経済産業省

第１回
産業サイバーセキュリティ研究会
ワーキンググループ２（経営・人材・国際）
サイバーセキュリティ人材の育成促進に向けた検討会
事務局説明資料

令和６年７月

経済産業省 商務情報政策局

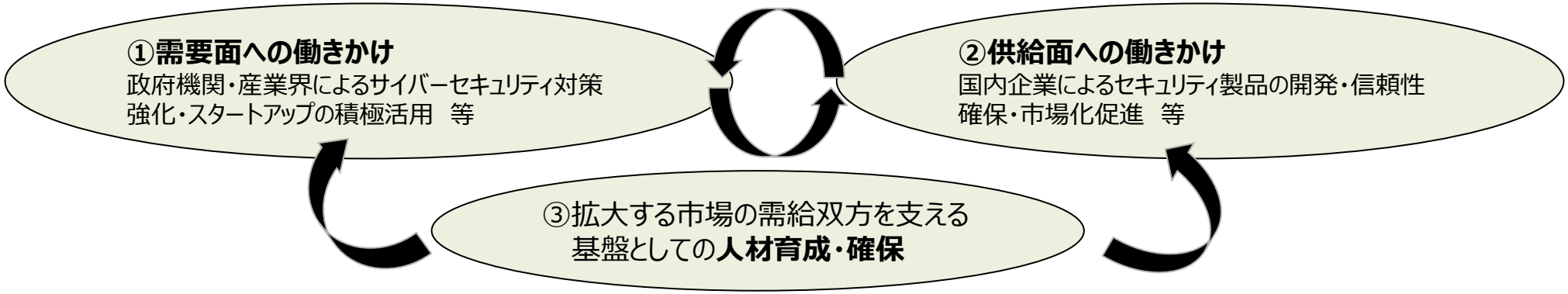
サイバーセキュリティ課

検討の背景

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＞



（資料）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

経済産業省におけるこれまでの人材育成・確保に係る取組

- 産業界におけるセキュリティ人材の育成・確保については、これまで、企業経営層向けの**人材活用の在り方の提示**や、セキュリティ人材として求められる**スキルセットの整理・標準化**、そうした標準も踏まえて**客観的に能力を評価できる試験制度の実施**、**直接的な教育・訓練機会の提供**を実施してきたところ。
- 各取組について**一定のアウトプットを生み出している**ものの、産業界におけるサイバーセキュリティ人材の**需給ギャップの解消・今後増大する需要に対応した人材育成・確保に向けては道半ばな状況**。

＜主なこれまでの取組＞

ガイドライン等

企業経営者等向けに、自社で**セキュリティ人材を確保し体制を整備するための実践的な指針**を提示。

・セキュリティ体制構築・人材の確保の手引き

スキル標準

企業のセキュリティ対策水準を高めるためには、企業の内外から**必要なスキルセットを把握・調達**した上で、これを効果的に統合することが重要。その観点から、IT関連業務（タスク）と、そのタスクの遂行に**必要な実務能力を客観的な評価の尺度**（ものさし）である**スキル標準**として定義。

・共通キャリア・スキルフレームワーク2008
・情報システムユーザースキル標準(UISS)2010
・ITスキル標準（ITSS)2012
・iCD(iコンピテンシ・ディクショナリ) 2014
・ITSS＋(セキュリティ領域)2017公開2020改定
・デジタルスキル標準（DSS）2022年公開2023年改定

試験制度

情報技術を利用する組織がセキュリティ人材の採用や評価を行う際に役立つよう、**セキュリティ人材の社会的地位の確立を図る**ためにスキル標準と紐づいた試験制度を実施。

・情報セキュリティアドミニストレータ試験(2001～2008)
　合格者数24,796人
・テクニカルエンジニア(情報セキュリティ)試験(2006～2008)
　合格者数4,904人
・情報セキュリティスペシャリスト試験(2009～2016)
　合格者44,201人
・情報セキュリティマネジメント試験(2016～)
　合格者数141,712人(R5年度末時点)
・情報処理安全確保支援士試験(2016～)
　合格者33,959人(現行制度)
　登録者数22,692人(R6.4.1現在　旧試験合格者を含む)

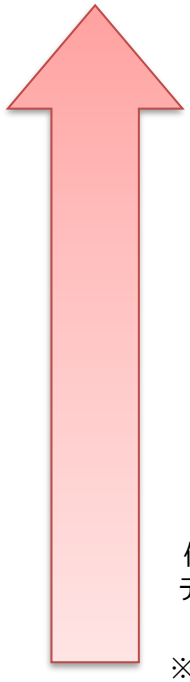
研修・演習プログラム

次代を担うサイバーセキュリティ人材の発掘・育成や、企業経営層と現場担当者を繋ぐ**中核人材を育成**するために、専門的知見を有するIPA（独立行政法人情報処理推進機構）を通じて**直接的な教育・訓練機会を提供**。

・セキュリティ・キャンプ(2004～)
　全国大会累計参加者1,152人
　地方大会（ミニキャンプ）、ネクストキャンプ、ジュニアキャンプも開催
・IPA中核人材育成プログラム(2017～)
　参加者累計435人

サイバーセキュリティ人材の育成・確保に係る状況

- マクロでみると、国内のサイバーセキュリティ人材は約11万人不足しているとの民間調査結果がある（次頁参照）。
- 「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っていない（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おり、**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

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、地方ベンダー実務担当者など

※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。

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

中核人材育成プログラム

登録セキスペ制度

課題

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っていない。

活躍の場が限定的・市場のミスマッチ

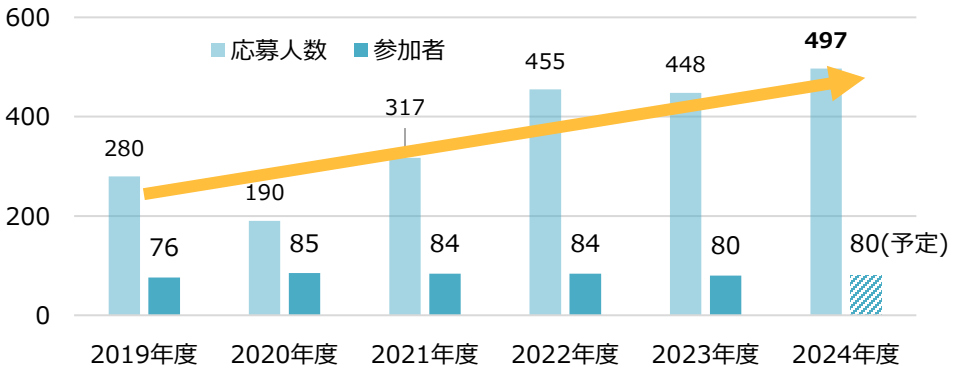
・・・登録セキスペを必要とする需要側企業（中小企業等）において、①サイバーセキュリティ対策の必要性が理解されていない場合（登録セキスペの活躍の場がない）や、②人材不足が懸念される場合（登録セキスペとのミスマッチが起きている）がある。
・・・結果として、登録更新に係る費用を支払うだけの動機が失われ、登録者数の大幅な増加には至っていない。

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）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

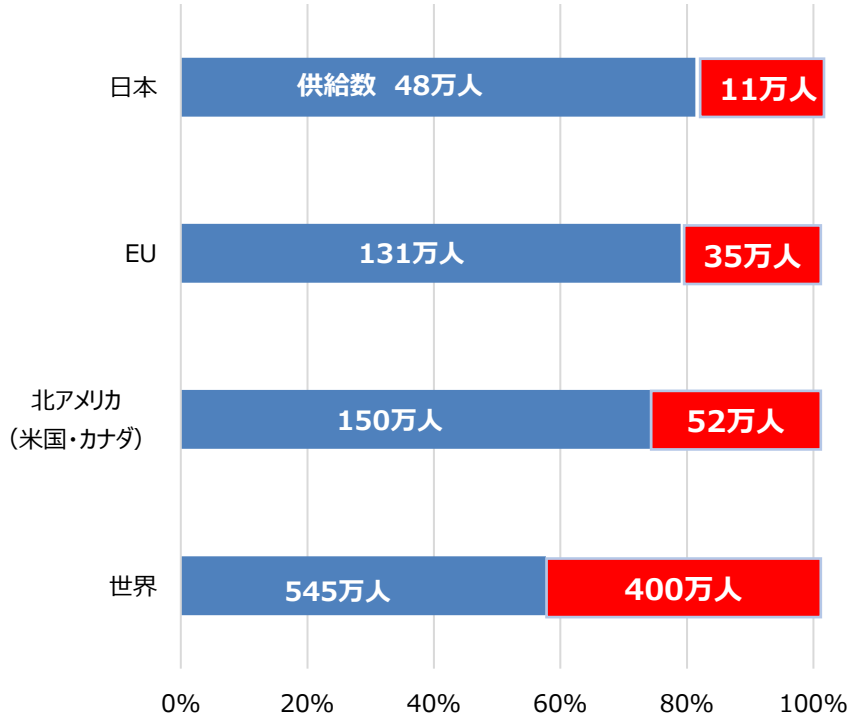


登録セキスペ 登録者数の推移

登録セキスペ 消除理由上位５位

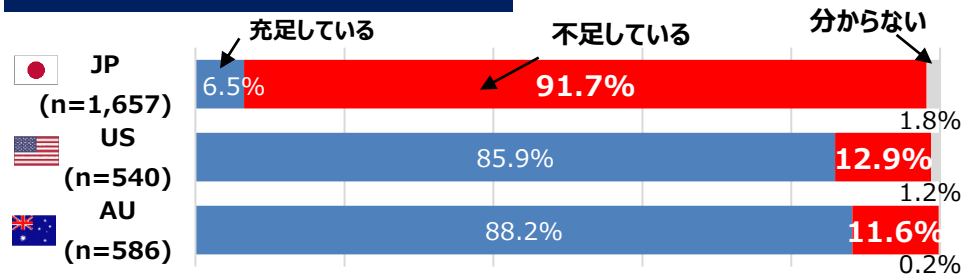
1 位　メリットなし、かつ費用が高額
2 位　転職、異動、業務上不要
3 位　費用が高額
4 位　メリットがない
5 位　転職＋費用負担されなくなった

セキュリティ人材の不足状況①

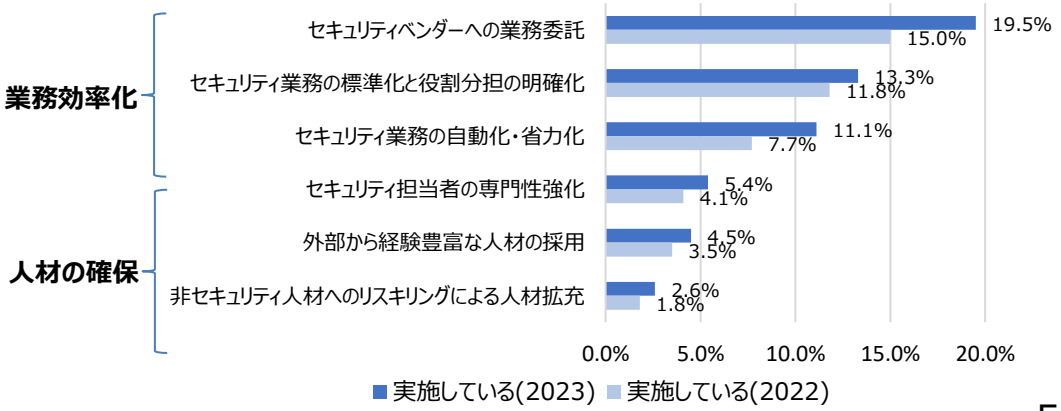


ISC2 Cybersecurity Workforce Study 2023を基に経済産業省作成

セキュリティ人材の不足状況②



セキュリティ人材不足を補う施策の実施状況



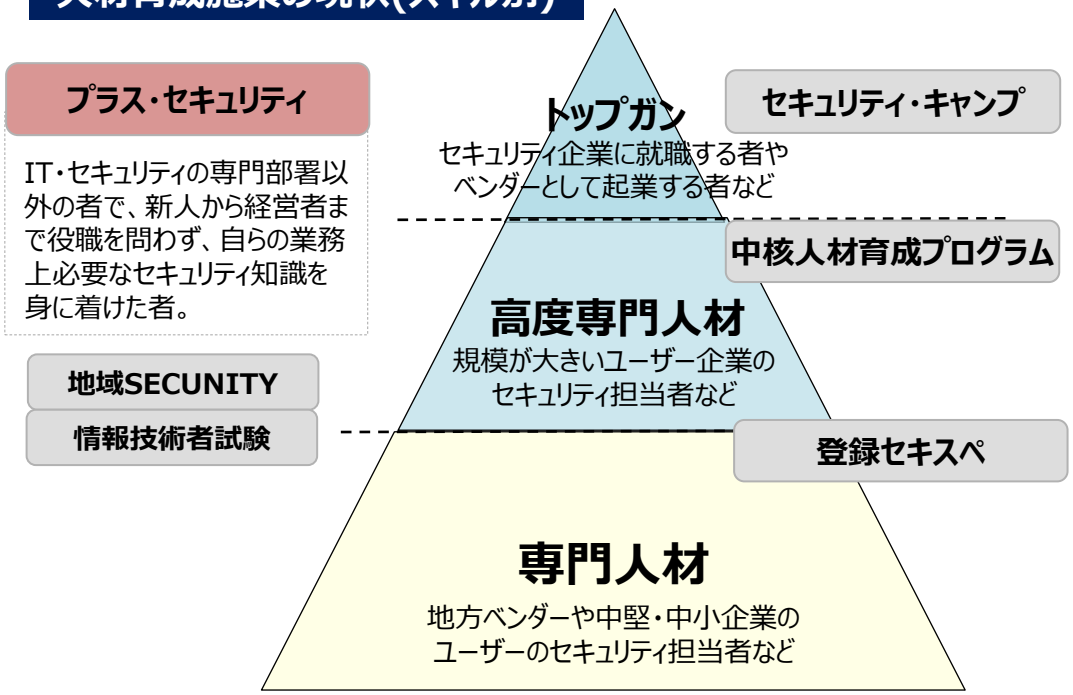
出典：NRI セキュア　企業における情報セキュリティ実態調査2023

サイバーセキュリティ人材の育成・確保に向けた取組の方向性

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

- セキュリティ人材施策として、セキュリティ・キャンプや中核人材育成PG、情報処理安全確保支援士試験を通じた**高度専門人材の育成**、地域SECUNITY活動等を通じた**プラス・セキュリティの普及**等を進めてきているが、**需給ギャップを解消するためには、セキュリティ人材の裾野を更に拡大するための施策の検討が必要**。
- セキュリティ人材不足は、企業の規模に関わらない、共通の課題。今後は、高度専門人材向けの育成を継続して実施するとともに、ユーザー企業や地域ベンダー等における専門人材の育成・確保についても議論してく必要。
- また、 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**ことも必要ではないか。

人材育成施策の現状(スキル別)



現状の課題

- これまで、トップガンや高度専門人材の育成は進めてきたものの、1年間に育成できる人数が限定的。
- 登録セキスペは、首都圏のベンダー側に偏っており、ユーザー企業での活用が進んでいない。
- これまで施策では、地方ベンダーや中堅・中小企業のユーザーのセキュリティ担当者などにアプローチできない。

今後の方向性

- トップガンの発掘・育成及び事業化促進に向けてセキュリティ・キャンプの拡張及び未踏事業との連携を検討。
- ユーザー企業における登録セキスペの活用を促進（中小企業等とのマッチング実証事業、DX促進施策との連動等）するとともに、制度の見直しも検討。これらを通じて、**登録人数**（2024年４月現在、約2.3万人）**を2030年までに５万人まで増加を目指す**。
- 専門人材の育成に関する課題整理を行うとともに、基礎知識・スキル習得できるような環境整備に関する検討を実施。

本検討会における検討のスコープ・論点

- これまでの施策を通じて一定のアウトプットを生み出せていることから、ゼロベースで検討して新規施策に切り替えるのではなく、**既存施策の拡充や改善などをベースとしつつ**、前述の課題に対応することが基本となるのではないか。
- 産業サイバーセキュリティ研究会で示した方向性も踏まえ、本検討会においては、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**の方向性・論点について議論いただきたい。

※なお、「サイバーセキュリティ人材の育成・確保」に向けては、そもそもユーザー企業（中堅・中小企業等）によるサイバーセキュリティ対策投資を増やす（＝セキュリティ市場の需要に働きかける）ことも必要であり、また、人材育成に係るその他の施策（IPA中核人材育成プログラムの深化、プラス・セキュリティ人材育成・確保、官民での人材交流の促進等）の重要性も否定されるべきではない。あくまで、本検討会では、網羅的な政策体系を構築することを目的とするのではなく、他の検討体で議論されるべき具体的施策についてはそちらに譲りつつ、その上で政策効果や実現可能性の観点から比較的有効と考えられる上記３つの施策の方向性についてスコープを絞って議論することとしたい。

①　セキュリティ・キャンプの拡充

- 応募者が増加していることなども踏まえ、参加者の裾野拡大に向けたキャンプの在り方（内容・方式等）を検討すべきではないか。
- 官民での人材交流の促進や企業間の連携を促進する観点から、修了生コミュニティを通じた連携強化をすべきではないか。

②登録セキスペの活用及び制度の見直し

- 市場のミスマッチを解消する観点も踏まえつつ、マネジメントポスト等においてユーザー企業における登録セキスペの活用を促進するためのインセンティブを付与すべきではないか。
- ユーザー企業における活用促進及び活躍の場の拡大を促進するため、高額な維持コスト等を見直すべきではないか。
- そうした観点から、義務講習免除対象の拡充（類似資格の保持、セキュリティ業務従事経験等）や、義務講習体系の見直し（IPAによるオンライン・対面講習の在り方等）の検討が必要ではないか。

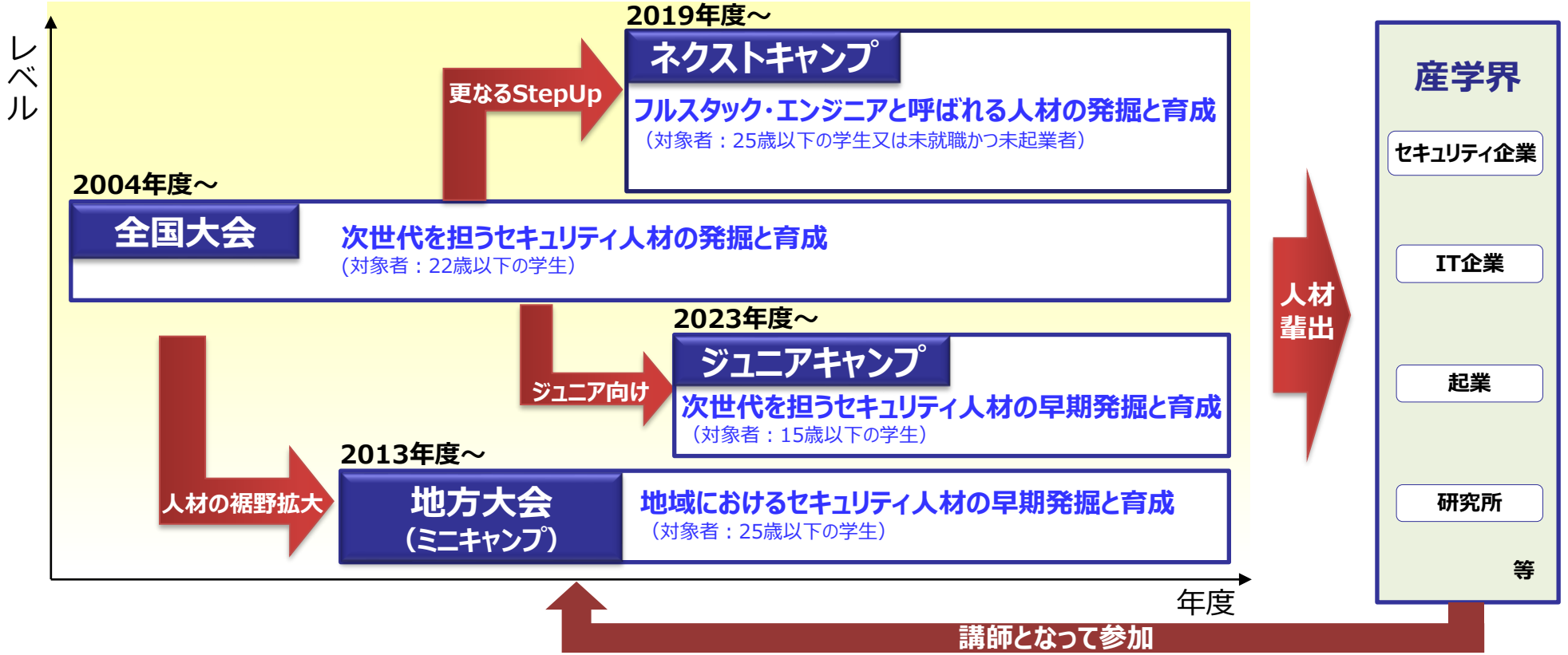
③中堅・中小企業等の内部でセキュリティ対策を推進する者の育成・確保に向けた施策の検討

- 「専門人材」のうち、実態や課題を踏まえ、特に不足している中堅・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・確保が肝要ではないか。
- こうした人材の育成を促すために、まずは、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役割について共通の認識を醸成することが必要ではないか。
- 当該役割を果たすために必要なスキル・知識及びその水準（深度）についての考え方を整理しつつ、当該考え方に沿った各種教育・訓練機会が民間事業者等により中堅・中小企業等に対して提供され、かつ、そうした教育・訓練機会が活用されるための、官民での連携・役割分担の在り方（民による市場原理の活用・官による市場の失敗の是正の在り方）を検討することが必要ではないか。

セキュリティ・キャンプの拡充

セキュリティ・キャンプ

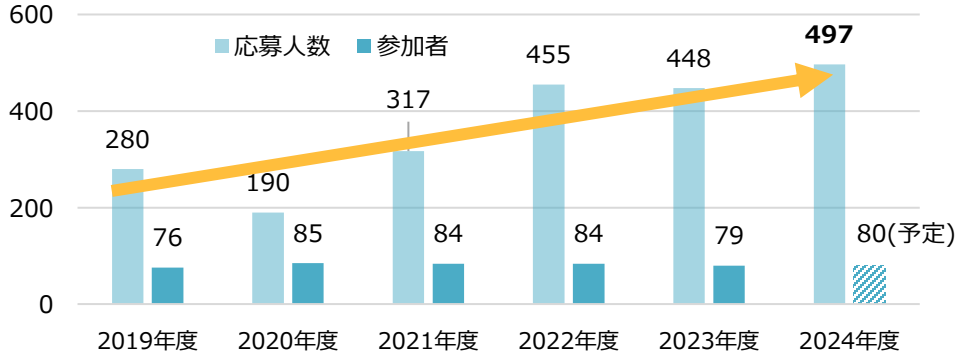
- 複雑かつ高度化しているサイバー攻撃に適切に対応するため、**若年層のセキュリティ人材発掘の裾野を拡大し、世界に通用するトップクラス人材を創出**することが必要。
- IPAとセキュリティ・キャンプ協議会は、選抜された22歳以下の学生・生徒を対象とした、次代を担う情報セキュリティ人材発掘・育成する「**セキュリティ・キャンプ全国大会**」を開催。**最新ノウハウも含めたセキュリティ技術を、倫理面と併せ、第一線の技術者から伝授**。2004年度の開始からこれまでに、累計で**1,152名**が修了。
- 2019年度からは、全国大会修了生の次のステップとして、選抜された25歳以下の学生・生徒等を対象とした、**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**43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。



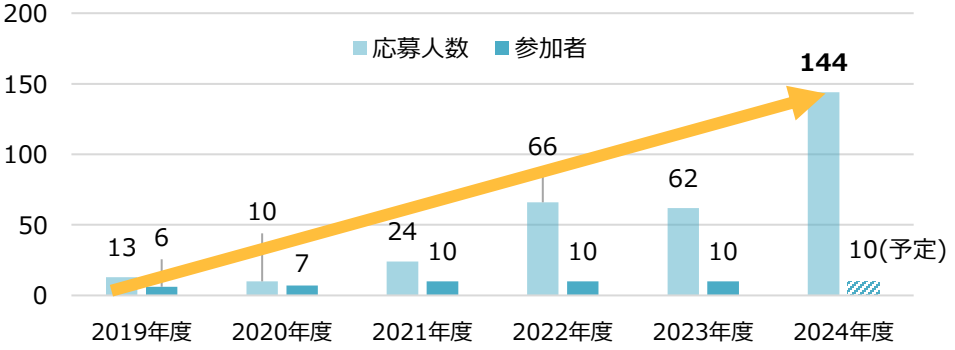
セキュリティ・キャンプの拡充

- 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や会場のキャパシティなどの関係から、参加者数（育成者数）の拡大ができていない。
- キャンプ修了生のフォローアップ調査は実施しており、一部のトップガンの存在は認められるものの、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、全数的な実態把握ができていない。また、産業界全体及び政府機関等におけるセキュリティ人材を確保する観点から、修了生の活用等も重要。
- これらのため、今後は、**参加者の裾野拡大を通じたトップガンの育成強化を図る**とともに、**ＩＰＡを中心とする事務局を整備し、修了生との関係強化を図ることが必要ではないか**。さらに、**キャンプ修了生が、セキュリティ産業の担い手（供給主体）として華々しく活躍できるような環境も整備する必要があるのではないか（例：起業促進等）**。

全国大会の参加状況



ネクストキャンプの参加状況



出典：IPA及びセキュリティ・キャンプ協議会からの情報をもとに経済産業省にて作成

修了生との関係構築

- （一社）セキュリティ・キャンプ協議会が主催するイベント等に修了生が登壇しているものの、参加者は限定的。
- 同団体において、「セキュリティ・キャンプ交友会」を整備しているが、会員制ではなく自主参加制のため、修了生の把握やフォローができていないといった課題がある。
- セキュリティ・キャンプの参加者は、次代の情報セキュリティ対策を担う優秀な人材であることから、修了生がノウハウを悪用しないためにも継続的につながることができる仕組みが必要。

今後の対応方針

- これまでキャンプに参加できなかった人材向けに、新たに第２セキュリティ・キャンプ（仮称）を実施し、セキュリティ・キャンプの育成数拡大を目指す。
- 修了生やIPAの講師が常時つながることができる会員制のコミュニティを整備。これにより、修了生同士のつながりを強化し、日々の業務の中で生じる課題の解決を促進するとともに、産業界及び政府機関等で修了生が活躍する際のチャネルとして活用していく。

登録セキスペの活用及び制度の見直し

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４月１日時点の登録者数は22,692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、さらに民間企業等が人材を活用できるよう登録簿を整備。**

◆ 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）登録セキスペ制度の全体像

1．登録セキスペになる資格を有する者になる段階

① 資格試験（登録セキスペ試験）

合格

・情報セキュリティスペシャリスト試験をベースに新設。
・受験手数料（７,５００円）
・全部又は一部免除制度。
→ 情報処理技術者試験との連携による一部免除制度は継続。
→ その他、大学等の教育課程修了者を一部免除については、9/29付けで下記を告示
CoE修了者：全部
大学、大学院、４年制専門学校：午前Ⅱ

② 資格試験合格と同等以上の能力を有する者

・国が指定するポストであって、当該ポストでの従事年数が一定期間を超える場合を想定。
→第一弾告示（警察・自衛隊）4/7施行
→第二弾告示（内閣官房・試験委員）9/29施行

③ 経過措置対象者

・以下の試験合格者が対象。
- 情報セキュリティスペシャリスト試験
- テクニカルエンジニア（情報セキュリティ）
・登録可能期限を設定（2年間、2018/8/19まで）

登録セキスペとなる資格を有する者

2．登録セキスペになる段階

登録申請

登録簿への登録

（情報処理安全確保支援士）登録セキスペ

・欠格事由に該当する場合は登録不可。
・登録手数料（10,700円）及び登録免許税（9,000円）の納付が必要。
・登録簿記載事項に変更が生じた場合、届出及び変更手数料（900円）の納付が必要。

義務違反の場合

登録取消し

又は

一定期間の名称使用停止

取消し後、2年間は再登録不可

3．登録セキスペとして活動、資格を維持する段階

登録情報の公開

・必須項目（登録番号等）を除き、公開する項目は本人の任意とする。

資格名称の独占使用

・情報処理安全確保支援士以外の者が名称を使用した場合は、30万円以下の罰金刑が課される。

義務遵守事項

（１）信用失墜行為の禁止

（２）秘密保持

・義務に違反した場合は、1年以下の懲役又は50万円以下の罰金刑が課される。

（３）講習受講

・更新期限内に、オンライン講習を毎年1回受講するとともに、実践講習を１回受講。

更新制

・３年ごとに登録の更新を受けなければ、期間の経過により、登録が失効。
・講習受講を条件に更新。

登録セキスペが目指すべき人材像

- 登録セキスペは、**スキル標準のレベル４に位置づけられる情報処理安全確保支援士試験**を通じて、サイバーセキュリティの専門家として必要とされる専門分野の知識・技能を有することを確認した人材である。
- デジタル技術を活用しDXを進めるためには、適切なセキュリティ対策とセットで推進する必要があり、そこで**サイバーセキュリティの専門家として必要とされている人材**は、**専門分野に関する知識・技能を有する**のみならず、**これを実践的に活用**でき、かつ、**様々なステークホルダーとコミュニケーションや技術的調整などを図ることができる人材**である。

スキル標準ＩＴＳＳによるレベル評価

	レベル評価
レベル７	• 社内外にまたがり、テクノロジやメソドロジ、ビジネス変革をリードするレベル • 市場への影響力がある先進的なサービスやプロダクトの創出をリードした経験と実績を持つ世界で通用するプレーヤ
レベル６	• 社内外にまたがり、テクノロジやメソドロジ、ビジネス変革をリードするレベル • 社内だけでなく市場から見ても、プロフェッショナルとして認められる経験と実績を持つ国内のハイエンドプレーヤ
レベル５	• 社内において、テクノロジやメソドロジ、ビジネス変革をリードするレベル • 社内で認められるハイエンドプレーヤ
レベル４	• 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３	• 要求された作業を全て独力で遂行するレベル • 専門を持つプロフェッショナルを目指し、必要となる応用的知識・技能を有する
レベル２	• 要求された作業について、上位者の指導の下、その一部を独力で遂行するレベル • プロフェッショナルに向けて必要となる基本的知識・技能を有する
レベル１	• 要求された作業について、上位者の指導を受けて遂行するレベル • プロフェッショナルに向けて必要となる基本的知識・技能を有する

登録セキスペが目指すべき人材像

企業等の内部に
１人は置かれるべき人材の到達点

企業等において、経営層、IT部門、事業部門、管理部門等との**コミュニケーション**や、IT／セキュリティベンダー企業との**技術的調整**を通じて、実施すべきセキュリティ対策を**必要十分な水準で**実現する人材。

又は

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

企業等の外部等から、セキュリティコンサル（中小企業等支援を含む）、脆弱性診断、セキュリティ監視、セキュリティ監査等の**専門的なセキュリティ対策を実施**することができる人材。

登録セキスペ講習制度の概要

- 登録セキスペは、講習の受講が法律により義務付けられている。

  ①**オンライン講習**（２万円／年）：試験合格時の知識・技能の維持、倫理の醸成など、登録セキスペが共通的に習得すべき内容の講習（毎年１回）【ＩＰＡが実施】

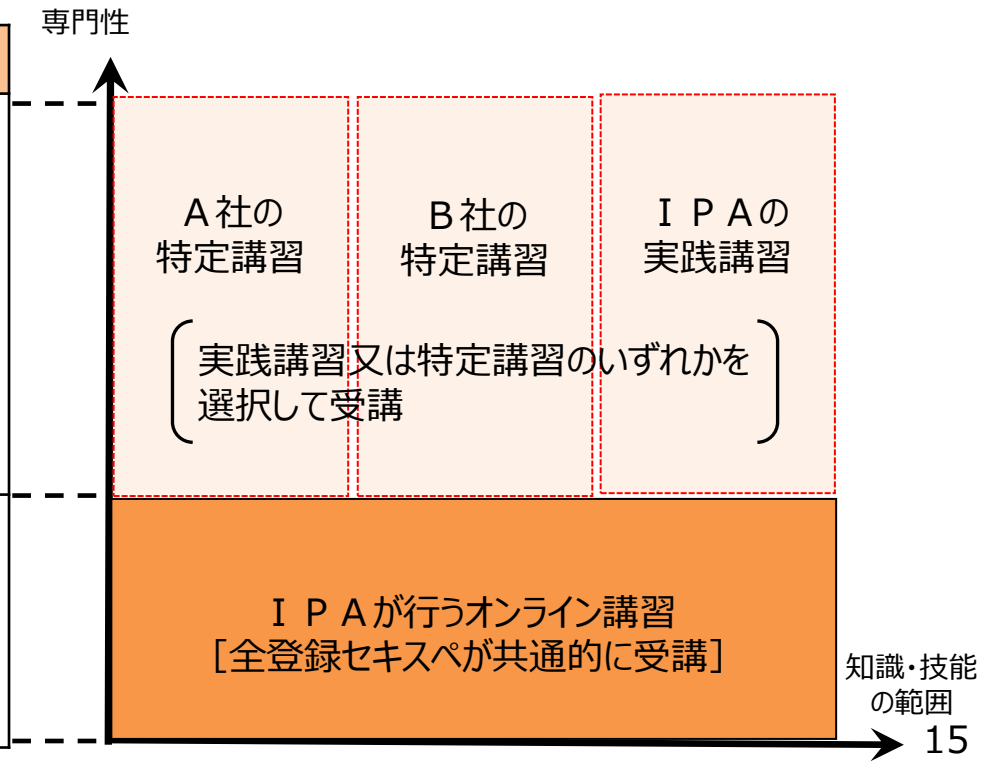
  ②**実践講習**（８万円）**又は特定講習**（民間事業者等が価格を設定）：登録セキスペの業務に必要となるサイバーセキュリティに関する専門的知識・技能の実践的な活用に関する講習（３年間に１回）【ＩＰＡ又は民間事業者等が実施】

- 資格更新のために、**３年間で少なくとも10万円以上の費用がかかる**ため、特に個人で支出するには大きな負担となっている。

＜講習制度＞

実施主体	手段・内容
ＩＰＡ 又は 民間事業者等 ＜②実践講習又は特定講習＞	手法：実習、実技、演習又は発表を伴う講習 期間：３年に１回、６時間以上 （半分以上の内容を実践的な方法で実施） 登録セキスペの業務に必要となるサイバーセキュリティに関する専門的知識・技能の実践的な活用に関する講習として、ＩＴＳＳ＋（セキュリティ領域）のうち、セキュリティに区分される分野から選択
ＩＰＡ ＜①オンライン講習＞	手法：オンライン講習 期間：毎年１回・６時間 • 最新の知識・技能のインプット • 倫理の醸成

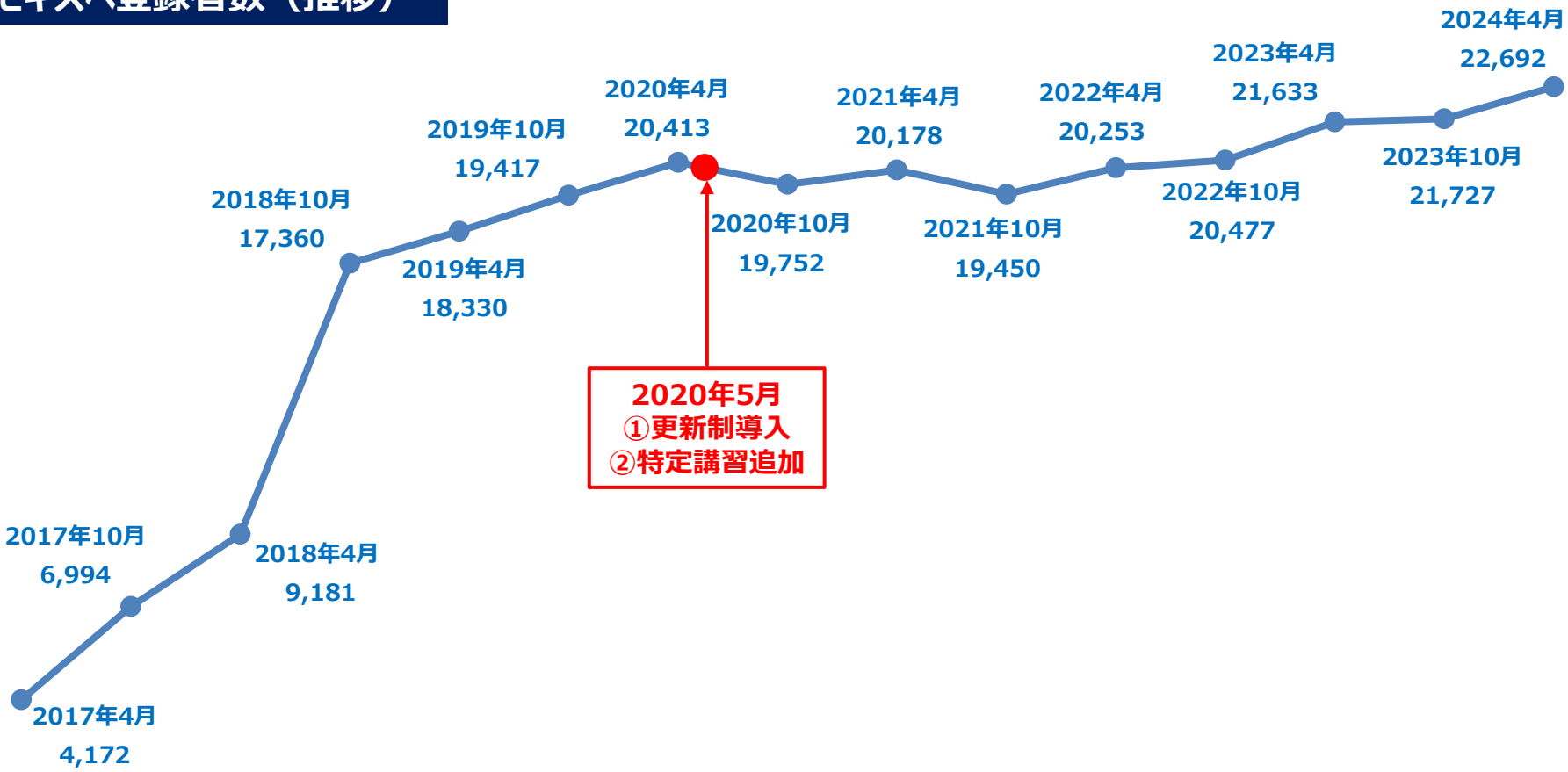
＜講習イメージ＞



登録セキスペ登録者数について

- 2016年に資格創設後、登録者は2019年以降横ばいで推移。
- 情報処理安全確保支援士試験合格者のうち、**<u>６割以上は未登録</u>**となっている。

登録セキスペ登録者数（推移）

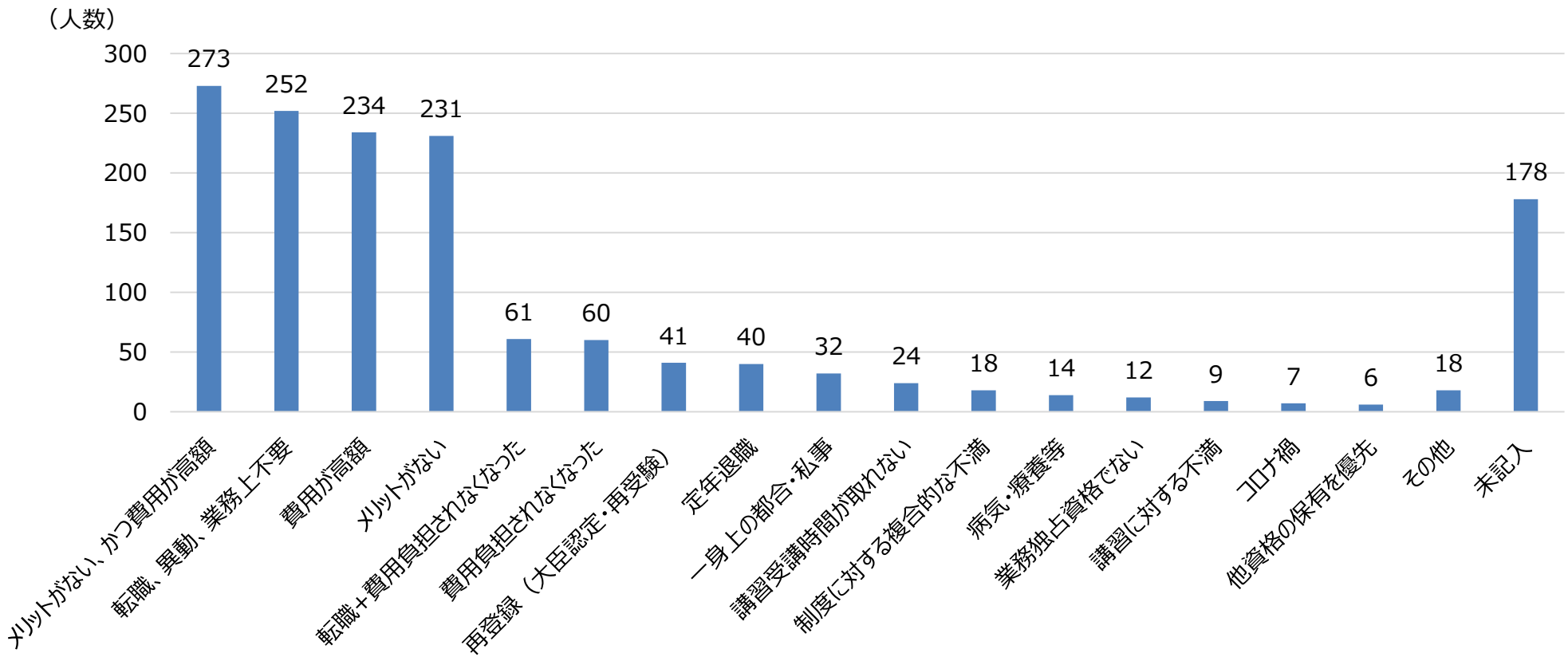


出典：https://www.ipa.go.jp/jinzai/riss/reports/data/index.html

登録セキスペの消除理由について

- 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**というコメントが目立っている。
- 登録セキスペの登録者増加のため、**活躍の場を増やす**ことに加え、**更新の費用負担の軽減**が必要ではないか。

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

登録セキスペの普及促進について

第10回産業サイバーセキュリティ研究会
ワーキンググループ２　資料３より抜粋・加工

- 情報処理安全確保支援士（登録セキスペ）は、**スキル標準のレベル４（※）に位置づけられる情報処理安全確保支援士試験に合格したものが登録することができる国家資格**。高度なセキュリティ知識を活かした様々なポストでの活躍が期待されており、**人材不足の解消の観点から、登録セキスペの活用促進、登録者の増加が重要**。

（※）独力で業務を遂行することおよび後進人材の育成が可能なレベル

- このため、マネジメントポスト等において**ユーザー企業における登録セキスペの活用を促進する**とともに、中小企業等とのマッチング実証事業、DX促進施策との連動等と通じて、更なる**社内外での活用を検討**。
- 併せて、高額な登録維持コストが課題と指摘されていることから、この維持コスト削減のための方策も検討。これらを通じて、登録人数（2024年４月現在、約2.3万人）を2030年までに５万人まで増加を目指す。

登録セキスペへの期待

- 企業等において、経営層、担当者（IT部門、事業部門、管理部門等）をつなぐようなCISO的な活躍
- IT／セキュリティベンダー企業との技術的調整を通じて、実施すべきセキュリティ対策を実現するマネジメント
- 中小企業等のコンサルとして、脆弱性診断、セキュリティ監視、セキュリティ監査等の専門的なセキュリティ対策の支援

現状の課題

- ベンダー側に偏っており、ユーザー企業での活用が進んでいない。
- 専業化がされておらず、活躍の場が限らている。
- 資格維持のためのコストが大きい（3年間で10万円以上必要）との意見あり。試験合格者の多くは未登録。

今後の方向性

（ユーザー企業での活用促進）

- デジタルガバナンス・コード2.0等の指針において、登録セキスペの活用の明記を検討
- 補助金等において、登録セキスペ配置あるいは活用の要件化及び加点措置の導入を検討
- 重要インフラ等の特定業種や企業規模に応じたセキュリティ対策を実施するため、登録セキスペの必置化を検討

（活躍の場の拡大）

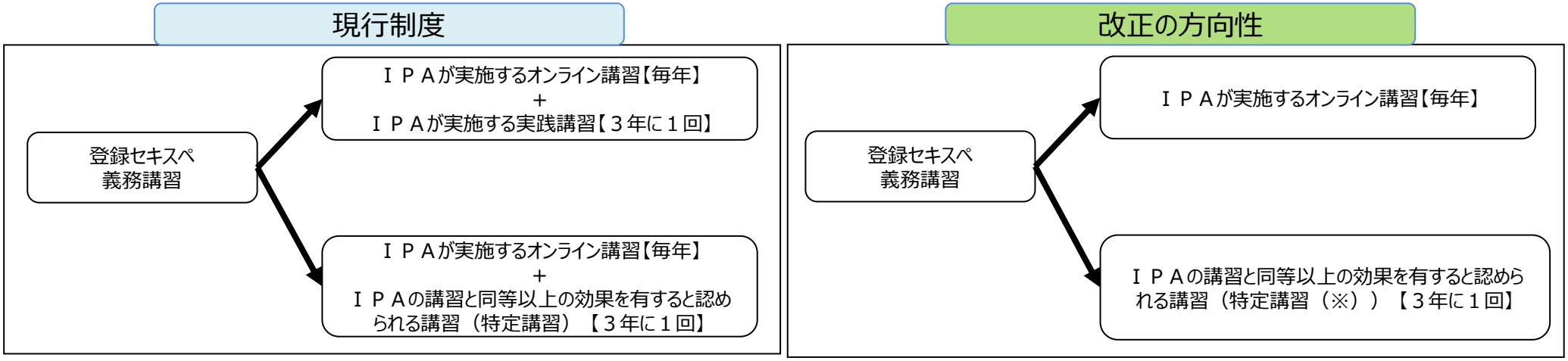
- 支援機関等と連携した中小企業等のマッチング実証事業を実施、登録セキスペのアクティブリストの整備
- セキュリティ監査での活用促進
- 政府機関・地方公共団体での活用促進

（維持コスト低減）

- 維持コスト削減のための方策（講習制度及び講習内容の見直し等）の検討

登録セキスペ義務講習の見直しについて①

- 情報処理の促進に関する法律（以下「情促法」という。）において、登録セキスペは「機構の行うサイバーセキュリティに関する講習（以下「ＩＰＡ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（以下「特定講習」という。）」を受けなければならないとされている。ＩＰＡ講習については、登録事務規程において、「オンライン講習」及び「実践講習」の両方を実施することと規定されている。
- 登録セキスペ取得者の資格維持のための費用負担を軽減する観点から、**ＩＰＡ講習については、「オンライン講習」（２万円／年×３回）に一本化する方向とするのはどうか**。
- 一方、民間事業者等が提供する特定講習については、分野を絞ったよりハイレベルの講習であり、より専門的な知識・スキルの習得を目指す登録セキスペの受け皿となることから、存置することとしたい。
- つまりは、**登録セキスペは、①ＩＰＡが実施するオンライン講習を毎年受講する、あるいは、②民間事業者等が実施する特定講習（※）を３年に１回受講することで更新の要件を満たすこととするのはどうか**。



（※） 必要に応じて既存のＩＰＡが行う実践講習（８万円／３年×１回）も含む

登録セキスペ義務講習の見直しについて②

- ＩＰＡ講習について、「オンライン講習」に一本化した場合でも、情促法が定める講習の水準は維持する必要がある。つまりは、**ＩＰＡが実施する「オンライン講習」と民間事業者等が実施する「特定講習」が同等の水準である必要がある**。
- ここで、「特定講習」の基準について、情促法施行規則第三十四条第２項第二号の「実習、実技、演習又は発表その他実践的な方法」により行うことと規定されている。
- ついては、**ＩＰＡが実施する「オンライン講習」において、「実習、実技、演習又は発表その他実践的な方法」を組み込むことで、民間事業者等が実施する特定講習との同等性を担保できないか**。

○情報処理の促進に関する法律施行規則（平成二十八年経済産業省令第百二号）
（講習）
第三十四条　機構の講習又は特定講習を受講する情報処理安全確保支援士は、法第二十三条第二項において準用する法第十一条により定められた登録事務規程に従わなければならない。
２　特定講習は、次の各号のいずれにも該当する講習として経済産業大臣が定めるものとする。
一　第二条第一項第二号及び第三号に掲げる支援士試験の科目（以下この項において単に「科目」という。）に係る内容を行うものとし、特定講習の総時間数は、六時間以上とすること。
二　**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こと**。
三　修得することが求められる知識又は技能の修得がなされていることを確認する内容を含むこと。
四　講師は、科目について効果的に指導できる知識、技能及び経験を有する者であること。
五　実習、実技、演習又は発表その他実践的な方法による特定講習にあっては、前号の講師のほか、特定講習の実施に必要な人数の講師の補助者を配置すること。
六　科目に応じた適切な内容の教材を用いること。
七　特定講習を実施する者の職員、特定講習の実施の方法その他の事項についての特定講習の実施に関する計画が特定講習の適正かつ確実な実施のために適切なものであること。
八　特定講習を実施する者が前号の当該講習の実施に関する計画の適正かつ確実な実施に必要な経理的及び技術的な基礎を有すること。
九　特定講習を実施する者が当該講習の実施状況について、経済産業大臣（機構が登録事務を行う場合にあっては、機構。）に報告する体制を有すること。
十　特定講習を受ける者に、当該講習を実施する者、その関係者が雇用する者又は当該講習を実施する者若しくはその関係者と密接な関係を有する者以外の者を含むこととされていること。

登録セキスペ義務講習の免除について

- 現行制度において、登録セキスペは講習の受講義務があるが、登録セキスペの業務を行うのに十分な能力を有するとして行政機関の長（※）が認める者であり、経済産業大臣が認定した者及びＩＰＡが行う実践講習の講師については、登録事務規程おいて、みなし受講申請書を申請し、機構の理事長により承認されることで、講習受講が免除されると規定されている。

（※）警察庁、防衛省、内閣官房、独立行政法人情報処理推進機構が含まれる。

- みなし受講を認める趣旨としては、現にサイバーセキュリティに関する業務に従事しており、義務講習を受講しなくとも、登録セキスペの資格を維持するに足る能力を有するということであり、つまりは、**資格維持の妥当性を客観的に判断することができることが肝要である**。

- 登録セキスペの中で、**セキュリティに関する実務要件を課している他の資格（CISSP等）も保有する者については、当該資格維持の年数をもって、登録セキスペの資格を維持するに足る能力を有する（資格更新のための義務講習を受講することと同等の実務を現に経験している）と客観的に判断することは可能ではないか**。

○情報処理の促進に関する法律施行規則第一条第一号に規定する経済産業大臣の認定について定める告示（経済産業省告示第九十四号）

第一条　情報処理の促進に関する法律施行規則（平成二十八年経済産業省令第百二号。以下「規則」という。）第一条第一号に規定する経済産業大臣の認 定は、次の各号に掲げる要件のいずれかに該当するものとする。ただし、申請日において当該要件に係る事務に従事しなくなった日の翌日から起算して三年を経過している場合にあっては、この限りでない。

一　**警察庁**（警察法（昭和二十九年法律第百六十二号）第十五条に規定する警察庁をいう。）又は都道府県警察（警察法第三十六条第一項に規定する都道府県警察をいう。）のうちいずれか一の機関において、犯罪の取締りのための電子情報処理組織及び電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。）の解析その他情報技術の解析に関する事務に従事した期間が通算して二年以上である者であって、情報処理の促進に関する法律（昭和四十五年法律第九十号。以下「法」という。）第六条に規定する業務を行うのに十分な能力を有すると警察庁長官が認める者であること。

二　**自衛隊**（自衛隊法（昭和二十九年法律第百六十五号）第二条第一項に規定する自衛隊をいう。）において、サイバーセキュリティに関する知識及び技能を要する事務に従事した期間が通算して二年以上である者であって、法第六条に規定する業務を行うのに十分な能力を有すると防衛大臣が認める者であること。

三　**内閣官房**（内閣法（昭和二十二年法律第五号）第十二条に規定する内閣官房をいう。）において、内閣の重要施策に関する情報の収集調査に関する事務であって、サイバーセキュリティに関する知識及び技能を要する事務に従事した期間が通算して二年以上である者であって、法第六条に規定する業務を行うのに十分な能力を有すると内閣情報官が認める者であること。

四　**独立行政法人情報処理推進機構**（以下、この号及び第二条において「機構」という。）から委嘱を受け、法第十条に規定する支援士試験事務（支援士試験の問題を作成するものに限る。）又はサイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律（平成二十八年法第三十一号）の施行前の情報処理の促進に関する法律第七条第二項に規定する情報処理技術者試験の実施に関する事務（情報セキュリティスペシャリスト試験の問題を作成するものに限る。）に従事した期間が通算して二年以上である者であって、法第六条に規定する業務を行うのに十分な能力を有すると機構の理事長が認める者であること。

（参考）他資格との比較（登録セキスペ・CISSP）

	登録セキスペ	CISSP（セキュリティプロフェッショナル認定資格制度）
オーナー	独立行政法人 情報処理推進機構	(ISC)² Japan
概要	サイバーセキュリティに関する専門的な知識・技能を活用して企業や組織における安全な情報システムの企画・設計・開発・運用を支援し、また、サイバーセキュリティ対策の調査・分析・評価を行い、その結果に基づき必要な指導・助言を行う者を対象とした資格。	情報セキュリティにおける理論やメカニズムを理解するだけでなく、その知識を体系的かつ構造的に整理し、状況に応じた適切な判断を行うための、合理的かつ実践的な「知識」と「理解度」が求められる情報セキュリティ・プロフェッショナル資格。
知識・能力	以下の知識・実践能力が要求される。 1. 情報システム及び情報システム基盤の脅威分析に関する知識をもち、情報セキュリティ要件を抽出できる。 2. 情報セキュリティの動向・事例、及びセキュリティ対策に関する知識をもち、セキュリティ対策を対象システムに適用するとともに、その効果を評価できる。 3. 情報セキュリティマネジメントシステム、情報セキュリティリスクアセスメント及びリスク対応に関する知識をもち、情報セキュリティマネジメントについて指導・助言できる。 4. ネットワーク、データベースに関する知識をもち、暗号、認証、フィルタリング、ロギングなどの要素技術を適用できる。 5. システム開発、品質管理などに関する知識をもち、それらの業務について、セキュリティの観点から指導・助言できる。 6. 情報セキュリティ方針及び情報セキュリティ諸規程の策定、内部不正の防止に関する知識をもち、情報セキュリティに関する従業員の教育・訓練などについて指導・助言できる。 7. 情報セキュリティ関連の法的要求事項、情報セキュリティインシデント発生時の証拠の収集及び分析、情報セキュリティ監査に関する知識をもち、それらに関連する業務を他の専門家と協力しながら遂行できる。	セキュリティ共通知識分野（CBK）の8分野への理解が求められる。 【CBKの8分野】 1. セキュリティとリスクマネジメント 2. 資産のセキュリティ 3. セキュリティアーキテクチャとエンジニアリング 4. 通信とネットワークのセキュリティ 5. アイデンティティおよびアクセス管理 6. セキュリティの評価とテスト 7. セキュリティの運用 8. ソフトウェア開発セキュリティ 資格取得のためには業務経験も必要であり、試験合格後の認定登録手続きで業務経験を明記した職務経歴書とエンドースメント(推薦状)を提出し、それを証明する必要がある。
国内人数	22,692人（2024年4月時点）	3,699人（2022年7月時点）
更新頻度	3年（3年ごとに登録更新を行うことが必要）	3年（3年毎の認定継続要件をパスすることが必要）
取得費用	• 初期費用27,200円（受験手数料7,500円＋登録手数料10,700円＋登録免許税9,000円） • オンライン講習20,000円（1年に1度） • 実践講習80,000円（3年に1度）	• 受験費用749米国ドル*1 • 年会費135米国ドル*2
義務	以下の3点の義務が課せられている。 1. 信用失墜行為の禁止　2. 秘密保持　3. 講習受講	特になし
合格水準	60点（100点中）以上	700点（1000点）以上
合格率	19.7%（令和５年度春期試験）	非公表
認定要件	試験合格 欠格事由に該当しないことへの誓約書を提出	試験合格 ISC2認定資格保有者からの推薦*3 ISC2倫理規約への合意*3 5年以上の業務経験（CISSP CBK 8ドメインのうち2ドメインに関連）*3 ※受験時は不要、認定登録時に必要(実務経験を満たすまで準会員、最大6年間)*4 ※最大1年間は免除可能（IT関連分野の大学卒業学位、または資格取得）*3

出典：*1. ISC2 CISSP 受験費用の更新 https://japan.isc2.org/about_faq_examprice.html
*2. ISC2 年会費 https://japan.isc2.org/member_annualfee.html
*3. ISC2 CISSP 認定要件 https://japan.isc2.org/cissp_outline.html
*4. ISC2 準会員（アソシエイト）とは https://japan.isc2.org/isc-2-new.html

（参考）他資格との比較（CISA･CISM）

	CISA（公認情報システム監査人）	CISM（公認情報セキュリティマネージャー）
オーナー	ISACA	
概要	情報システムの監査および、セキュリティ、コントロールに関する高度な知識、技能と経験を有するプロフェッショナルとして認定する国際資格。*1	情報セキュリティマネジメントの知識と経験を認定する国際資格。*4 以下の観点を考慮して資格が創設されている。*4 ・情報セキュリティマネージャーに特化した資格として設計 ・情報セキュリティマネージャーの実際の業務分析を元にした、基準と試験問題を開発 ・情報セキュリティマネジメントの実務経験を資格認定の前提とする
知識・能力	以下の5つのドメインにおける知識が要求される。*2 ドメイン1：情報システム監査のプロセス ドメイン2：ITガバナンスとITマネジメント ドメイン3：情報システムの調達、開発、導入 ドメイン4：情報システムの運用とビジネスレジリエンス ドメイン5：情報資産の保護	以下の4つのドメインにおける知識が要求される。*4 ドメイン1：情報セキュリティガバナンス ドメイン2：情報セキュリティリスクの管理 ドメイン3：情報セキュリティプログラムの開発と管理 ドメイン4：情報セキュリティのインシデントの管理
国内人数	3,601人（2024年2月、CISA保有者のうちISACA東京支部の人数）*3 ※世界人数：151,000人以上*3	779人（2024年2月、CISA保有者のうちISACA東京支部の人数）*3 ※世界人数：48,000人以上*3
更新頻度	3年（3年毎の認定継続要件をパスすることが必要）	
取得費用	・受験費用： 760米国ドル（非会員）、575米国ドル（ISACA会員）*2 ・申請手数料： 50米国ドル*2 ・年間維持費： 85米国ドル（非会員）、45米国ドル（ISACA会員）*5 ※毎年1月15日までに支払い*6	
義務	ISACA職業倫理規定の遵守*6	
合格水準	450点（800点中）以上*2	
合格率	非公表	非公表
認定要件	試験合格 ISACA規定類への合意（職業倫理規則等）*7 5年以上の実務経験（情報システム監査、コントロール、またはセキュリティ）*7 ※受験時は不要、認定登録時に必要(試験合格から5年以内に申請)*7 ※申請前10年以内の実務経験であること*7 ※最大3年間代替・免除可能（情報システムの開発経験、学士　等）*7	試験合格 ISACA規定類への合意（職業倫理規則等）*4 5年以上の実務経験（4つのCISMジョブ・プラクティスドメインのうち3つのドメイン）*4 ※受験時は不要、認定登録時に必要(試験合格から5年以内に申請)*4 ※申請前10年以内の実務経験であること*8 ※最大2年間免除可能（情報システムのマネジメント経験、学士　等）*8

出典：
*1. ISACA東京支部 CISA https://www.isaca.gr.jp/cisa/index.html
*2. ISACA Exam Candidate Guide https://www.isaca.org/credentialing/exam-candidate-guides
*3. ISACA東京支部 CISM資格のご紹介 https://www.isaca.gr.jp/cism/img/2024_cism.pdf
*4. ISACA東京支部 CISM https://www.isaca.gr.jp/cism/index.html
*5. ISACA東京支部 FAQ https://www.isacar.jp/faq/index.html
*6. ISACA CISA CPE Policy https://www.isaca.org/credentialing/how-to-earn-cpe#cpe-policy
*7. ISACA東京支部 CISA認定申請について https://www.isaca.gr.jp/cisa/200906gokakusiryo/CISA_ninteishinsei.pdf
*8. ISACA CISM APPLICATION FORMS https://www.isaca.org/credentialing/cism/get-cism-certified#download-pdfs

（参考）他資格との比較（CSA）

	CSA（公認システム監査人）
オーナー	日本システム監査人協会（SAAJ）
概要	システム監査技術者試験合格者もしくは同等の能力を有し、且つ一定の実務経験を重ねた者を認定する。*1
知識・能力	高度IT人材として確立した専門分野をもち、高い倫理観の下、監査対象から独立かつ客観的な立場で、情報システムや組込みシステムを総合的に検証・評価して、監査報告の利用者に情報システムのガバナンス、マネジメント、コントロールの適切性などに対する保証を与える、又は改善のための助言を行う者*2
国内人数	353人（2023年度末時点での累計）*3
更新頻度	**2年（継続教育の認定要件を満たすことが必要）**_*4_
取得費用	システム監査技術者試験 受験費用：7,500円*5 認定申請手数料：33,000円（非会員）、22,000円（SAAJ会員）*6 認定登録手数料：55,000円（非会員）、33,000円（SAAJ会員）*6 維持費（2年毎の更新手数料）：33,000円（非会員）、22,000円（SAAJ会員）*7
義務	宣誓書の提出（システム監査人倫理規定の遵守、継続教育について）
合格水準	午前Ⅰ・午前Ⅱ・午後Ⅰ：60点（100点中）以上　　午後Ⅱ：ランクA（論述式）*2
合格率	16.4%（2023年度秋 システム監査技術者試験 合格率）*8
認定要件	システム監査技術者試験合格（特別認定制度あり）*6 2年以上の監査実務経験*6 ※SAAJが開催するシステム監査セミナー等も実務経験とみなすことができる*6 宣誓書の提出*6 小論文の提出（監査実務経験に基づいた内容、1800字以上2200字以内）*6 面接試験（監査実務経歴書に関する質問等、30分程度）*6

出典：*1. SAAJ 公認システム監査人のご案内 https://www.saaj.or.jp/csa/pdf/CSAASApanf20220510.pdf
*2. IPA 試験要綱 https://www.ipa.go.jp/shiken/syllabus/nq6ept00000014lt-att/youkou_ver5_3.pdf
*3. SAAJ 第23期総会資料 https://www.saaj.or.jp/soukai/pdf/SAAJ2024SOKAI20240216.pdf
*4. SAAJ 継続教育要項 https://www.saaj.or.jp/csa/2nen_koushin.html
*5. IPA 試験情報 https://www.ipa.go.jp/shiken/mousikomi/schedule.html
*6. SAAJ 募集要項 https://www.saaj.or.jp/csa/csaboshu/620301CSAASAbosyuyoko.pdf
*7. SAAJ 認定資格更新申請手続 https://www.saaj.or.jp/csa/pdf/620504koshin20231130.pdf
*8. IPA 統計資料（令和6年4月） https://www.ipa.go.jp/shiken/reports/nq6ept000000i5c9-att/toukei_r06h_oubo.pdf

（参考）他資格との比較（CISSP）

- 資格を更新するためには、**3年間で120CPEクレジットが必要**（毎年40CPEクレジットの取得を推奨）。
  - 30CPEはグループBからも取得可能、それ以外はグループAから取得。
  - 1つのアクティビティで最大40CPEまで登録可能。

カテゴリ	内容	付与数		グループ
ISC2イベント等への参加	ISC2公式トレーニング、ISC2 Webinar など	1時間ごとに	1CPE	A
教育	トレーニングコースやセミナーの受講、大学院の授業　など	1時間ごとに	1CPE	CISSPのドメインに関連：A その他の専門領域：B
	書籍の購読	1冊ごとに	最大5CPE	CISSPのドメインに関連：A その他の専門領域：B
	雑誌の有料購読	1冊ごとに	最大5CPE	CISSPのドメインに関連：A その他の専門領域：B
	ホワイトペーパーの購読	1つごとに	1CPE	CISSPのドメインに関連：A その他の専門領域：B
専門的な 活動による貢献	書籍の執筆	1冊ごとに	単著：40CPE 共著：20CPE 編集：10CPE	A
	記事の執筆	1つごとに	単著：20CPE 共著：10CPE 編集：5CPE	A
	専門的なブログ・ホワイトペーパーの執筆	1つごとに	単著：10CPE 共著：5CPE 編集：2CPE	A
	Webinar、ポッドキャスト、プレゼンテーション、トレーニングの準備	1つごとに	1日コース：2CPE 2日コース：5CPE 5～7日コース：10CPE 12週以上のコース：20CPE	A
	専門家としてのパネルディスカッション参加 ※雇用主・顧客とは異なるグループに、CISSPドメインに関連するサービスを無償提供	1時間ごとに	1CPE	A
独自性の高い業務活動	業務として行った、独自性の高いプロジェクト・課題・活動・演習 ※通常業務とは異なる内容であること	1つごとに	最大10CPE	A
CISSPドメイン以外の 専門能力の開発	トレーニングやセミナー受講、プレゼンテーション・講義の準備　など	1時間ごとに	1CPE	B

出典：　ISC2 CPEクレジット https://japan.isc2.org/member_cpecredit.html
ISC2 CPEハンドブック　https://japan.isc2.org/files/MEM-CPE-Handbook-Digital-Japanese%20(1)%20(1).pdf

ユーザー企業での活用促進（投資促進施策における登録セキスペの配置等）

- 登録セキスペ登録者は、現状ベンダー側に偏っており、ユーザー企業での活用を進めるためにインセンティブを付与する必要がある。
- 例えば、政府の補助金において要件を課すことが考えられる。直近の投資促進施策においても、既に補助金の要件に、登録セキスペの配置又は活用を明記。引き続き、**経済産業省の補助金施策の要件や各種指針等との紐付けや、重要インフラ等の特定業種における必置化等を検討し、その実効性を強化していく**。

投資促進施策における登録セキスペの要件化

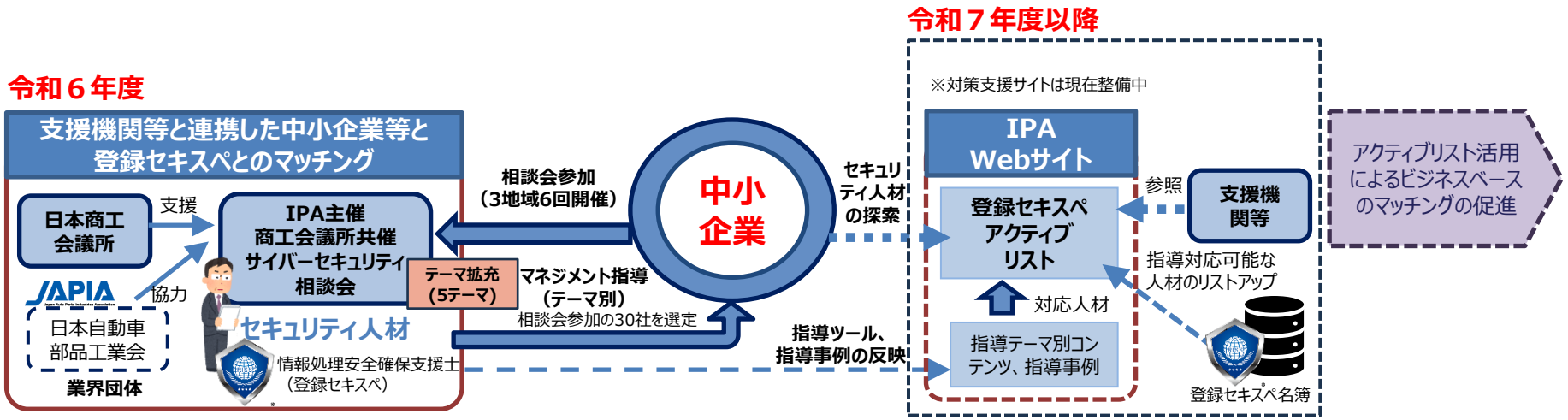
- 令和５年度補正グローバルサウス未来志向型共創等事業費補助金におけるサイバーセキュリティ要件（抜粋）
  - ２．補助対象事業が工場に係るものについて、サイバーセキュリティの対処（※）が適当か
    ※サイバーセキュリティの対処とは、「**サイバーセキュリティの確保に関する運用を的確に行うに足りる知識及び技能を有する者として、情報処理安全確保支援士又はこれと同等以上の知識及び技能を有すると認められる者を配置又は活用していること**及び①サイバーセキュリティの確保のための管理体制について、第三者認証（ISO 27001）を取得し、維持していること、もしくは②定期的に、サイバーセキュリティに関する外部監査等（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】

活躍の場の拡大（登録セキスペと中小企業等とのマッチング事業）

- 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**ことが挙げられている。
- そこで、令和６年度は、支援機関等と連携した中小企業等とセキュリティ人材（登録セキスペ）とのマッチングを促す場を構築し、**登録セキスペの社外での活用検討**と、中小企業がセキュリティ人材を探索しやすくするための、**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）整備のための実証**を行う。
- 将来的には、**マネジメント指導メニューの拡充やリストが常にアクティブであるための仕組みを検討**しつつ、**全国版アクティブリストを整備**し、**支援機関等と連携しながらビジネスベースのマッチングを促進**していく。

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**する。
- 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**を実施する。
- 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）**について検討する。
  - 将来的に**IPAのWebサイト**に、指導テーマ別コンテンツ・指導事例、登録セキスペのアクティブリストを掲載し、中小企業および支援機関からの**セキュリティ人材（登録セキスペ）を探索しやすい環境と活用促進**を目指す。



（参考）登録セキスペ制度の普及に向けた施策

目的	目標	対象	施策
1.試験応募者を増やす	登録セキスペの存在と価値を伝え、応募者数の増加を図る。	サイバーセキュリティに関心のある個人・団体・企業	**●試験の広報活動と連携した他団体セミナーでの講演など** ●応用情報技術者試験合格者向けチラシ配布
2.登録者を増やす	登録有資格者の登録率を向上させる。	試験合格して未登録の方、経営層 等	**●登録セキスペ制度説明会（合格者向け）** **（情報処理安全確保支援士試験合格発表に合わせて年2回開催）** ●経営者・企業担当者向けセミナー開催
3.登録セキスペを減らさない	登録セキスペの更新率を向上させる。	登録セキスペ	**●資格維持に必要な講習受講、更新等の情報配信** **（メール、電話などによる案内）** **●更新の案内はがきの発送** **（毎年6月、12月頃に更新対象者へ発送）**
4.登録セキスペの満足度向上	登録セキスペの満足度向上、活躍の場の認知を図る。	登録セキスペ	**●情報処理安全確保支援士ポータルサイトからの情報配信** **●更新申請・各種変更手続のオンライン化** **●徽章（バッジ）貸与** ●登録セキスペの活用に関する制度の周知 （中小企業の情報セキュリティマネジメント指導業務）
5.登録セキスペの活用（認知度向上）	登録セキスペの存在と価値を伝え、活用を促進することで、登録セキスペの社会的価値を醸成する。	主に中小企業のCEO・CIO・CSOなど情報セキュリティの責任者	**●登録セキスペインタビュー、活用企業インタビューの公開** **●制度案内パンフレットの配布** **●イベント出展、セミナー等での講演** ●一般社団法人情報処理安全確保支援士会等主催イベントでの講演

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

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・確保に向けた課題

- デジタル技術を活用しDXを進める企業、デジタル環境を介して外部とつながる企業等は、企業の規模を問わず、セキュリティ対策が必要であり、専門性を有する外部ベンダー等を活用する場合であっても、組織におけるセキュリティ対策の実効性、適切性を確保するために**社内で最低限の知識を持ったセキュリティ担当者**の育成・確保が必要。
- 重要インフラ企業や大企業においてはそうした人材の確保は進められている一方、特に**中堅・中小企業等においてはこのような内部人材が不足**しているとの声は依然としてみられる。
- 中堅・中小企業においては、セキュリティ対策の必要性に対する理解やコスト負担といった課題を乗り越えたとしても、こうした内部人材を育成・確保するために、**どのようなスキル・知識をどの程度まで獲得することが必要なのか不明確**であり、かつ、そうした**スキル・知識を獲得できる訓練機会を探索することが容易ではない**状況であり、人材の確保が困難。
- そこで、こうした課題に対応するための方策を検討したい。

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。

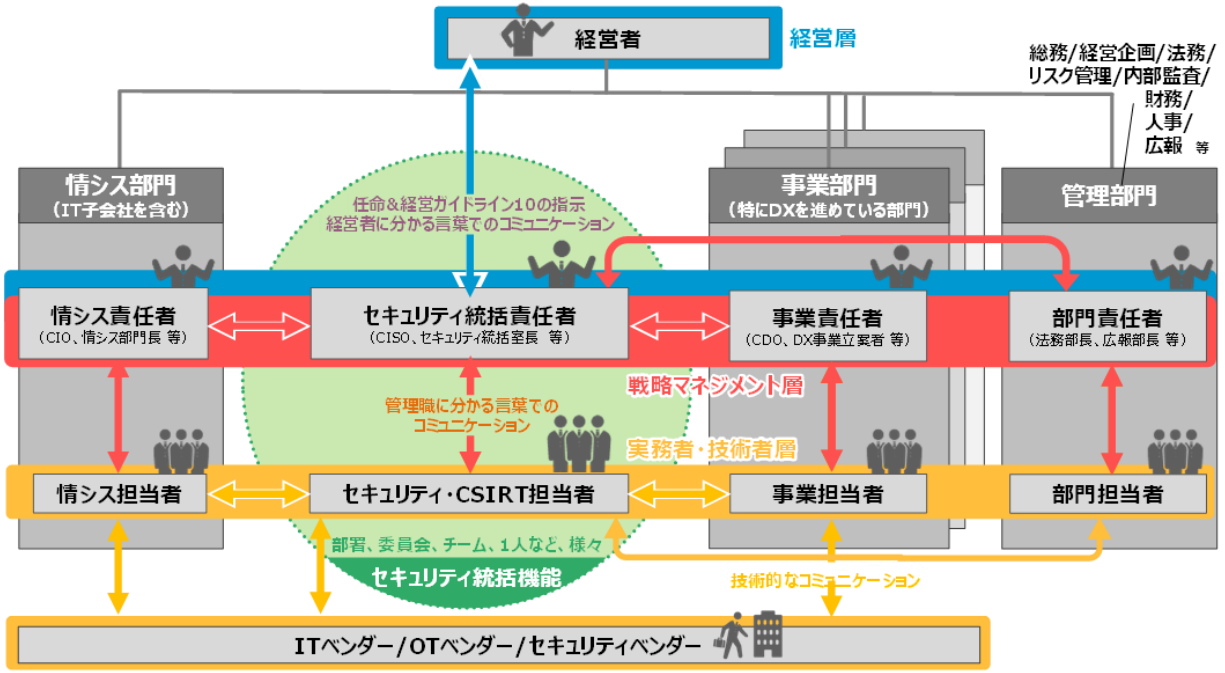
既存の関連施策①：サイバーセキュリティ体制構築・人材確保の手引き

- 「サイバーセキュリティ経営ガイドライン 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」においては、全社的なサイバーセキュリティ体制の構築のために、**CISO等の経営層を補佐する「セキュリティ統括機能」を設置することの有効性**について言及するとともに、**「セキュリティ統括機能」が担うタスク**を示している。

※サイバーセキュリティ対策を主たる目的とする業務や役割としては、「セキュリティ経営（CISO）」、「セキュリティ統括」、「セキュリティ監査」、「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」等が挙げられるが、**「セキュリティ統括」分野については**、企業におけるリスクマネジメント活動の一部として、**対策を推進する立場の人材を自社の要員として割り当てる必要があり、当該分野を担う人材にはサイバーセキュリティに関するリスクと対策について理解するのに必要なスキル・知識が求められる**旨が示されている。

- なお、「セキュリティ統括機能」は、**「機能」であって「組織」として設置しなくてもよい**（企業組織の状況に応じて、最適な形態は異なる）とされる。

図表8　セキュリティ統括機能のイメージ



出典：https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf

図表9　セキュリティ統括機能が担うタスク※1

セキュリティ統括				
方針策定	セキュリティ戦略	法令対応（国内法対応、各国法対応）		
		セキュリティポリシー 策定		
		リスクマネジメント・事業継続管理（BCM）		
		組織体制・業務分掌・業務権限 策定		
		セキュリティ基準・政府等ガイドライン対応		
実務	セキュリティ実務	規程・社則・技術的ガイドライン策定		
		構成管理指針策定・アセスメント実施		
		情報共有・情報連携		
		インシデント管理・CSIRT活動（SOC 含む）		
支援	セキュリティ対応	新規技術・サービス導入		
		データ管理		
実務支援	事業分野別セキュリティ対策	IoT	IT	OT※2
	企画	セキュリティ戦略 / 予算措置		
	設計	セキュリティバイデザイン		
	調達	選定基準（機器・サービス等）		
	運用	運用保守基準 / 品質管理		
	監査	アセスメント / 監査		
	調達先管理	サプライチェーンリスク管理		
	委託先管理			

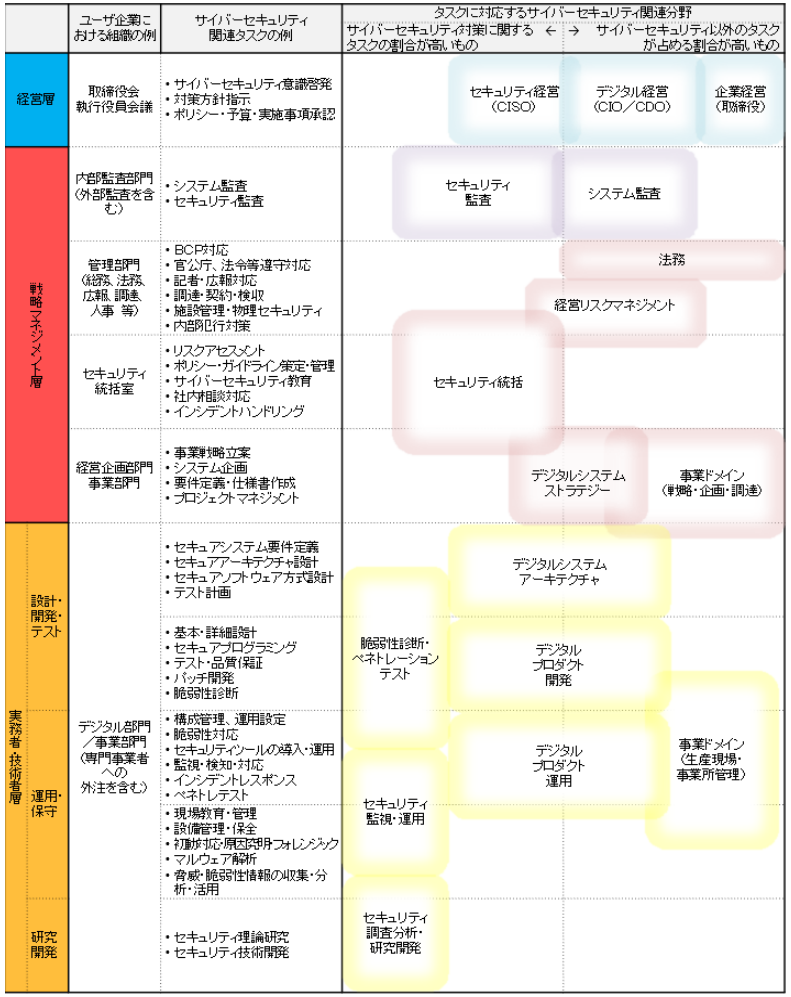
※1 一般社団法人サイバーリスク情報センター 産業横断サイバーセキュリティ人材育成検討会（CRIC CSF）：『ユーザー企業のためのセキュリティ統括室構築・運用キット（統括室キット）Part 1』（2018年11月）
https://cyber-risk.or.jp/contents/Security-Supervisor_Toolkit_Part1_v1.0.pdf

※2 Operational Technology（製造設備や重要インフラなどの制御技術）

既存の関連施策②：ITSS＋「セキュリティ領域」

- ITSS+は、第4次産業革命に向けて求められる**新たな領域の“学び直し”の指針**として、データサイエンス、アジャイル等の領域を対象に策定された**スキル標準**であり、サイバーセキュリティについても「セキュリティ領域」として定義されている。　※前頁の「サイバーセキュリティ体制構築・人材確保の手引き」においては、ITSS+（セキュリティ分野）の整理を活用。
- **サイバーセキュリティに関するタスクをまとめて17種類の「分野」を設定**し、その担当部署/機能の例を提示。

ITSS＋「セキュリティ領域」で定義されている17分野



ITSS＋「セキュリティ領域」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）	●サイバーセキュリティ意識啓発
	デジタル経営（CIO/CDO）	●対策方針の指示
	企業経営（取締役）	●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

出典：https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/security.html

既存の関連施策③：デジタルスキル標準／ＤＸ推進スキル標準

- 経済産業省では、**DX時代の人材像を「デジタルスキル標準」として整理し、公表**。**個人の学習や企業の人材確保・育成の指針**としている。

※ デジタルスキル標準は、デジタルスキル標準のうちすべてのビジネスパーソンが身に着けるべき能力・スキルを定義した「DXリテラシー標準」と、**DXを推進する人材類型の役割や習得すべきスキルを定義した「DX推進スキル標準」**から構成されている。

- 「DXスキル標準」の中で、「業務プロセスを支えるデジタル環境におけるサイバーセキュリティリスクの影響を抑制する対策を担う人材」として、**「サイバーセキュリティ」人材類型を提示**している。

全てのビジネスパーソン（経営層含む）

＜DXリテラシー標準＞

全てのビジネスパーソンが身につけるべき知識・スキルを定義

DXを推進する人材

＜DX推進スキル標準＞

DXを推進する人材類型の役割や習得すべきスキルを定義

- ビジネスパーソン一人ひとりがDXに参画し、その成果を仕事や生活で役立てる上で必要となるマインド・スタンスや知識・スキル（Why、What、How）を定義し、それらの行動例や学習項目例を提示

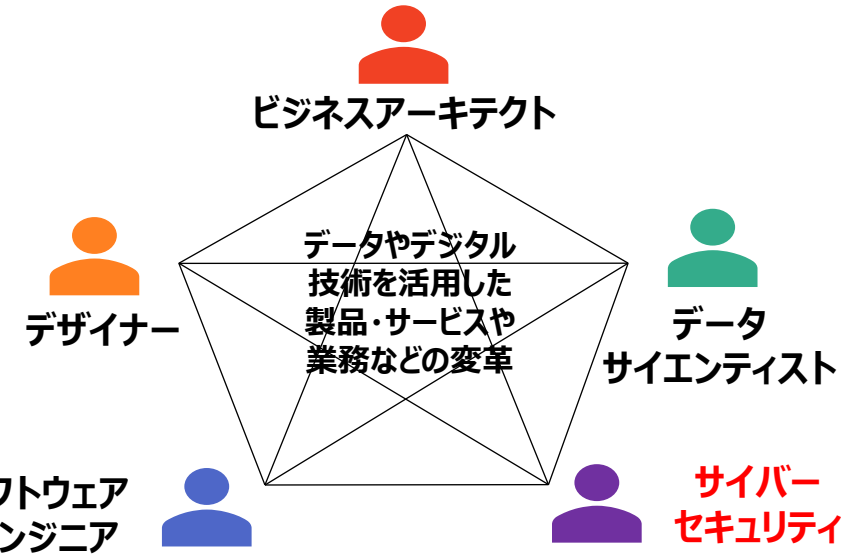
Why
DXの背景
社会、顧客・ユーザー、競争環境の変化

What
DXで活用されるデータ・技術
ビジネスの場で活用されているデータやデジタル技術

How
データ・技術の利活用
データやデジタル技術の利用方法、活用事例、留意点

マインド・スタンス
社会変化の中で新たな価値を生み出すために必要な意識・姿勢・行動

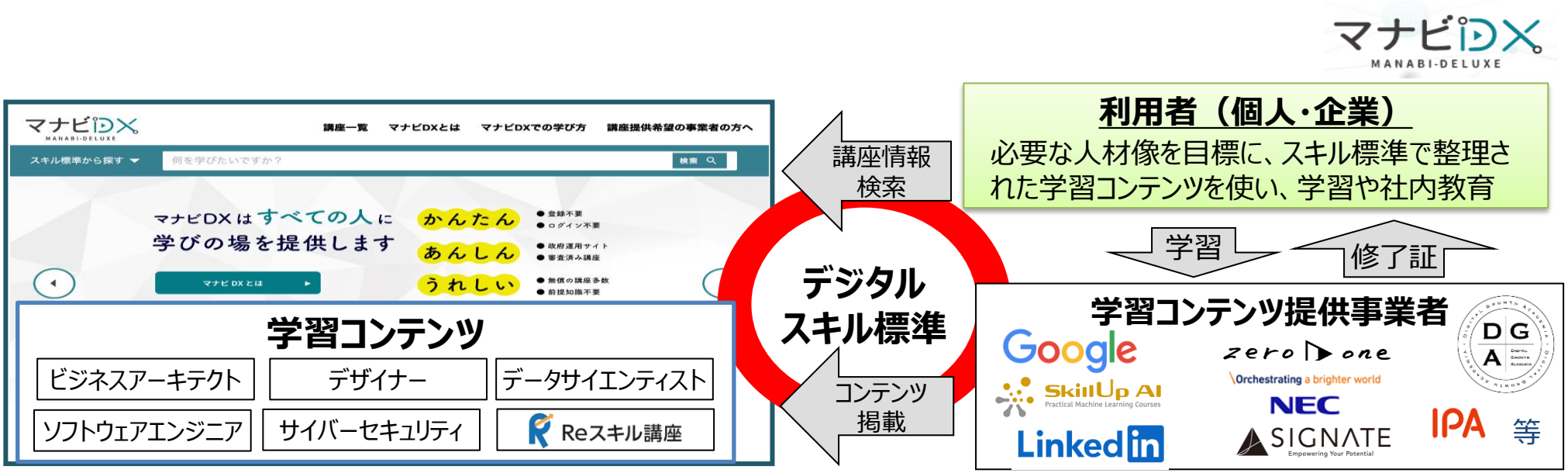
- DX推進に主に必要な５つの人材類型、各類型間の連携、役割（ロール）、必要なスキルと重要度を定義し、各スキルの学習項目例を提示



出典：デジタルスキル標準（DSS） https://www.ipa.go.jp/jinzai/skill-standard/dss/
（資料）第19回 産業構造審議会 経済産業政策新機軸部会　資料３より抜粋・加工

既存の関連施策④：マナビＤＸ

- 経済産業省では、IPAを通じ、**<u>デジタルスキル習得に関する講座を紹介するポータルサイト</u>**である「マナビＤＸ（デラックス）」を運営。
- デジタルに関する新しい知識・スキルを習得したいが、何をどのように学んだらよいかわからない方のために**<u>経済産業省・IPAで策定した各種スキル標準（デジタルスキル標準など）を活用して講座を探すことが可能</u>**。
- 同サイトで提供する**<u>一定レベル以上の認定講座</u>**について、厚生労働省が定める要件を満たした場合は、**<u>厚労省の個人向けや企業向けの支援策（専門実践教育訓練給付、人材開発支援助成金）の対象</u>**となる。



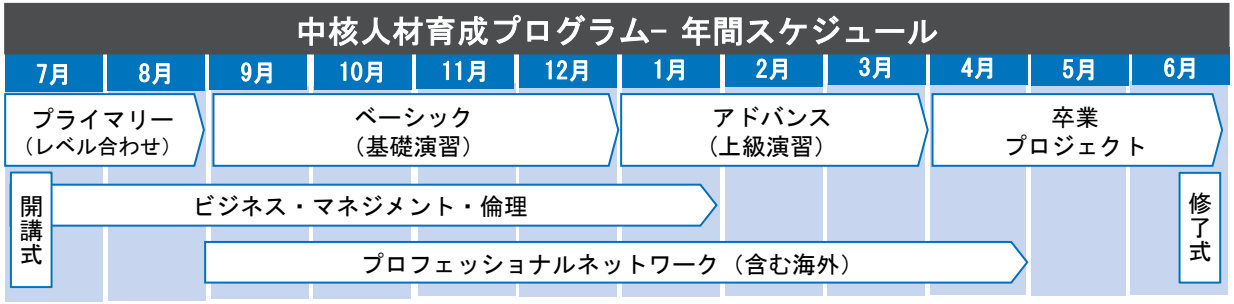
（資料）第19回 産業構造審議会 経済産業政策新機軸部会　資料３より抜粋

既存の関連施策⑤：IPA産業サイバーセキュリティセンター（ICSCoE）(2017年4月設置)

- 社会インフラ・産業基盤における防護力の強化のため、OT(制御技術）とIT（情報技術）の知見を結集させた**世界レベルのサイバーセキュリティ対策の中核拠点**として、IPA内に発足。
- ICSCoEでは世界的にも限られている、制御系セキュリティにも精通する講師を招き、テクノロジー、マネジメント、ビジネス分野を総合的に学ぶ1年の集中トレーニング等を実施。

□　１年を通じた集中トレーニング

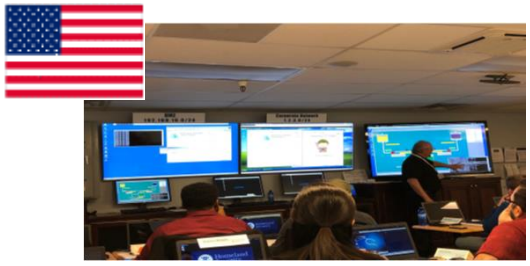
□　電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣
（第1期：76人、第2期：83人、第3期：69人、第4期：46人、第5期：48人、第6期：48人、第7期：65人）



- IT系・制御系に精通した専門人材の育成
- 模擬プラントを用いた対策立案
- 実際の制御システムの安全性・信頼性検証等
- 攻撃情報の調査・分析

現場を指揮・指導するリーダーを育成

□　米・英・仏等の海外とも協調したトレーニングを実施



➢ DHSが開催する高度なサイバーセキュリティトレーニングである301演習への参加

➢ 政府機関、自動車業界、スタートアップ企業の代表者等からの講義や意見交換を実施

➢ 政府機関、産業界等のセキュリティ専門家との意見交換や研究機関の施設見学等を実施

など

既存の関連施策⑥：その他

- JNSAが策定している知識体系を整理したディクショナリーや、試験制度の運用、独法や大学を通じた演習等を実施。

施策	推進主体	概要
セキュリティ知識分野（SecBoK）	JNSA	要求されるセキュリティの知識・スキルの項目を役務毎に一覧化したディクショナリー
情報処理安全確保支援士試験	経済産業省（IPA）	セキュリティに係る最新の知識・技能を備えた専門人材の国家資格
情報セキュリティマネジメント試験	経済産業省（IPA）	情報セキュリティマネジメントの計画・運用・評価・改善を通して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習得する試験
「プラス・セキュリティ」知識の補充のためのモデルカリキュラム	NISC	プラス・セキュリティ知識を習得とするためのカリキュラムの参考例
ITSS+（プラス）セキュリティ領域	経済産業省	企業のセキュリティ対策に必要となるセキュリティ関連業務のまとまりを 17 分野に整理し、それぞれの分野に求められるセキュリティ知識・スキルの概要をまとめたもの
enPiT	大学	高度化する情報セキュリティの脅威を理解し、リスクマネジメントに必要な知識、基本的技術、実践力を備えた人材を育成することを目的としたプログラム。
中核人材育成プログラム	IPA	制御系セキュリティにも精通する講師にるテクノロジー、マネジメント、ビジネス分野を総合的に学ぶ1年間のプログラム
CYDER	NICT	サイバー攻撃を受けた際の一連の対応（インシデント対応）をパソコンを操作しながらロールプレイ形式で体験できる演習
SC3共通語彙集	SC3	米国における企業側と教育側のCAE-Cにおける共通的な部品をマッピングし、産学の双方で活用することを想定した語彙集
J17（情報セキュリティ）	一般社団法人情報処理学会	大学において、情報学を専門とする学科対象の教育カリキュラム標準(J17)のサイバーセキュリティに関するカリキュラム。

出典：各種公開資料より、経済産業省にて作成

本日議論いただきたい点

本日議論いただきたい点①（セキュリティ・キャンプの拡充）

【新たなセキュリティ・キャンプの実施】

- 応募者数が増加していることなども踏まえ、これまで参加ができなかった人材向けに、**新たに第２セキュリティ・キャンプ（仮称）を実施し**、セキュリティ・キャンプの**育成数拡大を目指す**こととしてはどうか。
- その際、**定量的な目標を設定**することの是非についてどのように考えるか。定量的な目標を設定することが望ましい場合、どのような目標が考えられるか。

【修了生コミュニティの形成】

- キャンプ修了生との継続的な関係を維持し、官民での人材交流や企業間を越えた修了生同士の連携を促進する観点から、**修了生やＩＰＡの講師が常時つながることができる会員制のコミュニティを構築する**こととしてはどうか。
- 現にセキュリティ・キャンプの中核的運営主体である**ＩＰＡを中心に事務局を整備する**こととしてはどうか。

【キャンプ修了生の活躍】

- キャンプ修了生が、セキュリティ産業の担い手（供給主体）として華々しく活躍するためには、**どのような政策課題にアドレスする必要があるか**。

本日議論いただきたい点②（登録セキスペの活用及び制度の見直し）

【更新に係る義務講習の見直し】

- 高額な維持コスト等を見直す観点から、登録セキスペ更新の要件を、「オンライン講習」＋「実践講習又は特定講習」を受講することから、①**ＩＰＡが実施するオンライン講習を毎年受講すること**、**又は**②**民間事業者等が実施する特定講習を３年に１回受講すること**、**に改める**こととしてはどうか。
- その上で、民間事業者等が実施する特定講習（上記②）との同等性を担保するために、**ＩＰＡが実施するオンライン講習**（上記①）**において、実践的な要素を組み込む**こととしてはどうか。その上で、オンライン講習において**実践的な要素を組み込むためにはどのような方法が考えられるか**。

【更新に係る義務講習の免除対象】

- 高額な維持コスト等を見直す観点から、登録セキスペの中で、**セキュリティに関する実務要件を課している他の資格も保有する者については、当該資格維持の年数をもって、**登録セキスペの資格を維持するに足る能力を有すると客観的に判断し、更新に係る**義務講習の免除対象としてはどうか**。
- その際、**セキュリティに関する実務要件を課している資格として、具体的にどのような資格が適当と考えられるか**。

【ユーザー企業での登録セキスペ活用促進】

- 補助金施策の要件や各種指針等との紐付けや、重要インフラ等の特定業種における必置化のほか、ユーザー企業における登録セキスペの活用を進めるために**どのような政策的対応が考えられるか**。

【登録セキスペ活躍の場の拡大】

- 市場の力も活用しつつ**登録セキスペと中小企業等とのビジネスベースのマッチングを促進する**ために、**どのような政策的対応が考えられるか**（指導メニュー、アクティブリストの内容、支援機関等との連携の在り方等）。
- 登録セキスペによる活躍の場を拡大するためには、**どのような政策課題にアドレスする必要があるか**。

本日議論いただきたい点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）

- 今後の進め方として、
  - ① まずは、**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役割について共通の認識**を醸成した上で、
  - ② **当該役割を果たすために必要なスキル・知識及びその水準（深度）についての考え方**を整理しつつ、
  - ③ 当該考え方に沿った各種教育・訓練機会が民間事業者等により中堅・中小企業等に対して提供され、かつ、そうした教育・訓練機会が活用されるための、**官民での連携・役割分担の在り方（民による市場原理の活用・官による市場の失敗の是正の在り方）**を検討することとしてはどうか。

- ①について、既存施策の拡充や改善などをベースとすることに鑑みれば、「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」において示す**「セキュリティ統括機能」の役割がベースになると考えらえるが、どうか**。　**⇒本日特に議論いただきたい**

- また、「セキュリティ統括機能」の役割について、**中堅・中小企業を対象とした場合**、その実態に照らして、**過不足はあるか**。あるいは、大企業と中堅・中小企業で当該役割に**差異を設けることは不適当か**。　**⇒本日特に議論いただきたい**

- ②について、政策効果・実現可能性・継続性等の観点から、**どの程度の抽象度・具体度で「必要なスキル・知識」及びその水準を定めることが適当か**。同様の観点から、国（政府機関）が、当該水準に到達するために必要な標準的な教育・訓練機会の水準（カリキュラム・シラバス）を整備することについてどのように考えるか。

- ③について、**民による市場原理の活用**・**官による市場の失敗の是正の在り方**をどのように考えるか。

※中堅・中小企業等による教育・訓練機会の活用を慫慂するための政策対応の例：試験制度との連携、マナビDXとの連携、SECURITY ACTION自己宣言要件への追加、サイバーセキュリティ経営ガイドライン・中小企業情報セキュリティ対策ガイドラインへの反映、厚労省の教育訓練給付制度との連携　等

今後のスケジュール

本検討会の今後のスケジュール

- 今年度内に議論をとりまとめるべく、以下の段取りで検討を進めてまいりたい。

	時期	主な討議事項（想定）
第２回	令和６年８月７日（水）	
第３回	令和６年９月～10月	中間とりまとめ（案）
第４回	令和７年１月頃	
第５回	令和７年２月～３月上旬	最終とりまとめ（案）