
- 令和7年3月に開始したJC-STAR制度(※1)の自己適合宣言において、IoT製品のセキュリティ評価を適切に実施できる個人の有資格者として、登録セキスぺの活用について引き続き検討。

制度名称・ロゴ・ラベル

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)

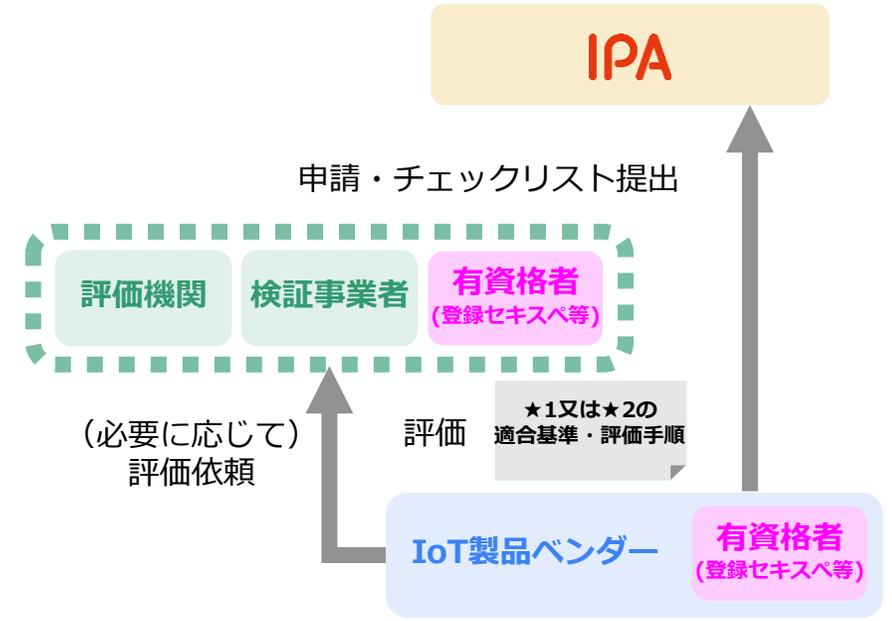


制度の概要 (イメージ)



令和7年3月25日に開始

★1、★2 (自己適合宣言) の評価者



(※1) 独立行政法人 情報処理推進機構 (IPA) 「セキュリティ要件適合評価及びラベリング制度 (JC-STAR)」 <https://www.ipa.go.jp/security/jc-star/index.html>

Ⅲ - 2 登録セキスぺに係る施策の分類・整理

②ユーザー企業における登録セキスぺの活用

3. DX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ぺの活用・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（登録セキスぺ）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。
- また、「**中堅・中小企業等向けDX推進の手引き**」において、DXを進める上での施策として、企業内外を問わず**サイバーセキュリティ**に関して、広く相談に応じ、また企業の取組に対して分析や評価を行い、助言や指導を行う役割を担う人材として**登録セキスぺ**を追記。
- 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ぺ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～（令和6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（システムの・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（登録セキスぺ）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。

○中堅・中小企業等向けDX推進の手引き2025（DXセレクション2025選定企業レポート）（令和7年3月）（抜粋）

企業DXに関連する政策一覧（令和7年3月時点）

情報処理安全確保支援士（登録セキスぺ）

- 企業のサイバーセキュリティの確保を支援するための、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者。企業内外を問わずサイバーセキュリティに関して、広く相談に応じ、また企業の取組に対して分析や評価を行い、助言や指導を行う役割を担うことができる。

【URL】 <https://www.meti.go.jp/policy/netsecurity/riss.html>

Ⅲ - 2 登録セキスペに係る施策の分類・整理

②ユーザー企業における登録セキスペの活用

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年度補正予算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（※）が適切か
※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】**

Ⅲ - 2 登録セキスぺに係る施策の分類・整理

②ユーザー企業における登録セキスぺの活用

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ぺの活用を促していく。**
- 直近では、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参加者等に対して、登録セキスぺ制度の紹介及び活用策についての周知を実施。
- これらの取組を通して、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

○（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）（抜粋）

2. デジタル人材の育成
デジタル人材が取得することが想定されるIT関連資格やスキル標準は、次のとおりです。

情報処理安全確保支援士（国家資格）（登録セキスぺ）

※セキュリティ分野の人材に有用

〈対象者〉

企業や組織における情報セキュリティ対策を効果的に支援する人材

〈内容〉

サイバーセキュリティの専門知識を有し、企業や組織における情報セキュリティ対策を効果的に支援する人材を育成・認定

Ⅲ - 2 登録セキスぺに係る施策の分類・整理

③更新コストの低減

1. 更新時の義務講習（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ぺについては**、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、**更新時の義務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を想定。

- これにより、更新時の負担軽減に加えて、前述の「**登録セキスぺの活用促進・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ぺが増加**することも期待。

2. オンライン講習の見直し

- 更新時の義務講習の一部である「**オンライン講習**」について、**講習単元の統合等を行い**、すべての登録セキスぺにとって、更新のために必要となる**講習の受講費用を低減**させることを検討。

更新時の義務講習（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、登録セキスへ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、登録セキスへには、講習の受講義務が設けられている。**
- また、登録セキスへは、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、登録セキスへ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。

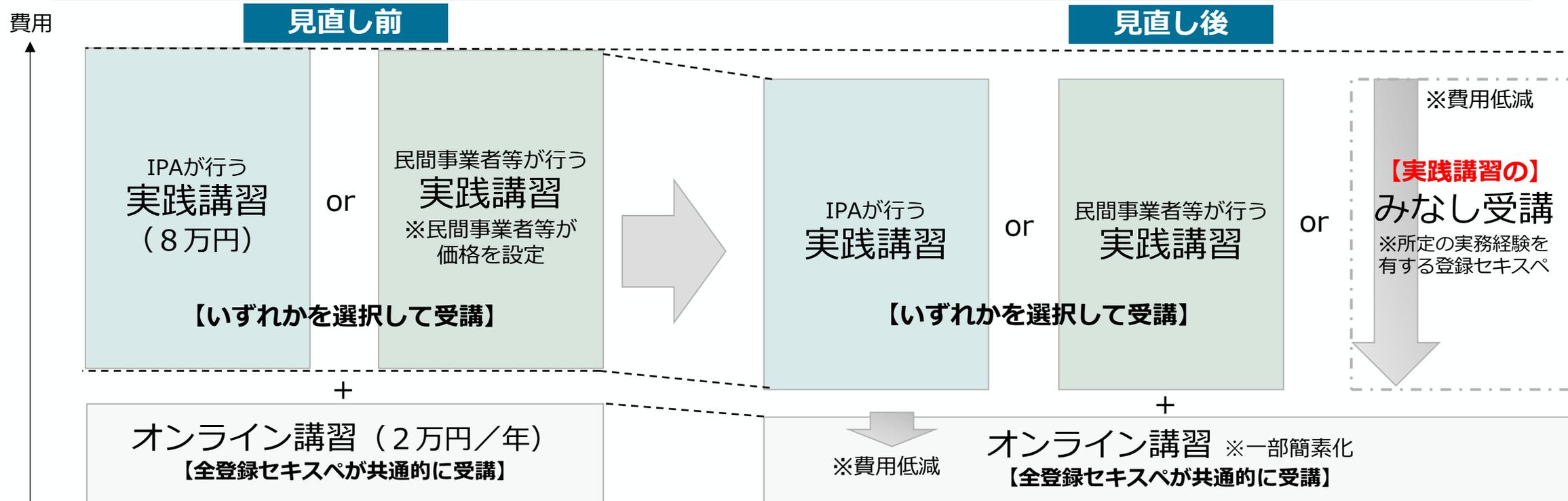
○情報処理の促進に関する法律施行規則（平成28年経済産業省令第102号）
（登録の更新）

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）

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（令和8年度中に制度開始想定）。



(参考) みなし受講制度検討の前提 (登録セキスへの業務等)

【登録セキスへの業務】

サイバーセキュリティの確保のための取組に関し、サイバーセキュリティに関する相談に応じ、必要な**情報の提供及び助言**を行うとともに、必要に応じその取組の実施の状況についての**調査、分析及び評価**を行い、その**結果に基づき指導及び助言**を行うことその他**サイバーセキュリティの確保を支援**

【登録セキスへの信頼性の確保】

サイバーセキュリティに関する知識及び技能に関する事項並びに遵守すべき倫理に関する事項を内容とした**法定講習の定期的な受講を義務**付けるとともに、**信用失墜行為の禁止**規定や罰則付きの厳格な**秘密保持義務**を設定

【更新制の導入】

サイバーセキュリティに関する**最新の知識・技能を確実に担保**できるように、登録に3年間の有効期限を設け、**義務講習を受講した者のみ更新**

みなし受講制度の対象とする実務経験の考え方

- みなし受講制度の対象とする実務経験については、講習代替性を充足する必要。
- 講習代替性を検討するに当たっては、①～④を総合的に考慮。

講習代替性

- サイバーセキュリティに関する最新の知識・技能を確実に担保するという法律の趣旨に鑑み、みなし受講制度の対象とする実務経験は、更新時に受講する講習と同等以上の内容・ボリュームを担保するものである必要

①本制度の効果

- 登録セキスぺの実務に従事する誘因を設定することで、登録セキスぺの一層の活用促進等に効果も期待
- 実践・特定講習の内容と同等以上の内容・ボリュームを有するサイバーセキュリティ関連業務に従事する登録セキスぺの講習費用の負担軽減にも資する

②客観的判断

- みなし受講の対象となる実務経験の証跡等を踏まえ、制度の信頼性を確保しつつ、客観的・外形的な判断が可能である必要

③事務負担

- 実効的で持続可能な制度運用が確保されるよう、みなし受講の審査コストを考慮する必要

④その他

- 必要な法令改正も視野に入れて制度設計を行う必要

更新時の義務講習に代替可能な実務経験の水準の担保の考え方 (イメージ)

- まず、更新時の義務講習に代替可能な実務経験について検討するため、法令レベルから運用レベルまで整理を行い、更新時の義務講習として求める要素を特定。

経済産業省令

- 特定講習（※1）は、
 - 支援士試験の科目に係る内容を行うものとし、特定講習の**総時間は6時間以上**とされるとともに、
 - 半分以上の内容を実習、実技、演習又は発表その他**実践的な方法**により行う
- 上記科目の内容は、情報セキュリティシステムの開発+（情報処理システム+関連業務におけるセキュリティ管理）に関する**専門的知識+専門的能力**

（※1）

特定講習の具体的内容は、上記のとおり、経済産業省令に規定されているところ、特定講習は、**機構の講習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とされていることから、**機構の講習として求める要素は、特定講習と同様。**

（※2）

民間事業者等が行う実践講習部分を指す。

特定講習（※2）募集等要領

- 試験科目の内容は、「募集要領」において敷衍されており、具体的には、
 - ITスキル標準レベル4相当**（一つまたは複数の専門を獲得したプロフェッショナルとして、専門スキルを駆使し、業務上の課題の発見と解決をリードするレベル、プロフェッショナルとして求められる、経験の知識化とその応用（後進育成）に貢献するレベル）に該当し、
 - 支援士試験シラバスにおける大項目のいずれかを含むこととされ、具体的には、シラバスの**小項目を複数含む内容**であれば、特定講習として認められる

支援士試験シラバス

- 上記大項目（4項目）が更に詳細化された小項目とその概要等（必要な指導・助言・支援の内容、要求される知識・技能）を設定

(参考) 情報処理安全確保支援士試験シラバスの大項目及び小項目

| 大項目 | 小項目 | 大項目 | 小項目 |
|--|-----------------------------|--|---------------------------|
| 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 | 1-1 情報セキュリティ方針の策定 | 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 | 3-1 暗号利用及び鍵管理 |
| | 1-2 情報セキュリティリスクアセスメント | | 3-2 マルウェア対策 |
| | 1-3 情報セキュリティリスク対応 | | 3-3 バックアップ |
| | 1-4 情報セキュリティ諸規程の策定 | | 3-4 セキュリティ監視並びにログの取得及び分析 |
| | 1-5 情報セキュリティ監査 | | 3-5 ネットワーク及び機器のセキュリティ管理 |
| | 1-6 情報セキュリティに関する動向・事例の収集と分析 | | 3-6 脆弱性への対応 |
| | 1-7 関係者とのコミュニケーション | | 3-7 物理的及び環境的セキュリティ管理 |
| 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 | 2-1 企画・要件定義（セキュリティの観点） | | 3-8 アカウント管理及びアクセス管理 |
| | 2-2 製品・サービスのセキュアな導入 | | 3-9 人的管理 |
| | 2-3 アーキテクチャの設計（セキュリティの観点） | | 3-10 サプライチェーンの情報セキュリティの推進 |
| | 2-4 セキュリティ機能の設計・実装 | | 3-11 コンプライアンス管理 |
| | 2-5 セキュアプログラミング | 4-1 情報セキュリティインシデントの管理体制の構築 | |
| | 2-6 セキュリティテスト | 4-2 情報セキュリティ事象の評価 | |
| | 2-7 運用・保守（セキュリティの観点） | 4-3 情報セキュリティインシデントへの対応 | |
| | 2-8 開発環境のセキュリティ確保 | 4-4 証拠の収集及び分析 | |
| | | 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 | |

※ 特定講習において、網掛けの小項目のみを対象とした講習では十分とは言えないため、他の項目と組み合わせて実施することとされている（募集要項）

(参考) 情報処理安全確保支援士試験シラバスの小項目概要 (抄)

| 大項目 | 小項目 | 概要 | 要求される知識 | 要求される技能 |
|-------------------------------|-----------------------|--|--|---|
| 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 | 1-1 情報セキュリティ方針の策定 | 経営者による情報セキュリティ方針の策定及び改定について、必要な指導・助言を行い、支援する。 | <ul style="list-style-type: none"> 情報セキュリティガバナンス及びITガバナンスに関する知識 マネジメントシステム（ISMS、BCMSなど）に関する知識 組織マネジメントに関する知識 | <ul style="list-style-type: none"> 組織内外の利害関係者のニーズと期待、組織内の経営戦略、事業戦略によって生じる要求事項を踏まえて情報セキュリティ方針を具体化する能力 法令、規制、契約、情報セキュリティに関する動向などによって生じる要求事項を踏まえて情報セキュリティ方針を具体化する能力 経営者とコミュニケーションする能力 |
| | 1-2 情報セキュリティリスクアセスメント | リスク基準の確立及び維持について、必要な指導・助言を行い、支援する。 リスク特定、リスク分析、リスク評価のプロセスの実施について、必要な指導・助言を行い、支援する。 | <ul style="list-style-type: none"> 情報の特性（機密性、完全性、可用性、真正性、責任追跡性、否認防止、信頼性など）に関する知識 リスク、リスク基準、リスク源、脆弱性及び脅威に関する知識 情報セキュリティリスクアセスメントのプロセス（特定、分析、評価）に関する知識 脅威分析（STRIDE分析、アタックツリー分析（ATA）など）に関する知識 | <ul style="list-style-type: none"> 情報資産損失の大きさ（失われる資産の価値、原因究明及び復旧の費用、社会的説明の費用）を算定し、評価する能力 リスク源、脆弱性及び脅威を、新たなITに関するものも含めて列挙する能力 情報資産とリスクを関連付けて整理する能力 リスクを優先順位付けする能力 |
| | 1-3 情報セキュリティリスク対応 | 情報セキュリティリスクアセスメントの結果に基づく適切な管理策の選定、情報セキュリティリスク対応計画の策定について、必要な指導・助言を行い、支援する。 | <ul style="list-style-type: none"> リスク対応の選択肢（リスク低減、リスク共有、リスク回避、リスク保有など）に関する知識 管理策の実施に要する費用の算定に関する知識 サイバー保険に関する知識 | <ul style="list-style-type: none"> リスクごとに、リスク対応の選択肢を選定する能力 リスク対応の実施に適切な管理策を選定する能力 情報セキュリティリスク対応計画を作成し、残留リスクと併せて説明する能力 |
| | 1-4 情報セキュリティ諸規程の策定 | 情報セキュリティに関連する諸規程の策定及び改定について、必要な指導・助言を行い、支援する。 事業継続に関する計画の策定及び改定について、必要な指導・助言を行い、支援する。 | <ul style="list-style-type: none"> 法令、規制、規格に関する知識 ITの動向（クラウドコンピューティング、仮想化、モバイル、組込みシステム、Web技術、AI（生成AIを含む）、ビッグデータ、IoTなど）及びその情報セキュリティへの影響に関する知識 事業継続に関する知識 | <ul style="list-style-type: none"> 業務プロセス、業務手順を踏まえた上で、情報セキュリティ諸規程で定めるべき事項を検討する能力 検討した事項及びその必要性を説明する能力 法令、規制、規格の変化やITの動向を踏まえて情報セキュリティ諸規程をレビューする能力 |

更新時の義務講習に代替可能な実務経験の水準の担保の考え方 (イメージ)

- 更新時に義務付けられている民間事業者等が行う実践講習として求める要素を特定後、それに代替可能な(=みなし受講の対象となる)「実務経験」として求める要素に変換。
- その際には、登録セキスペを、**法定の業務**(相談に応じて情報提供・助言/調査・分析・評価を行いサイバーセキュリティの確保を支援するという法律が定める登録セキスペの業務)に向かわせ、もって**登録セキスペの一層の活用促進・サイバーセキュリティ対策の向上を図る**という**みなし受講制度の政策目的**を踏まえて検討。

民間事業者等が行う実践講習として求める要素

- ITスキル標準レベル4相当(一つまたは複数の専門を獲得したプロフェッショナルとして、専門スキルを駆使し、業務上の課題の発見と解決をリードするレベル、プロフェッショナルとして求められる、経験の知識化とその応用(後進育成)に貢献するレベル)
- 支援士試験シラバスの小項目に関する業務
- 総時間6時間以上
- 半分以上の内容を実習、実技、演習又は発表その他実践的な方法

みなし受講の対象となる実務経験として求める要素

- 支援士試験シラバスの小項目(ITスキル標準レベル4に相当するものとして記載)に該当すること
- 支援士試験シラバスの小項目に該当するひとかたまりの業務

(左記「6時間以上」は講習の受講時間に関し設定されたものであることを踏まえ、ひとかたまりの業務を実施したかを確認)

(左記「半分以上が実践的方法」は講習の方法関し設定されたものであることを踏まえ、「実務経験」の要素としては特段の設定を要しないものと整理)

上記のみなし受講制度の政策目的を踏まえ、「**実務経験**」は**法定の登録セキスペの業務**

ITスキル標準レベル4相当として記載された支援士試験シラバスの小項目(シラバスの小分類の概要・要求される知識・技能)に該当し、かつ、**同小項目に該当するひとかたまりの業務**について、受講義務の対象講習に代替することを認めることを基本としてはどうか。

更新時の義務講習に代替可能な実務経験の判断手法

- 実務経験が、シラバスの小項目に関する業務（シラバスの小分類の概要及び要求される知識・技能の記載で判断）に該当するものとして、所属組織（独立系の登録セキスベにあってはその顧客）が、一定の書式の下でこれを証した場合には、みなし受講を認めることが相当ではないか。
- 更なる信頼性確保策として、みなし受講申請書の工夫、申請内容に虚偽がないことの宣誓、サンプル調査の実施等が考えられる。

信頼性確保策の検討例

| 方策 | 詳細項目 | デメリット・リスク・懸念 | 実現可能な施策 |
|-------------------|---|---|--|
| ①シラバス小項目の該当性の判断 | 対象業務の特定 | （具体例を提示する案に対し）例示通りに申請する者が現れる可能性がある | 領域ごとに具体例を示し、具体例通りの記載は認めないことを明示（cf：建築士の実務経歴証明書） |
| | レベルの担保 | 書類審査で知識や技能の深度を見極めることは難しい | 業務内容をITスキル標準レベル4と紐づけ、具体例をもって明示（cf:技術士試験のように実務経歴証明書の提出を求め、口頭試験を行う方法も考えられるが、リソースと申請期間の問題で非現実的である） |
| | 証明書 | — | <ul style="list-style-type: none"> • 申請書と申請内容を証明する書類を用意する（他資格でも必ずセットになっている） • 実施した業務については、所属組織（独立系であれば顧客）からの証明をもって信頼性を担保 |
| | 業務委託契約書 | 申請者本人の担当領域が契約内容に織り込まれているケースは稀であり、証拠書類としての機能を果たさない | — |
| ②業務実績を裏付ける証拠資料の提示 | ログ（GitHub、業務システムの監査ログ、JIRAなど） | 証拠書類としての機能は果たしても、申請者本人が実行したかどうかは明確ではないため内容の評価は難しい | — |
| | 成果物や報告書（セキュリティポリシー、監査報告、脆弱性診断など） | 機密性の高い情報が多いため対外的に情報を出せないか、仮に出せたとしてもマスキングが必要なため実現可能性が低い | — |
| | 所属長や顧客の署名入りとする | — | （上記「証明書」における記載の通り） |
| | 既存資格保有者によるエンドーズメント | 業務内容を正確に評価できる社内や取引先にスペシャリストがいるケースが全てではない | — |
| ③第三者の確認 | 役務提供された側（所属長や顧客）から実施業務の評価や推薦を提示してもらう | 申請者本人に見えない形で評価する必要がある、運用上実現可能性が低い | — |
| | 認証機関の設置（経産省/IPA /支援士会/有識者/既存資格保有者によるエンドーズメント） | <ul style="list-style-type: none"> • 現行の更新申請期限（更新の60日前）を前提とする場合、いずれの場合であっても、相当のコスト・時間がかかり、期限までの審査が間に合わないリスクが大きい • また、申請者に対しても、早期の申請書提出を強いることになり、申請者の利便性を損なう可能性が高い | — |
| | ランダムな精査（サンプリングチェック） | — | 申請事案の中からサンプル調査を行う |
| ④虚偽申告に対するペナルティの導入 | 罰則規定（資格取り消し、一定期間の業務停止、受験禁止などの措置） | — | 経済産業大臣の資格取消権（法第19条第2項）で対応可能 |
| | 申請者への宣誓書要求 | — | 申請書に虚偽の記載がないことの宣誓同意文言の追加 |

I 検討会における議論の全体像

II セキュリティ・キャンプ

III 登録セキスペ

**IV 中堅・中小企業等の内部でセキュリティ対策
を推進する者の確保・育成**

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

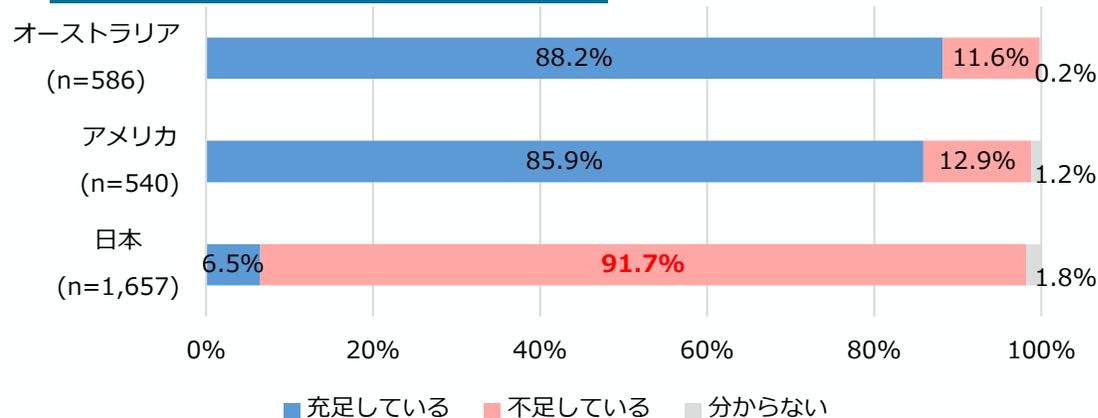
- 1 中堅・中小企業のセキュリティ人材の現状・課題
- 2 人材確保・育成の実践的方策ガイドの位置付け
- 3 実践的方策ガイドにおける4つのStep
- 4 令和7年度の活動概要
(有識者プレゼンテーション等を踏まえたブラッシュアップ)

IV-1 中堅・中小企業のセキュリティ人材の現状・課題

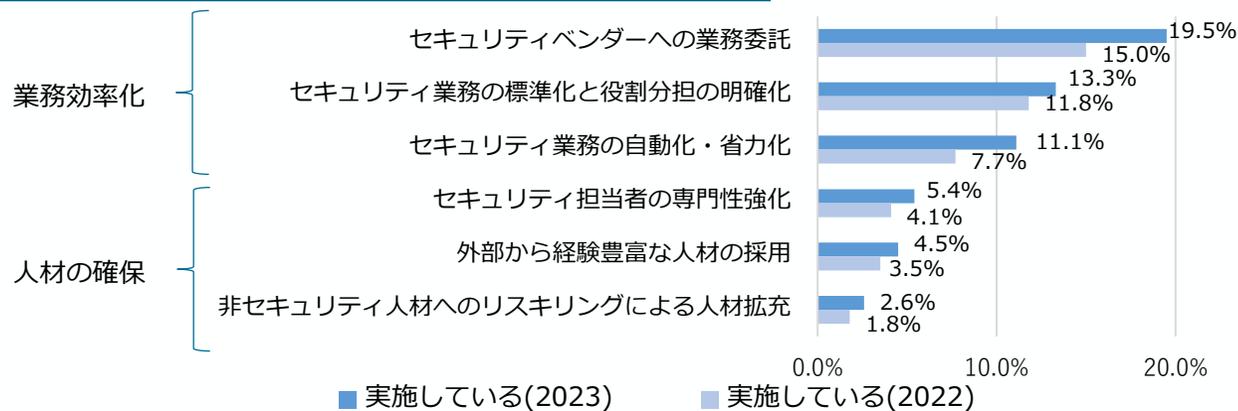
- 民間調査によると、我が国では企業の規模に関わらず、**9割の企業がセキュリティ人材が不足している**と回答。また、社内のセキュリティ人材不足を補う施策として、人材確保の取組を実施している企業は少ない。
- 令和6年度に実施した中小企業実態調査では、**セキュリティ対策の社内体制が無いこと**や、情報セキュリティ教育が実施されない要因として**適切なコンテンツが分からない**という結果を得られた。
- 経済産業省およびIPAでは、企業のセキュリティ人材の確保・育成に資するガイドライン等を策定してきたが、多くの中堅・中小企業にとって**長文のガイドラインを読むことは困難**であり、セキュリティ人材の確保・育成の取組促進につながっていない状況。

→ この状況を踏まえ、企業におけるセキュリティ人材の確保・育成を促進するため、既存のガイドライン等を整理し、分かりやすく提示する効果的なガイドを作成

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



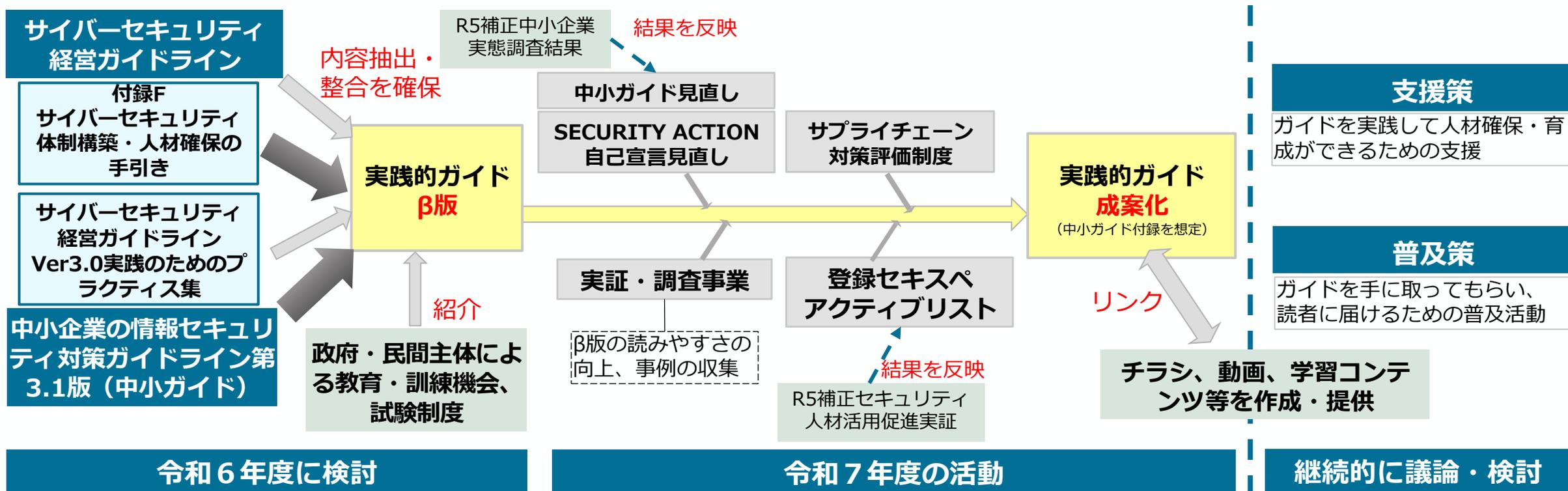
出典：NRI セキュア 企業における情報セキュリティ実態調査2023

中小企業実態調査(R6年度実施事業)

- 回答企業の47%が「セキュリティ対策の必要性を感じたことがない」
- 回答企業の70%においてセキュリティ対策に関わる社内体制が無い（専門部署、兼務担当者の任命がない）
- 回答企業の64%が従業員に対する情報セキュリティ教育を「特に実施していない」
 - 人材育成の外部研修を活用しない、活用する意向がない主な理由は「適切な演習がない・わからない」（41%）

IV-2 人材確保・育成の実践的方策ガイドの位置付け

- 人材の確保・育成については既に、「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2.0版」等が策定されているところ、使いやすさをより向上させる観点から、**人材確保・育成策の標準的なエッセンスを段階的かつコンパクトに示すガイドを策定**。
- 併せて、セキュリティ対策に関する**経営者へ向けたメッセージ**、**外部人材の活用方策**や**教育・訓練機会**等も提示。
- 既存のガイドライン**等から、具体的なセキュリティ対策や人材の確保策に関する内容を抽出して**整合性を確保**しつつ**充実**を図った上で、「**中小企業の情報セキュリティ対策ガイドライン**」の**付録**とすることを想定。
- 令和7年度、関連施策の進展や実証・調査事業の成果を踏まえ、使いやすさを向上させて成案化。ガイドの普及策やガイドに書かれた方策実行のための支援策は継続的に検討。



IV-3 実践的方策ガイドにおける4つのStep

- 企業が実施するセキュリティ対策を4つのStepに分け、対策の実施に必要なタスク、人材の確保・育成策を提示。

| | | 実施するセキュリティ対策 | 人材の確保・育成の方策（外部人材の活用） | |
|---------------|--------------------------|--|---|--|
| （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か条の実施 | 「兼務であっても、一人はセキュリティ担当者を配置」 ・配置転換、社内公募による人材確保 | 取組の開始前や取組中において、不明点等を登録セキスペ等の外部のセキュリティ専門家に相談することも有効 |
| | Step2 「組織的な取組」 | 担当者の下で、組織的な取組を開始 ・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 | 「兼任人材の増員」 ・配置転換、社内公募による兼任人材の増員 ・既存情報、学習コンテンツ、セミナーの活用 ・試験、資格の活用 | |
| （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 | 「自社のセキュリティ体制を構築」 ・専任人材、セキュリティ責任者の任命 ・配置転換、社内公募による兼任人材の増員 ・既存情報、学習コンテンツ、セミナーの活用 ・試験、資格の活用 | 必要なセキュリティ対策を全て内部人材で実施することは困難であるが、自社で実施する業務と外部委託が可能な業務を判断し、適切に委託先を管理することが必要 |
| | Step4 「継続的な改善より強固な対策」 | 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 | 「自社のシステムに応じた脆弱性の管理、インシデント対応に必要な人材を確保」 ・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 ・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 ・専任の人材による兼任人材への指導 ・教育プログラムの受講 | 自社の人材育成、リスクの洗い出し、実施すべき対策の検討等においては、登録セキスペ等の外部のセキュリティ専門家の活用が有効 |

IV-4 令和7年度の取組（人材確保・育成のための実践的方策ガイド）

① 成案化に向けた取組

- 有識者プレゼンでは、**中堅・中小企業にとってセキュリティ人材の確保・育成に関する事例やインシデント事例を示すことが重要**との意見が得られたことから、より身近な中堅・中小企業における事例収集や改善点を整理するためのヒアリング調査と、実践的方策ガイドβ版を一定期間活用していただく**実証**を行う。調査・実証で得られた事例や課題は、**実践的方策ガイドβ版に反映し、より実効性の高いものとして成案化する**。
 - ✓ **調査**：事例集に掲載するためのセキュリティ対策の実施及び検討の契機となる事例（ホラーストーリーやグッドプラクティス）、実践における課題や改善点並びに業界や企業規模に応じた特性を考慮した課題や改善点等をヒアリング調査で収集。
 - ✓ **実証**：実践的方策ガイドβ版の活用事例や改善点、社内人材の配置転換に関する判断基準、育成策の選定理由等を調査し、企業が実践する際の課題や補足情報を収集。

② 普及策の展開

- 有識者プレゼンでは、**人的資源の不足などの課題を抱える中小企業に対して、長文のガイド以外の訴求方法が望ましい**との意見が得られたことから、ガイドの内容を経営者や担当者向けに、**動画やチラシなどの媒体で普及を図るための取組を進める**。
- 地域SECURITYや各地方局を通じて各地域で開催するセミナーやイベントにおいて、実践的方策ガイドを紹介。これにより、**地域において中小企業のセキュリティ対策を支援する民間企業や団体が、実践的方策ガイドを踏まえた活動をすることも可能**。

③ 他制度との連携

- SA宣言：実践的方策ガイドのStep1とStep2はSECURITY ACTION（SA）宣言の一つ星と二つ星に関連しているが、**SA宣言は令和7年度中に基準の改訂を実施する予定であるため、内容の整合性を図る**。
- SC対策評価制度：令和8年度の制度開始を目指し、検討中の**サプライチェーン（SC）対策評価制度と実践的方策ガイドを関連付けて検討**。また、ガイドでは対策の実施方法や人材の確保・育成、外部人材の活用法を記載し、**SC対策評価制度の定着にも役立つ文書と位置付け**。
- 登録セキスペ：登録セキスペアクティブリストを活用した中小企業支援策の具体化を踏まえつつ、**外部人材としての登録セキスペの活用方を記載**。

〔有識者プレゼン等での声〕

実践的方策ガイドの内容

- 大企業や海外ではなく、**国内の中小企業による取組事例**を生々しく発信すべき。
また、**企業の規模や産業別に事例**を収集できると良い。
- PDCAの観点から**継続的に対策を見直す必要性**を訴求する必要がある。
- 人間の脆弱性で攻撃を受けてしまうことから、社内リテラシーや社内教育が必要。

<以上有識者プレゼン等>

〔令和7年度以降における対応の方向性〕

- ✓ 実践的方策ガイド（β版）を中小企業に実際に活用いただくこと等により、**調査・実証を実施し、以下の事例等を収集し、β版の成案化に際して追加。**
 - サイバーセキュリティ人材確保・育成の事例、工夫点
 - 内部人材の役割、外部人材の活用に関する事例
- （β版に、①継続的な対策見直しの必要性、②社内における理解促進についても追記）

実践的方策ガイドの普及

- 人的資源の不足等により多忙な中小企業が多い中、長いガイドを読むことは難しく、**映像コンテンツによる訴求が有効**ではないか。
- 実践的方策ガイドを踏まえて、中小企業に受け取ってもらいやすいコンテンツを提供し、ユーザに届ける役割を（民間企業として）担うことが考えられる。

<以上有識者プレゼン等>

- ✓ 支援機関、業界団体、教育コンテンツ提供者等を通じた普及のほか、**読者に応じたチラシの作成、映像コンテンツ等の作成による普及も推進。**
- ✓ 地域において中小企業のセキュリティ対策を支援する民間企業や団体が、**実践的方策ガイドを踏まえた活動をすることも可能。**



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（案）

1. 実践的方策ガイドの目的

企業のサイバーセキュリティ対策を実施するためには、**自社の業務を理解し、対策をリードする人材を組織として確保・育成することが重要**です。

本ガイドは、**これからセキュリティ対策を始める、今後セキュリティ対策を強化していきたい**中堅・中小企業の経営者やサイバーセキュリティ対策の担当者の皆様が、**セキュリティ人材の確保・育成を実践できるようにすることを目的に**、以下の内容をまとめました。

- ①**実施していただきたいセキュリティ対策を段階的に提示**
- ②**各段階における社内セキュリティ担当者の役割・業務を提示**
- ③**対策を実行するための人材の確保・育成の方策を紹介**

本ガイドを活用して、適切なセキュリティ体制の構築、対策の実施に役立てていただければ幸いです。

2. 本ガイドにおけるStepの全体像

本ガイドでは、皆様に実施していただきたいセキュリティ対策を段階的に4つのStepに分けています。さらに、各Stepにおいて、「実施するセキュリティ対策」から「対策実施のためのタスク」、「人材の確保・育成策」に至るまでを提示しています。

自社の状況に応じたStepから、対策実施のためのタスクや人材確保・育成策を参考に取組を進めてください。また、各Stepの取組結果を考慮し、ステップアップを含めて取組を不断に見直す必要があります。

4つのStepを提示

Step1

取組の開始

兼務の担当者を一人確保

Step1の取組は、規模や業種に関わらず、全ての企業が実施しましょう。

Step2

組織的な取組

兼務の担当者を増員

Step3

本格的な取組

専任担当者の確保
兼任担当者の増員

Step4

継続的な改善
より強固な対策

必要な人材・体制の
見直しと確保

各Stepごとに取組を提示

実施するセキュ
リティ対策

対策実施のため
のタスク

人材の確保・
育成策

- ▶ 社内人材の確保
- ▶ 外部人材の活用
- ▶ 既存情報・学習コンテンツ・セミナーの活用
- ▶ 試験・資格の活用

サイバーセキュリティお助け隊サービス <https://www.ipa.go.jp/security/otasuketai-pr/>

取組の開始前や各Stepの取組と合わせて、中小企業のサイバーセキュリティ対策に不可欠な各種サービス（見守り、駆付け、保険）をワンパッケージで安価に提供する、国が認定したセキュリティサービスである「サイバーセキュリティお助け隊サービス」の導入が有効です。

情報処理安全確保支援士（登録セキスペ） <https://www.ipa.go.jp/jinzai/riss/index.html>

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である情報処理安全確保支援士（登録セキスペ）への相談も有効です。サイバーセキュリティに関する相談に応じて、企業の取組に対して分析や評価を行い、その結果に基づいて指導・助言を行います。

3. 経営者の皆様へ

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おそれ**があります。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**につながります。さらに、事業活動の停止は、自社が不利益を被るだけでなく、**自社が属するサプライチェーン全体にも広く影響を与えかねない**ものです。

このように、企業にとって、**セキュリティ対策に取り組むことは必要不可欠であり、社会的な責務**と言えます。対策を進めるにあたっては、**自社の事業を理解してセキュリティ対策を推進**したり、**いざというときにすぐに対応する自社の担当者が必要不可欠**です。また、技術的なセキュリティ対策を導入しても、従業員の対応次第でサイバー攻撃を受けてしまうこともあり得ます。

したがって、**経営者は、セキュリティ対策の重要性を認識し、社内の対策の推進役であるセキュリティ担当者の業務を支援**するとともに、担当者を通じて、**各従業員が必要なセキュリティ対策を理解し、実施できるように**することが求められます。併せて、適切な外部人材の活用も重要です。

「あなたの対策が、自社や取引の安全を守る第一歩です！」

サイバー攻撃被害^{*}の約6割が中小企業！
大企業に限ったものではありません！

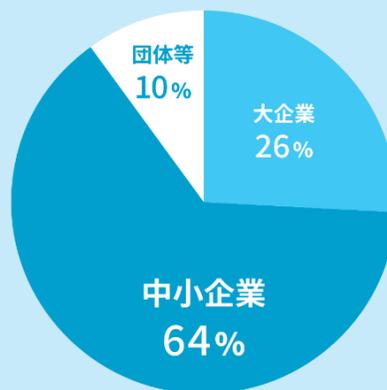
※ランサムウェアによる被害



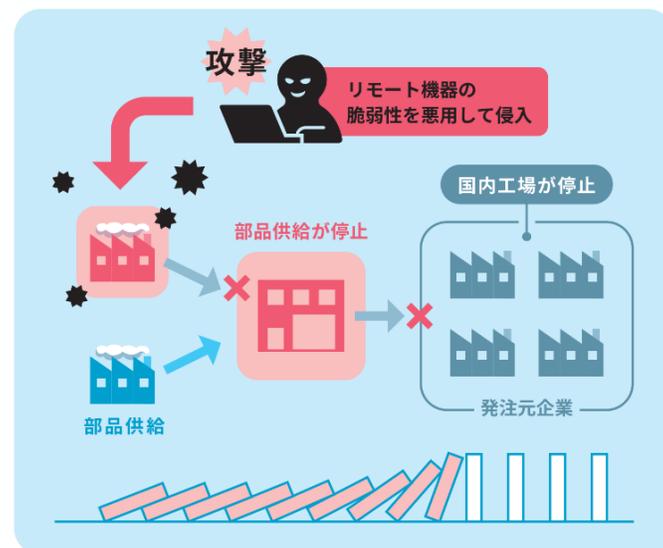
サイバー攻撃により、被害が連鎖して取引先やその先まで企業の業務が停止する「**サイバードミノ**」が起こります！



ランサムウェア被害企業等の規模別割合



警察庁：「令和6年上半年期におけるサイバー空間をめぐる脅威の情勢等について」に基づき作成



4. 段階的な取組 Step 1 取組の開始 1/2

全ての企業が実施すべき基本的なセキュリティ対策に取り組み、自社の業務・情報・従業員・取引先を守る土台を作りましょう。

実施するセキュリティ対策のポイント

基本的な対策を実施しましょう

(情報セキュリティ5か条⁽¹⁾の実施)

①利用するパソコン等への対策

- ・OSやソフトウェアの最新化 ・ウイルス対策ソフトの導入
- 対策を実施する対象機器を把握しましょう。
定期的なチェックをしましょう。

②従業員が理解、実施する対策

- ・パスワードの強化 ・攻撃の手口を知る

長く複雑なパスワードを設定しましょう。パスワードを使いまわさないようにしましょう。

不審メール、不正サイトやランサムウェア、攻撃の手口を知りましょう。

③利用するシステムへの対策

- ・共有設定の見直し

個人情報や企業秘密は正規の必要な人のみアクセスできるようにしましょう。

対策実施のためのタスク

内部人材のタスク

①OSやソフトウェア、NW機器更新のための活動

→ 自社が保有するパソコン、NW機器等を確認し、自動更新設定がある場合は実施します。OS等の更新において従業員の作業が必要な場合は、実施マニュアルを作成し、周知します。

②従業員に対策を周知し、継続してもらうための活動

→ 情報セキュリティ5か条の内容を朝礼や社内メール等によって従業員に周知します。従業員の作業が必要な場合は、実施マニュアルを作成し、周知します。
→ 社内のセキュリティ相談、報告の窓口として対応します。

③利用サービス、NW機器等に適切な設定をする活動

→ 保有するデータやサービス、アカウント等を社内の誰が利用可能か明らかにし、必要に応じてITベンダーと相談して、適切な設定を実施します。

④上記の活動に必要なIT知識を身に付けるための活動

→ 既存コンテンツ活用、資格取得に向けた学習等を実施します。

基本的な取組事項である情報セキュリティ5か条については、自社において理解のうえ対応することが原則ですが、外部人材の支援を要する場合、例えば以下のような活用が考えられます。

外部人材のタスク

(企業からの依頼に応じて対応)

①企業のセキュリティに関する助言

→ セキュリティ対策の必要性の理解を助け、情報セキュリティ5か条の実施に必要な助言をします。

②従業員向け教育の提案、実施対応

→ 情報セキュリティ5か条を全従業員で実践するために必要な、セキュリティ担当者への教育、全従業員への講演等を提案・実施します。

※セキュリティ関連タスクに応じた、外部委託の判断基準について、詳しくは「[サイバーセキュリティ体制構築・人材確保の手引き](#)(2)」(以下、人材手引き)p20に記載があります。

(1)情報セキュリティ5か条:https://www.ipa.go.jp/security/security-action/download/5point_poster.pdf

(2)サイバーセキュリティ体制構築・人材確保の手引き:<https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf>

4. 段階的な取組 Step1 取組の開始 2/2

- 基本的なセキュリティ対策を実施するためには、兼務でも社内に1人はセキュリティ担当者を確保しましょう。
- 内部だけで実施が難しい対策については、外部の人材・リソースに相談しましょう。
- 基本的な映像コンテンツを活用したり、基本的な資格試験へのチャレンジを促しましょう。

確保

社内人材

- 情報セキュリティ5か条を実践するために、セキュリティ担当者を兼務でも1人は確保しましょう。
- ＜配置転換＞（人材手引きp25）
- セキュリティの知見がある従業員がいなくても、少しでも関連業務の経験がある者をセキュリティ担当を兼務させます。
 - ・災害対策等を行う部署
 - ・IT部門
 - ・監督者
 - ・PC導入担当
- ＜希望者の登用＞
- セキュリティ業務の実施を希望する従業員の社内公募を実施し、セキュリティ担当者を兼務させます。
 - ※自社の事業特性から、高いセキュリティレベルが求められる場合は、外部からの専門人材の採用を検討します。

外部人材の活用

- 既にパスがある（付き合いがある）ITベンダーや、商工会・商工会議所等の支援機関と、自社のセキュリティについてコミュニケーションを取り、情報セキュリティ5か条の実施に関する課題、従業員への周知方法、教育方法について相談します。
- [IPA情報セキュリティ安心窓口](#)(3)を活用し、セキュリティに関する不安や課題を相談します。
- ※相談に当たっての注意点
 - 相談ポイントが分からない場合もあるかもしれませんが、例えば「データの漏洩が心配」「従業員の教育が不十分ではないか」「ニュースで聞いたランサムウェア攻撃、自社は大丈夫か」など身近なところから課題を挙げてみましょう。
 - 相談の際には、自社の業種・規模、実施中のセキュリティ対策について簡単に説明することで、より具体的なアドバイスを受けやすくなります。

育成

既存情報、学習コンテンツ、セミナーの活用

- [IPA映像コンテンツ](#)(4)の視聴
 - 情報セキュリティ5か条説明：<https://www.youtube.com/watch?v=OP7O12w6KnQ>
 - ランサムウェア攻撃の説明：<https://www.youtube.com/watch?v=TWqJ5P8oaUM>
 - メール詐欺の説明：<https://www.youtube.com/watch?v=6DKJEG3woRU>
 - パスワード強化：<https://www.ipa.go.jp/security/chocotto/index.html>
- デジタル知識・スキルが学べるデジタル人材育成プラットフォームである[マナビDX](#)(5)のリテラシー講座の受講
- 1テーマ5分で情報セキュリティについて勉強できる無料の学習コンテンツIPA5分のできる！[情報セキュリティポイント学習](#)(6)による学習
- NISC[インターネットの安心・安全ハンドブック 中小企業向け抜粋版](#)(7)を社内研修の資料として活用する。

試験、資格の活用

- 情報セキュリティを含むIT全般の基本的知識に関する試験「[ITパスポート試験](#)」(8)を取得を促し、IT知識を習得。（人材手引きP38）

(3) IPA情報セキュリティ相談窓口：<https://www.ipa.go.jp/security/anshin/index.html>

(4) IPA映像コンテンツ一覧：<https://www.ipa.go.jp/security/videos/list.html>

(5) マナビDX：<https://manabi-dx.ipa.go.jp/>

(6) IPA5分のできる！情報セキュリティポイント学習：https://www.ipa.go.jp/security/sec-tools/5mins_point.html

(7) インターネットの安心・安全ハンドブック：https://security-portal.nisc.go.jp/guidance/books/digital_book_sme/book/index.html#target/page_no=1

(8) ITパスポート試験：<https://www.3jitec.ipa.go.jp/JitesCbt/index.html>

4. 段階的な取組 Step2 組織的な取組 1/2

組織的な対策をはじめます。自社の情報セキュリティ基本方針を作成し従業員へ周知しましょう。また、自社のセキュリティ対策の実施状況を把握し、対策を決定し周知しましょう。

実施するセキュリティ対策のポイント

組織的な取組を開始しましょう

①従業員の指針となる情報セキュリティ基本方針の作成

管理体制の整備、法令・ガイドライン等の遵守、セキュリティ対策の実施など、組織の基本方針を決定し従業員や顧客などの関係者に周知します。

②組織の実施状況の把握

自社が、現在どの程度情報セキュリティ対策を実施できているかを把握します。

③対策の決定と周知

USB等の記録媒体の保管、インターネット利用等に関する従業員としての対策、従業員への教育の実施、緊急時の体制整備など組織としての対策を決定し、周知します。

対策実施のためのタスク

セキュリティ基本方針は自社自身が策定する必要があります。ただし、方針の内容に関する助言を受けたり従業員への社内教育を実施するためには、外部人材の活用が有効です。

内部人材のタスク

①基本方針を検討、策定する活動

→ 「[情報セキュリティ基本方針（サンプル）](#) (9)」を参考にして、事業の特徴や顧客の期待などを考慮し、自社に適した基本方針を作成します。

②自社組織のセキュリティ対策の状況を把握する活動

→ 「[5分でできる！情報セキュリティ自社診断](#) (10)」を利用して、自社のセキュリティ対策の実施状況を把握します。

③自社の対策を決定し、従業員に周知する活動

→ ②の診断結果と「5分でできる！情報セキュリティ自社診断」の解説編を参考に、自社で実施すべき対策を決定し、従業員に周知します。

④上記の活動に必要なIT知識を身に付けるための活動

→ 既存コンテンツを活用して、資格取得に向けた学習等を実施します。

外部人材のタスク

(企業からの依頼に応じて対応)

①企業のセキュリティに関する課題相談対応

→ 企業の事業特性に合わせた情報セキュリティ基本方針について提案します。

→ 企業に応じて実施すべきセキュリティ対策を提案します。

②従業員向け教育の提案・実施

→ 組織的な対策実施のために必要なセキュリティ担当者への教育、従業員への講習等を提案・実施します。

(9)情報セキュリティ基本方針（サンプル）：<https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000108033.pptx>

(10) 5分でできる！情報セキュリティ自社診断：<https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055848.pdf>

4. 段階的な取組 Step2 組織的な取組 2/2

- ・組織的なセキュリティ対策を実施するために、兼務のセキュリティ担当者を複数確保し、育成しましょう。
- ・従業員への教育や講習について、外部の人材やリソースを活用しましょう。
- ・社内の役割に応じた映像コンテンツを視聴したり、少し上位の資格へのチャレンジを促しましょう。

確保

| 社内人材 | 外部人材の活用 |
|--|---|
| <ul style="list-style-type: none"> ○社内ルールを作り、社員に守らせるなど業務量が増えることに応じて、担当者も増やす必要が出てきます。 ○そのため、Step1で示した隣接分野での業務経験を有する人材の<配置転換>、<希望者の登用>を引き続き実施します。 <p>※自社の事業特性から、高いセキュリティレベルが求められる場合は、外部からの専門人材の採用を検討します。</p> | <ul style="list-style-type: none"> ○既にパスがあるITベンダーや、商工会・商工会議所等の支援機関などに、組織的なセキュリティの取組、社内の情報セキュリティ基本方針の作成等について相談します。 ○IPAセキュリティプレゼンター⁽¹¹⁾を活用し、従業員へのセキュリティ教育や講習が実施可能な人材を確保します。 ○セキュリティに関する身近なコミュニティ(*)に参画し、交流・情報収集を行うことで、外部人材の活用の幅が広がる可能性があります。 <p>*地域SECURITY 地域の民間企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティであり、イベントの継続開催による意識向上や人材育成、国や専門家からの情報提供の場となります。詳しくは地域SECURITY⁽¹²⁾をご覧ください。</p> |

育成

| 既存情報、学習コンテンツ、セミナーの活用 | 試験、資格の活用 |
|--|--|
| <ul style="list-style-type: none"> ○所属、役職に適したIPA映像コンテンツの視聴 経営者向け動画：https://www.youtube.com/watch?v=qlcIBHIUKd0 全従業員向け啓発動画：https://www.youtube.com/watch?v=5K9U0-ASQM8 新入社員向け啓発動画：https://www.youtube.com/watch?v=FljLaQA-cRU ○IPAセキュリティプレゼンターによる社内セミナー聴講 ○マナビDXのセキュリティ関連講座の受講 ○IPA重要なセキュリティ情報⁽¹³⁾を確認し、危険性が高い最新のセキュリティ上の問題と対策情報の収集 | <ul style="list-style-type: none"> ○組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的なスキルを認定する試験である「情報セキュリティマネジメント試験⁽¹⁴⁾」の資格取得を促し、IT知識を習得。(人材手引きP38) |
| | コミュニティへの参加 |
| | <ul style="list-style-type: none"> ○セキュリティに関する地域のコミュニティに参加し、他社担当者からの情報収集、意見交換を実施 |

(11) IPAセキュリティプレゼンター：<https://www.ipa.go.jp/security/sme/presenter/index.html>

(12) 地域SECURITY：<https://www.meti.go.jp/policy/netsecurity/secunity.html>

(13) 重要なセキュリティ情報：<https://www.ipa.go.jp/security/security-alert/index.html>

(14) 情報セキュリティマネジメント試験：<https://www.ipa.go.jp/shiken/kubun/sg/about.html>

4. 段階的な取組 Step3 本格的な取組 1/2

本格的なセキュリティ対策をはじめましょう。自社体制の整備、対応すべきリスク(事故が発生したとき事業へ損害を与える危険性)を特定したうえで、適切な対策を記述した情報セキュリティ規程を作成し、実行しましょう。

実施するセキュリティ対策のポイント

本格的な取組を開始しましょう

①管理体制の構築

情報セキュリティ基本方針を実践し、情報セキュリティ対策を推進する体制として「責任分担と連絡体制の整備」、「緊急時対応体制の整備」をします。

②予算の確保

情報セキュリティ対策の実施に必要な予算を確保します。

③情報セキュリティ規程の作成

「対応すべきリスクの特定」、「対策の決定」をし、自社に適した対策を記述した文書(情報セキュリティ規程)を作成しましょう。規程には、以下の項目が想定されます。

- ・ **情報資産管理**：情報資産の管理や持ち出し方法、バックアップ、破棄などのルールを定めます。
- ・ **アクセス制御及び認証**：情報資産に対するアクセス制御方針や認証のルールを定めます。
- ・ **委託管理**：業務委託にあたっての選定や契約、評価のルールを定めます。
- ・ **セキュリティインシデント対応、事業継続管理**：情報セキュリティに関する事故対応や事業継続管理などのルールを定めます。

④点検と改善

計画した情報セキュリティ対策が実行されているか、見落としがないか、確認をしましょう。

対策実施のためのタスク

自社体制の決定、予算確保は経営判断であり、自社自身が決める必要があります。ただし、専門性の求められるシステム保守(ユーザー権限管理等は自社で実施)、自社規程に沿った対策のうち、内部人材で実施困難なタスクは外部委託が有効です。

内部人材のタスク

①自社のセキュリティ体制を検討、整備する活動

→ 「情報セキュリティ責任者」、「教育責任者」、「点検責任者」等の役職の役割と責任を決め、緊急時の連絡体制を整備します。

→ 朝礼や社内メール、掲示板等を活用し、従業員に周知します。

②対策に必要な予算を検討し、確保する活動

→ 外部専門家やITベンダーを活用し、必要な対策と予算額を検討し、社内で理解を得て予算を確保します。

③情報セキュリティ規程の内容を作成し周知する活動

→ 「[情報セキュリティ関連規程\(サンプル\)](#) (15)」を参考に、自社に適した規程を作成します。

④セキュリティ対策の実効性を確保する活動

→ 社内確認テストや簡易的な社内監査を実施し、計画したセキュリティ対策を実行されているか、改善点がないかを確認します。

⑤上記の活動に必要なIT知識を身に付けるための活動

→ 既存コンテンツを活用し、資格取得に向けた学習等を実施します。

外部人材のタスク

(企業からの依頼に応じて対応)

①企業のセキュリティに関する課題相談対応

→ 体制構築、情報資産管理、リスクを特定した上で必要なセキュリティ対策の検討、インシデント発生時の訓練企画などに関して支援を実施します。

②従業員向け教育の提案、実施対応

→ 所属、役職に応じた教育計画の提案と実施をします。

③専門性が求められるタスクの実施

→ 決定した対策を実現させるためのシステムや機器への設定変更、システム保守等を実施します。

4. 段階的な取組 Step3 本格的な取組 2/2

- ・本格的なセキュリティ対策を実施するために、専任のセキュリティ担当者確保・育成しましょう。
- ・特に技術的・専門的な対策については、社内のリテラシーを高めつつ外部の専門家やサービスを活用しましょう。
- ・インシデント対応に関する映像コンテンツや、高度な研修プログラムへの参加も視野に入ります。

確保

社内人材

- 社内に適切な体制を確保するとともに、セキュリティ対策業務に関して知識と経験を持つ人材の確保が必要です。
 - Step1で示した隣接分野での業務経験を有する人材の<配置転換>、<希望者の登用>を引き続き実施し体制を構築します。
- <人材の採用>
- 他社等でサイバーセキュリティ対策業務に従事した経験を有する人材を中途採用し、自社で活用します。(手引きp25)

外部人材の活用

- 情報セキュリティ規程の策定や周知、改善に関して、支援機関等への相談を実施します。また、ITベンダーに情報セキュリティ規程に沿った必要な対策の実施について相談します。
- 外部のセキュリティ専門家の支援を活用し、自社の対策を分析・評価・助言できる人材を確保しコンサルティングを依頼します。
- 外部のセキュリティ専門家の支援を活用し、インシデント時の対応や事業継続管理などのルールの策定、訓練等を実施します。
- 適切な異常監視、インシデント対応を実施するために、外部のセキュリティサービスを導入します。

育成

既存情報、学習コンテンツ、セミナーの活用

- IPA映像コンテンツの視聴
情報セキュリティ規程作成、運用手順：<https://www.youtube.com/watch?v=fot-PEzBZO4>
セキュリティインシデント、対応：https://www.youtube.com/playlist?list=PLi57U_f9scILiLjIAIRzTjFODLto9q78o
- IPA産業サイバーセキュリティセンター(ICSCoE)短期プログラムの受講
責任者向け講習：<https://www.ipa.go.jp/jinzai/ics/short-pgm/cyberspex/index.html>

試験、資格の活用

- 情報システムに係るリスクを分析し、コントロールを検証・評価することによって、組織体の目標達成に寄与し、利害関係者に対する説明責任を果たす監査人や情報システム責任者向けの「システム監査技術者試験⁽¹⁷⁾」の資格を習得。

(16)ICSCoE短期プログラム：<https://www.ipa.go.jp/jinzai/ics/short-pgm/index.html>

(17)システム監査技術者試験：<https://www.ipa.go.jp/shiken/kubun/au.html>

4. 段階的な取組 Step4 継続的な改善、より強固な対策 1/2

より強固なセキュリティ対策のためには、人的・組織的な対策だけでなく、技術的な対策の強化・外部の専門セキュリティサービスの活用が必要です。

実施するセキュリティ対策のポイント

組織的な取組を開始しましょう

①利用システムに応じたセキュリティ対策の実施

ウェブサイト、クラウドサービス、テレワーク等、自社が利用するシステム、ソフトウェアに応じたセキュリティ対策を実施しましょう。

②セキュリティサービスの活用、技術的対策の実施

セキュリティ監視、運用などのセキュリティサービスと、セキュリティ機器の設置や対策ソフトなどの技術的対策を自社の環境に合わせて活用しましょう。

③セキュリティインシデント対応の強化

「検知・初動対応」、「報告・公表」、「復旧・再発防止」の3つの段階に分けて、事業継続、早期復旧のために備えましょう。

④詳細なリスク分析の実施

自社が保有する「**情報資産の洗出し**」→情報資産の重要度と被害の発生可能性を考慮した「**リスク値の算定**」→リスク値の大きいものから、リスクの低減や回避を実現するための「**情報セキュリティ対策の決定**」の手順で、もれなくリスクを特定し対策を検討します。

対策実施のためのタスク

専門性が求められるセキュリティサービスや技術的対策の導入・運用に当たり、必要性の判断、委託仕様の策定を自社で行い、外部委託を活用します。

ただし、セキュリティ対策実施の外部委託先の管理は、自社自身で実施する必要があります。

内部人材のタスク

①自社特性に応じた対策を検討し、外部委託を適切に活用、管理する活動

→ 自社の利用するシステム、事業特性に応じたセキュリティ対策を検討し、外部委託を活用してセキュリティサービス、技術的対策に関する情報収集、導入を実施します。

→ インシデント発生を想定し、事業継続の観点から被害の最小化、早期復旧のための備えについて、外部委託を活用して検討、実施します。

→ リスク値の算定やリスクの低減には、外部委託を活用して、脆弱性診断の実施やセキュリティ監視サービスを利用します。

外部人材のタスク

(企業からの依頼に応じて対応)

①企業のセキュリティに関する課題相談対応

→ より強固な対策として、セキュリティサービス、技術的対策に関する提案・導入・運用、適切なインシデント対応体制の整備支援を実施します。

②従業員向け教育の提案、実施対応

→ インシデント発生を想定した社内教育、導入されているセキュリティサービスを従業員が適切に利用できるように教育を実施します。

③高い専門知識を必要とするリスク分析の実施

→ 情報資産ごとの重要度の算定、リスク脆弱性診断、セキュリティ監視・運用、情報収集、詳細なリスク分析支援などを実施します。

4. 段階的な取組 Step4 継続的な改善、より強固な対策 2/2

- ・より強固なセキュリティ対策を実施するために、新規採用や専門家の役員招聘も視野に入ります。
- ・技術的対策の相談に加えて、定期的な外部監査の活用や社外の情報共有の枠組みへの参画も視野に入ります。
- ・専門性を高めるための映像コンテンツの活用や、高度な資格へのチャレンジも促しましょう。

確保

| 社内人材 | 外部人材の活用 |
|--|--|
| <ul style="list-style-type: none">○より強固な対策のために、自社の事業を理解し、現状のセキュリティ対策の実効性確保・改善、脆弱性への迅速な対応、新たな対策の検討・実施などが必要です。○このため、一層高い知識・経験・技能を持った人材を確保し、体制を整備する必要があります。Step3までで示した確保策に加えて、次の取組を実施します。 <p><人材の採用></p> <ul style="list-style-type: none">○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（手引きp25）○セキュリティ専門家を招聘して、CISO等に任命します。（手引きp20） | <ul style="list-style-type: none">○ITベンダーに対して、自社の実施している対策、保有するウェブサイト、クラウドサービス、テレワークの利用状況、事業特性などに合わせた追加のセキュリティサービス、技術的対策の必要性について相談します。○法令等遵守対応のため、弁護士等の助言を得るための契約をします。（手引きp20）○監査には、内部監査（第一者）、外部監査（第二者・第三者）がありますが、営業秘密や個人情報等の特に十分な対策が必要な場合には、外部からのセキュリティ監査を実施する第三者を探します。○取引先や同業者を経由したサイバー攻撃も増えていることから、日本シーサート協議会⁽¹⁸⁾や同業界の事業者同士でサイバーセキュリティに関する情報の共有・分析などを行う組織である、ISAC(*)などの情報共有の仕組みを活用します。 |

育成

| 既存情報、学習コンテンツ、セミナーの活用 | 試験、資格の活用 |
|--|---|
| <ul style="list-style-type: none">○IPA映像コンテンツを視聴。 脆弱性発見手法：https://www.youtube.com/playlist?list=PLi57U_f9scIInRwz4QUipc3d3nL_MicfR テレワークセキュリティ：https://www.youtube.com/watch?v=zDs88SLymwo 安全なウェブサイト運用：https://www.youtube.com/playlist?list=PLi57U_f9scIjv-3QIRu5Hc2Bz4-D4-Apa○脆弱性の概要や対策方法等の知識を実習形式で体系的に学べるツール脆弱性体験学習ツール AppGoat⁽¹⁹⁾による学習を実施。 | <ul style="list-style-type: none">○サイバーセキュリティ対策を推進する人材の国家資格である、情報処理安全確保支援士（登録セキスペ）の資格を取得。 <p>コミュニティへの参加</p> <ul style="list-style-type: none">○セキュリティに関する地域のコミュニティに参加し、他社担当者からの情報収集、意見交換を実施。○業界内での情報共有・連携の取り組み推進を図る組織である業界ISACや日本シーサート協議会への参加により情報収集を実施。 |

(18)日本シーサート協議会：<https://www.nca.gr.jp/>

(19)脆弱性学習ツールAppGoat：<https://www.ipa.go.jp/security/vuln/appgoat/index.html>

本ガイドで使用している主な用語の説明

アクセス制御

ユーザ認証とアクセス認可の2段階からなり、利用者や情報機器がデータなどにアクセスすることができる権限や認可を制御する技術です。

監査

組織内においてサイバーセキュリティ対策が適切に実施されているかどうかを判定するために、監査証拠を収集し、それを客観的に評価するための、体系的で、独立し、文書化したプロセスのことです。監査には、内部監査（第一者）又は外部監査（第二者・第三者）があります。

クラウドサービス

サーバー等を自前で所有する代わりに、インターネット経由で同様の機能を提供するものをいいます。レンタルサーバー、SaaS(Software as a service)、ASP(Application Service Provider)などがクラウドサービス的一种です。

CISO (Chief Information Security Officer)

経営陣の一員、もしくは経営トップからその役を任命された、セキュリティ対策を実施する上での責任者のことです。

情報資産

様々な「情報」のうち、企業として管理すべき対象として選択されたものです。また、情報システムなども「情報資産」に含める場合があります。

脆弱性

ソフトウェア等における、管理者の意図しない動作やイベントにつながる可能性のあるセキュリティ上の弱点のことです。

セキュリティインシデント（対応）

セキュリティの事故・出来事のこと、単に「インシデント」という事もあります。例えば、情報の漏えいや改ざん、破壊・消失、情報システムの機能停止またはこれらにつながる可能性のある事象等がインシデントに該当します。インシデント対応には、「検知・初動対応」「報告・公表」「復旧・再発防止の」3つの基本ステップがあります。

ファームウェア

ハードウェア(スマートフォンや家電、ルーターなどのネットワーク機器)を制御するソフトのことです。

リスク分析

リスクの特質を理解し、リスクレベル(ある事象の結果とその起こりやすさとの組合せとして表現されるリスクの大きさ)を決定するプロセスのこと。

セキュリティ監視

組織のITシステムやネットワークを常時モニタリングし、セキュリティ上の脅威を検知・対処するための取り組みのことです。不審な動きを検知し、被害を未然に防ぎます。