経済産業省

資料３

第２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８月

経済産業省 商務情報政策局

サイバーセキュリティ課

登録セキスペの活用及び制度の見直し

前回御議論いただいたこと、御指摘

- 第１回検討会においては、主に以下のような御意見をいただいた。

- 「メリットがない」ことの方が「費用が高い」ことよりも問題。メリットを示す必要。
- 企業内部人材とベンダー人材で目指す点が異なるのではないか。
- 更新コストを下げることの対外的な説明は困難ではないか。
- 国家資格としてのブランドを維持・強化すべき。
- 登録セキスペ制度内でのポイント制（公認会計士類似のもの）も検討してはどうか。
- オンライン講習で実践的要素を組み込むことは難しい。
- 業種横断対策水準との連動など、活用策とセットで検討すべき。

登録セキスペが目指すべき人材像

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
サイバーセキュリティ人材の育成促進に向けた検討会　資料４より抜粋

- 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。

登録セキスペの果たすべき役割の変化

- 制度創設時の趣旨として、登録セキスペは、企業における安全な情報システムの企画・運用等の支援を行うことや、サイバーセキュリティ対策の調査・分析等を行い、その結果に基づき必要な指導・助言を行うことを想定していた。そうした趣旨に基づき、現に提供されている**特定講習の内容は、実務者・技術者層向けを想定した講座が多い**。また、**現状、登録者は外部企業を支援するようなベンダー企業側に偏っている**。
- サイバー攻撃は今後ますます増加するとともに高度化・複雑化していくおそれがある中、一定水準規模以上の企業においては、サイバーセキュリティ対策に外部委託を積極活用しつつも、**企業におけるリスクマネジメント活動の一部として、自社のサイバーセキュリティリスクを把握し、必要な意思決定や管理を行い、対策を推進する立場の人材を割りあてる必要**がある。
- こうした状況において、**登録セキスペは「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」としてのみならず、「企業等の内部に置かれるべき人材」としての役割を果たす期待が高まっているのではないか**。
- ついては、ユーザー企業における登録セキスペの配置を促進していく必要があるが、「企業等の内部に置かれるべき人材」にとっては、「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」が持ち合わせているスキル（マルウェアの解析等）までは必ずしも求められていないのではないか。
- **「企業等の内部に置かれるべき人材」と「企業等の外部から専門的なセキュリティ対策を実施できる人材」とで、必要な知識・スキルはどのように異なるか**。

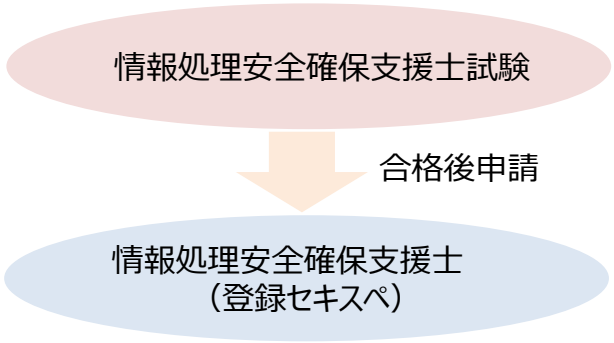
○情報処理の促進に関する法律（昭和四十五年法律第九十号）
（情報処理安全確保支援士の業務）
第六条　情報処理安全確保支援士は、情報処理安全確保支援士の名称を用いて、事業者その他の電子計算機を利用する者によるサイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。以下同じ。）の確保のための取組に関し、**サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うとともに、必要に応じその取組の実施の状況についての調査、分析及び評価を行い、その結果に基づき指導及び助言を行うことその他事業者その他の電子計算機を利用する者のサイバーセキュリティの確保を支援することを業とする**。

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・運用の支援を行うこと
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・助言を行うことを想定

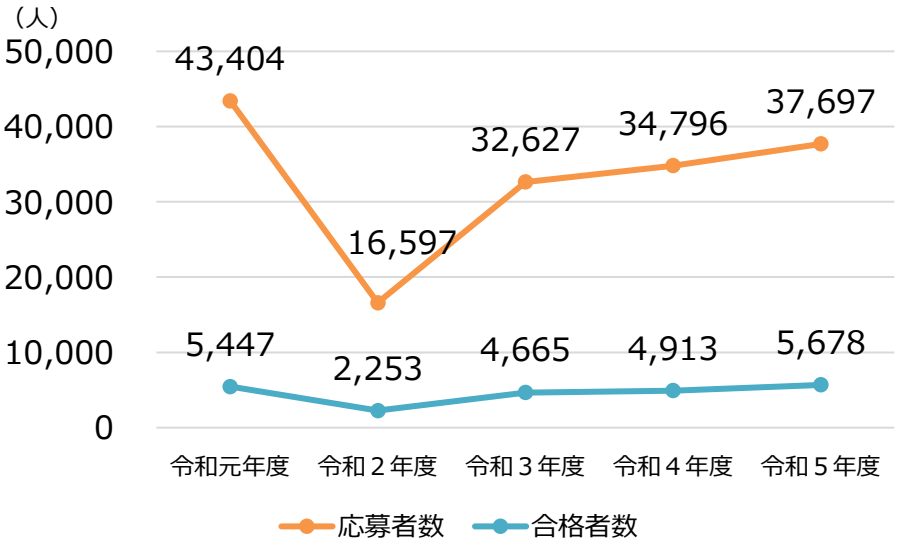
（参考）情報処理安全確保支援士試験

- 平成29年度から「情報処理安全確保支援士試験」を開始。筆記による春期（4月）、秋期（10月）の年2回実施。

○試験と登録セキスペの関係



○試験応募者数及び合格者数の推移



※令和2年度は新型コロナウイルス感染症の影響により、春期試験を中止したため、応募者数が大幅に減少。

○試験問題例

【令和６年度春期午後試験問題】
問１:APIセキュリティを題材に、セキュリティ設計及び脆弱性対応について出題
問２:サイバー攻撃への対策を題材にリモートワーク及びDDoS攻撃に対するセキュリティ対策について出題
問３:クラウド環境で構築されたWebサイトを題材に脆弱性を悪用した攻撃手法とその対策について出題
問４:Webアプリケーションの脆弱性対策を題材にLinuxの権限設定及びセキュアコーディングについて出題

【令和５年度秋期午後試験問題】
問１：Webアプリケーションプログラムの脆弱性悪用によって発生したインシデントへの対応を題材に、悪用されたクロスサイトスクリプティング（XSS）脆弱性の把握と対応について出題
問２：アパレル業におけるセキュリティ対策の見直しを題材に、サーバ証明書の検証、秘密鍵の管理及び無線LAN環境の見直しについて出題
問３：継続的インテグレーションサービスを提供する企業とその利用企業にセキュリティインシデント対応を題材に、クラウドサービスを使ったシステムで起こりうる攻撃手法とその防御について出題
問４：業務委託関係にある百貨店と運送会社を題材に、個人情報に関するリスクアセスメントについて出題

登録セキスペ特定講習

- 特定講習は民間事業者等により提供される講習であり、令和６年６月現在、**13実施機関47講習**が経済産業大臣により選定されている。ＩＰＡが行う実践講習は汎用的な内容であるのに対して、**特定講習は特定の専門分野についての知識・技能の習得を目的とする内容**となっている。
- 特定講習の該当する分野については、ITSS＋（セキュリティ領域）17分野から選択。現状、**「セキュリティ監視・運用」「セキュリティ調査分析・研究開発」などの実務者・技術者層向けの講習が大半を占めており、経営層および戦略的マネジメント層向けの講習は僅か**。

特定講習のITSS＋（セキュリティ領域）内訳

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

※令和６年度特定講習の内訳

特定講習の例

マルウェア解析ハンズオン専門コース（株式会社ラック）

○主な分野：セキュリティ調査分析・研究開発
○講習内容
- マルウェアに施された耐解析機能への対応手法や隠された機能を特定する手法などを習得。
- 具体的には、耐解析機能と概要、アセンブラ、デバッガとその使い方、耐解析機能の回避、マニュアルアンパックと必要な知識、マニュアルアンパック実践、静的解析、簡易静的解析、IDA入門、IDA実践、演習と時間短縮テクニック、総合演習を行う。

○到達目標
- 耐解析機能を持つマルウェアの解析ができるようになる
- マルウェアの機能を論理的に理解できるようになる
- 膨大なアセンブラ命令から必要な情報を抽出し、見るべきポイントを抑える

インシデントハンドリング実践コース（株式会社インターネットイニシアティブ）

○主な分野：セキュリティ監視・運用
○講習内容
- SOCサービスが検知したインシデント報告書をもとに、セキュリティ機器やサーバから必要なログを採取し、発生しているインシデントの被害状況を把握し、初動対応から封じ込め、根絶を実施。また、発生したインシデントに対する再発防止策をグループで検討・発表することでインシデントハンドリングに関する一連の流れを習得。

○到達目標
- 以下のスキルを習得することでインシデントの連絡を受けた際にインシデントハンドリング一連の流れを行えるようになる
  ①必要なログを収集・解析し被害範囲の特定を行うことができる
  ②発生したインシデントに対し初動対応を行うことができる
  ③経営的な視点も考慮した再発防止策の検討を行うことができる

（参考）登録セキスペ特定講習一覧（2024年６月１日現在）

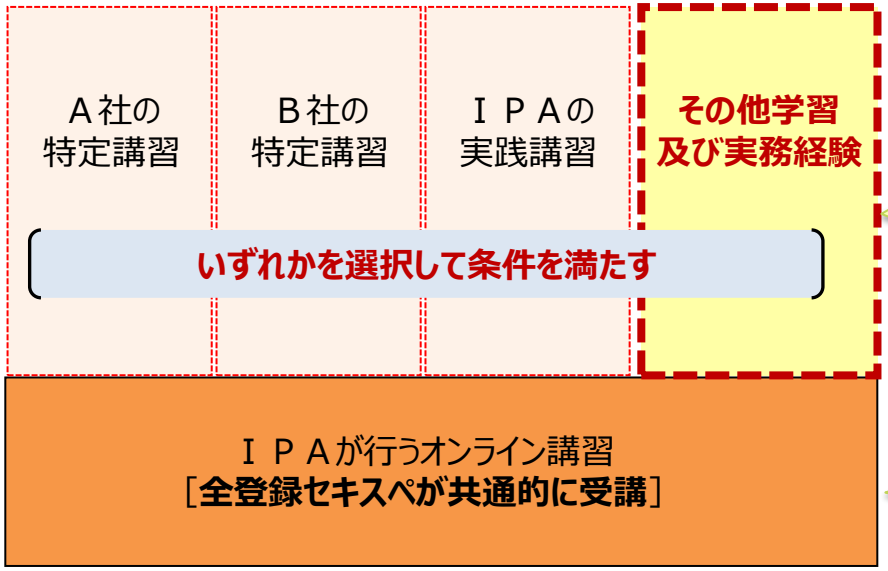
No.	実施機関名	講習名	主な分野
1	大日本印刷株式会社	サイバー・インシデントレスポンス・マネジメントコース　基礎演習	セキュリティ監視・運用
2	大日本印刷株式会社	サイバー・インシデントレスポンス・マネジメントコース 基礎演習１日版	セキュリティ監視・運用
3	大日本印刷株式会社	サイバー・インシデントレスポンス・マネジメントコース 基礎演習２日版	セキュリティ監視・運用
4	株式会社ワイ・イー・シー	Ｗｉｎｄｏｗｓ　Ｆｏｒｅｎｓｉｃｓ	セキュリティ調査分析・研究開発
5	株式会社ワイ・イー・シー	Ｍａｃ　Ｆｏｒｅｎｓｉｃｓ	セキュリティ調査分析・研究開発
6	株式会社ワイ・イー・シー	Ｆｉｌｅ　Ｓｙｓｔｅｍ　Ｆｏｒｅｎｓｉｃｓ	セキュリティ調査分析・研究開発
7	株式会社ワイ・イー・シー	マルウェア解析基礎	セキュリティ調査分析・研究開発
8	トレンドマイクロ株式会社	標的型攻撃 対応・防御トレーニング５日版	セキュリティ監視・運用
9	トレンドマイクロ株式会社	標的型攻撃 対応・防御トレーニング３日版	セキュリティ監視・運用
10	トレンドマイクロ株式会社	インシデント調査トレーニング クライアント端末版	セキュリティ監視・運用
11	トレンドマイクロ株式会社	ランサムウェア 対応・防御トレーニング	セキュリティ監視・運用
12	ＮＥＣビジネスインテリジェンス株式会社	ＣＳＩＲＴ強化トレーニング マルウェア感染対応編	セキュリティ監視・運用
13	ＮＥＣビジネスインテリジェンス株式会社	ＣＳＩＲＴ強化トレーニング テクニカル編（ＣＴＦ形式）	セキュリティ調査分析・研究開発
14	ＮＥＣビジネスインテリジェンス株式会社	サイバー防御トレーニング―Ｂｌｕｅ　Ｔｅａｍ　Ｔｒａｉｎｉｎｇ―	セキュリティ監視・運用
15	ＮＥＣビジネスインテリジェンス株式会社	インシデントレスポンス基礎　－マルウェア解析編－	セキュリティ調査分析・研究開発
16	ＮＥＣビジネスインテリジェンス株式会社	【フリーシナリオ形式】実践！サイバーセキュリティ演習	セキュリティ調査分析・研究開発
17	ＮＥＣビジネスインテリジェンス株式会社	【ステップバイステップ形式】実践！サイバーセキュリティ演習	セキュリティ調査分析・研究開発
18	ＮＥＣビジネスインテリジェンス株式会社	サイバー攻撃トレーニング　－Ｒｅｄ　Ｔｅａｍ　Ｔｒａｉｎｉｎｇ－	脆弱性診断・ペネトレーションテスト
19	ＮＥＣビジネスインテリジェンス株式会社	インシデントレスポンス基礎　－フォレンジック解析編－	セキュリティ調査分析・研究開発
20	ＮＥＣビジネスインテリジェンス株式会社	インシデントレスポンス基礎　－ログ解析編－	セキュリティ調査分析・研究開発
21	株式会社ラック	Ｗｅｂアプリケーション脆弱性診断ハンズオンコース	脆弱性診断・ペネトレーションテスト
22	株式会社ラック	プラットフォーム脆弱性診断ハンズオンコース	脆弱性診断・ペネトレーションテスト
23	株式会社ラック	マルウェア解析ハンズオン入門コース	セキュリティ調査分析・研究開発
24	株式会社ラック	マルウェア解析ハンズオン専門コース	セキュリティ調査分析・研究開発
25	株式会社ラック	セキュリティオペレーション実践コース 初級編	セキュリティ監視・運用
26	株式会社ラック	セキュリティオペレーション実践コース 中級編	セキュリティ監視・運用
27	株式会社ラック	デジタル・フォレンジックコース	セキュリティ監視・運用
28	株式会社ラック	情報セキュリティ事故対応１日コース 机上演習編	セキュリティ調査分析・研究開発
29	株式会社ラック	マルウェア解析ハンズオン専門演習コース	セキュリティ調査分析・研究開発
30	株式会社ラック	情報セキュリティ事故対応2日コース 実機演習編	セキュリティ監視・運用
31	株式会社アイ・ラーニング	情報セキュリティマネジメント構築	セキュリティ統括
32	株式会社アイ・ラーニング	プロが教えるインシデント対応実践ワークショップ	セキュリティ調査分析・研究開発
33	株式会社インターネットイニシアティブ	インシデントハンドリング実践コース	セキュリティ監視・運用
34	株式会社インターネットイニシアティブ	攻撃技術理解・防御 APT対策基礎コース	セキュリティ監視・運用
35	株式会社インターネットイニシアティブ	セキュリティ対策基礎 実践コース	セキュリティ監視・運用
36	国立研究開発法人情報通信研究機構（NICT）	実践サイバー演習 RPCI（リプシィ）	セキュリティ監視・運用
37	株式会社バルクホールディングス	Ｃｙｂｅｒ－Ｔｈｒｅａｔｓ　ａｎｄ　Ｄｅｆｅｎｓｅ　Ｅｓｓｅｎｔｉａｌｓ	セキュリティ監視・運用
38	株式会社バルクホールディングス	Ｆｏｒｅｎｓｉｃｓ　Ｔｒａｉｎｉｎｇ	セキュリティ調査分析・研究開発
39	NRIセキュアテクノロジーズ株式会社	セキュアＥｇｇｓ応用編（インシデント対応）	セキュリティ監視・運用
40	NRIセキュアテクノロジーズ株式会社	セキュアＥｇｇｓ応用編（フォレンジック）	セキュリティ調査分析・研究開発
41	NRIセキュアテクノロジーズ株式会社	セキュアＥｇｇｓ応用編（Ｗｅｂアプリケーションセキュリティ）	脆弱性診断・ペネトレーションテスト
42	グローバルセキュリティエキスパート株式会社	Ｍｉｃｒｏ　Ｈａｒｄｅｎｉｎｇ：Ｅｎｔｅｒｐｒｉｓｅ　Ｅｄｉｔｉｏｎ（マイクロハードニング：エンタープライズエディション）	セキュリティ監視・運用
43	株式会社日立アカデミー	ケーススタディから学ぶ情報セキュリティリスク対策	セキュリティ統括
44	株式会社サイバーディフェンス研究所	OTシステムハッキング｜独自プロトコル解析とサイバー攻撃の実践	脆弱性診断・ペネトレーションテスト
45	株式会社サイバーディフェンス研究所	ハッキング｜ハードウェア	脆弱性診断・ペネトレーションテスト
46	株式会社サイバーディフェンス研究所	マルウェア解析Ⅰ	セキュリティ調査分析・研究開発
47	株式会社サイバーディフェンス研究所	マルウェア解析Ⅱ	セキュリティ調査分析・研究開発

登録セキスペ義務講習のみなし受講規定

- **更新費用の負担が大きい**と感じられる登録セキスペが少なからず存在。そのため、**実務経験等を通じた更新講習受講義務の軽減の在り方についても検討**する必要がある。例えば、
  - ✓ CISSPのように個別具体の活動それぞれについて一定の基準を設定し、各々の登録セキスペからの申告内容を審査して減免量を設定
  - ✓ 「登録セキスペアクティブリスト」に掲載された登録セキスペを対象として、そこに掲載される活動総時間や活動種類に応じて減免量を設定

  するなどの方策が考えられるが、**基準の設定に際しては、具体的かつ資格維持の妥当性を客観的に判断することができる必要がある**。当該基準の更新及び運用のコスト、登録セキスペとして望ましい活動（兼業等を通じた中小企業等の支援等）を促進するなどの観点から、どのような方策が現実的と考えられるか。
- また、基準の対象となる学習及び実務経験の一部が、CISSP等の他のセキュリティ資格の更新要件の一部となるなどの連続性についても検討できないか。

＜新しい更新制度イメージ（案）＞



特定講習・実践講習と並ぶオプションとして、講習によって得られる知識・スキルと同等の学習及び実務経験に応じたみなし受講の規定を新設

（※）学習及び実務経験の例
- **・登録セキスペアクティブリストに掲載されている者の活動**
- **・指定書籍、記事等の購読・執筆**
- **・ユーザー企業内部における業務内容の報告・レビュー　等**

国家資格としての登録セキスペの責務や倫理等に係る内容の講習は引き続きＩＰＡが実施し、全登録セキスペが共通的に受講

講習のみなし受講として取りうる方策

- 特定講習及びＩＰＡが提供する実践講習は、講習の性質上、講習の一部分を切り分けることは難しい。特に、特定講習は、提供する事業者や講習内容も多種多様であることも踏まえると、**講習の一部をみなし受講とすることは困難なのではないか**。

※　講習の「一部」をみなし受講とする仕組みを導入するためには、多様な特定講習及び実践講習について、特定の種類・量の実務経験が、それぞれに対し各講習のうちどの部分に相当するのか等をあらかじめ決定する必要がある。そのためには、一定の考え方に基づき講習内容を細分化して重み付けするなどの検討が必要となるが、毎年内容が更新され、かつ、提供事業者も変更・増加し得る特定講習それぞれについて、そうした事務を行う負担と政策効果とのバランスや、一定以上の実務経験をもって講習の「全部」を受講したとみなす場合における政策効果との比較において、現実的な選択肢としては考えにくい。

- ついては、**講習によって得られる知識・能力と同等の実務経験等を一定以上行った者については、特定講習又は実践講習をすべて受講したとみなすこととするのはどうか**。

特定講習の例

マルウェア解析ハンズオン専門コース

○提供事業者：株式会社ラック
○主な分野：セキュリティ調査分析・研究開発
○講習内容
- マルウェアに施された耐解析機能への対応手法や隠された機能を特定する手法などを習得。
- 具体的には、耐解析機能と概要、アセンブラ、デバッガとその使い方、耐解析機能の回避、マニュアルアンパックと必要な知識、マニュアルアンパック実践、静的解析、簡易静的解析、IDA入門、IDA実践、演習と時間短縮テクニック、総合演習を行う。

○到達目標
- 耐解析機能を持つマルウェアの解析ができるようになる
- マルウェアの機能を論理的に理解できるようになる
- 膨大なアセンブラ命令から必要な情報を抽出し、見るべきポイントを抑える

インシデントハンドリング実践コース

○提供事業者：株式会社インターネットイニシアティブ
○主な分野：セキュリティ監視・運用
○講習内容
- SOCサービスが検知したインシデント報告書をもとに、セキュリティ機器やサーバから必要なログを採取し、発生しているインシデントの被害状況を把握し、初動対応から封じ込め、根絶を実施。また、発生したインシデントに対する再発防止策をグループで検討・発表することでインシデントハンドリングに関する一連の流れを習得。

○到達目標
- 以下のスキルを習得することでインシデントの連絡を受けた際にインシデントハンドリング一連の流れを行えるようになる
  ①必要なログを収集・解析し被害範囲の特定を行うことができる
  ②発生したインシデントに対し初動対応を行うことができる
  ③経営的な視点も考慮した再発防止策の検討を行うことができる

（参考）オンライン講習のシラバス

登録初年度の方向けオンライン講習

スキルレベル	ITSS（ITスキル標準）レベル4
コース形態	e-ラーニング
コースの目的、ねらい	登録セキスペとして期待される役割にふさわしい情報セキュリティ実践のために必要な知識・技能・倫理について学習する。
達成目標	次の内容について理解し、指導・助言・支援を求めている人に対して、説明できるようになる。 ・ 登録セキスペの役割と責任、情報セキュリティを取り巻く環境や脅威の背景、能動的な情報およびそれらから検討した具体的なセキュリティ対策 ・ 組織のマネジメントとガバナンス確保におけるサイバーセキュリティ基本法とガイドライン類の活用 ・ 組織としてのセキュリティ対応体制の構築、全社的取り組み、委託関係や契約・法的課題（Readinessの観点） ・ システムライフサイクルの運用フェーズにおけるインシデント発生から、対応、収束、再発防止に向けた対応（Responseの観点） ・ 登録セキスペとして適切な倫理的判断登録セキスペとしての業務に関係する法令等
標準学習時間	知識：１時間 技能：３時間 倫理：２時間　計６時間
コース概要	１．知識　①登録セキスペに期待される役割と知識 ２．技能　①情報セキュリティマネジメント ②インシデント対応【組織編】 ③インシデント対応【技術編】 ３．倫理　①倫理とコンプライアンス ②コンプライアンスを実現するための法令等
修了基準	全単元の受講および理解度確認テスト全問正解 アンケートの回答

（参考）他資格との比較（CISSP）

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
サイバーセキュリティ人材の育成促進に向けた検討会　資料４より抜粋

- 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

（参考）他資格の研修・講習に係るみなし受講規定

- 職業能力開発促進法では、キャリアコンサルタントは、登録についてその更新を受けなければその効力を失う旨の規定が設けられており、職業能力開発促進法施行規則において、更新の要件として、講習の受講が義務付けられている。同規則において、一級の技能検定に合格しているキャリアコンサルタントにより行われるキャリアコンサルティングの実務等について、講習とみなすことができる旨の規定が定められている。

○職業能力開発促進法（昭和四十四年法律第六十四号）
（キャリアコンサルタントの登録）
第三十条の十九　キャリアコンサルタント試験に合格した者は、厚生労働省に備えるキャリアコンサルタント名簿に、氏名、事務所の所在地その他厚生労働省令で定める事項の登録を受けて、キャリアコンサルタントとなることができる。
2　次の各号のいずれかに該当する者は、前項の登録を受けることができない。
一　心身の故障によりキャリアコンサルタントの業務を適正に行うことができない者として厚生労働省令で定めるもの
二　この法律又はこの法律に基づく命令に違反し、罰金以上の刑に処せられ、その執行を終わり、又は執行を受けることがなくなつた日から二年を経過しない者
三　この法律及びこの法律に基づく命令以外の法令に違反し、禁錮以上の刑に処せられ、その執行を終わり、又は執行を受けることがなくなつた日から二年を経過しない者
四　第三十条の二十二第二項の規定により登録を取り消され、その取消しの日から二年を経過しない者
3　第一項の登録は、五年ごとにその更新を受けなければ、その期間の経過によつて、その効力を失う。
4　前項の更新に関し必要な事項は、厚生労働省令で定める。

○職業能力開発促進法施行規則（昭和四十四年労働省令第二十四号）
（講習）
第四十八条の十七　**法第三十条の十九第三項の更新を受けようとする者は、**法第三十条の二十のキャリアコンサルタント登録証（以下「登録証」という。）の有効期間が満了する日の五年前から同日までの間に、**次の各号に掲げる講習ごと当該各号に定める時間以上の講習を受けなければならない。**
一　労働関係法令その他キャリアコンサルティングを適正に実施するために必要な知識の維持を図るための講習として別に厚生労働省令で定めるところにより厚生労働大臣が指定するもの　八時間
二　キャリアコンサルティングを適正に実施するために必要な技能の維持を図るための講習として別に厚生労働省令で定めるところにより厚生労働大臣が指定するもの　三十時間
2　キャリアコンサルティングに関し、一級の技能検定に合格しているキャリアコンサルタントにより行われるキャリアコンサルティングの実務に関する指導又はキャリアコンサルティングの実務は、前項第二号の規定の適用については、十時間以内に限り講習とみなす。
3　キャリアコンサルティングに関し、一級又は二級の技能検定に合格した者に対しては、当該合格の日から五年以内に法第三十条の十九第三項の更新を受けようとする際にその者が受けるべき第一項の講習を免除する。
4　キャリアコンサルティングに関し、一級の技能検定に合格した者に対しては、第一項第二号の講習を免除する。
5　キャリアコンサルタント試験に合格した日から五年を経過した日以降に法第三十条の十九第一項の登録を受けようとする者については、前各項の規定を準用する。この場合において、第一項中「法第三十条の二十のキャリアコンサルタント登録証（以下「登録証」という。）の有効期間が満了する日」とあるのは、「法第三十条の十九第一項の登録を受ける日」とする。

（参考）キャリアコンサルタントのみなし受講

- キャリアコンサルタントは、次にあげる時間については、技能講習を受けたとみなされ、技能講習の必要時間からその時間数分を免除することができる（最大10時間まで）。
  - ① 技能検定キャリアコンサルティング職種1級に合格したキャリアコンサルタントからキャリアコンサルティングの実務に関する指導を受けた時間
  - ② キャリアコンサルティングの実務に従事した時間
- それぞれ、「1級キャリアコンサルティング技能士による実務に関する指導証明書」「実務従事に関する証明書」の内容について、個別判断がなされている。

技能検定キャリアコンサルティング職種1級に合格したキャリアコンサルタントにより行われるキャリアコンサルティングの実務に関する指導

- 指導者が、技能検定キャリアコンサルティング職種1級に合格しており、かつキャリアコンサルタントであること。
- 指導者から被指導者への指導が、一対一、または個別指導が成立する程度の一対少人数（概ね6名以内）形態で、対面・応答的方式により行われること。
- 指導が、被指導者がキャリアコンサルタントとして従事した事例に基づくものであること（職業キャリアの分野以外のカウンセリング事例に基づくもの等は対象とならない。）また、指導者が被指導者のキャリアコンサルタントとしての課題や目標を把握した上で、これを踏まえキャリアコンサルティングの技能等に関して個別・具体的な指導を行っていること。

キャリアコンサルティングの実務に従事

- キャリアコンサルティングによる支援対象者が、「労働者」であること。なお、ここでいう労働者とは、現在就業している方のみならず、現在仕事を探している求職者（ハローワーク等の職業紹介機関に求職の申込みを行っている方、学卒就職希望者等）を含む。
- 相談の内容・目的が職業の選択、職業生活設計又は職業能力開発及び向上に関するものであること。
- キャリアコンサルティングが一対一で行われるもの、又はこれに準ずるもの（少人数（概ね6名以内）グループワークの運営等）であること（情報提供に止まるもの、授業・訓練の運営そのもの等は含まない。）。

出典：https://careerconsultant.mhlw.go.jp/n/update.html
https://careerconsultant.mhlw.go.jp/n/faq_update.html

ユーザー企業における登録セキスペの活用イメージ

- 昨今のサイバー攻撃は、多様化・高度化している中、外部委託にセキュリティ対策のすべてを任せるのではなく、**企業等の内部にセキュリティ対策を行うことができる人材を配置する必要性が高まってる**。こうした状況において、企業等の内部に配置すべき人材として、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登録セキスペに期待される役割は大きい。
- 他方で、企業によって、規模、業種、情報資産・IT依存度、サプライチェーン上の重要度等が様々であることを踏まえると、**企業ごとに登録セキスペの活用方法は異なるのではないか**。

ユーザー企業における活用イメージ

企業類型

**中小企業
小規模事業者**

（例）専任でセキュリティ対策を推進する人材の確保が困難な企業

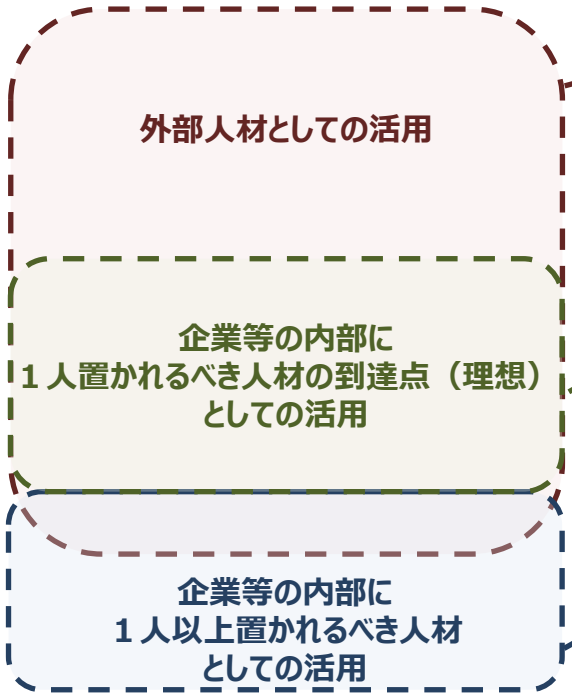
**中堅企業
サプライチェーン企業**

（例）「セキュリティ統括機能」としてセキュリティ対策を推進する専任人材を置くべき企業

**大企業
重要インフラ等事業者**

（例）機密性の高い情報を保有する大企業、重要インフラ・基幹インフラ等の重要物資を取り扱う企業

登録セキスペの活用像



登録セキスペの具体的活用イメージ

企業外部からの支援

・・・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を行う場合、または、マルウェア解析等のより専門的な知見や技術を要する業務を実施する場合を想定。登録セキスペアクティブリストを利用したマッチング等により促進。

「セキュリティ統括機能」の体現

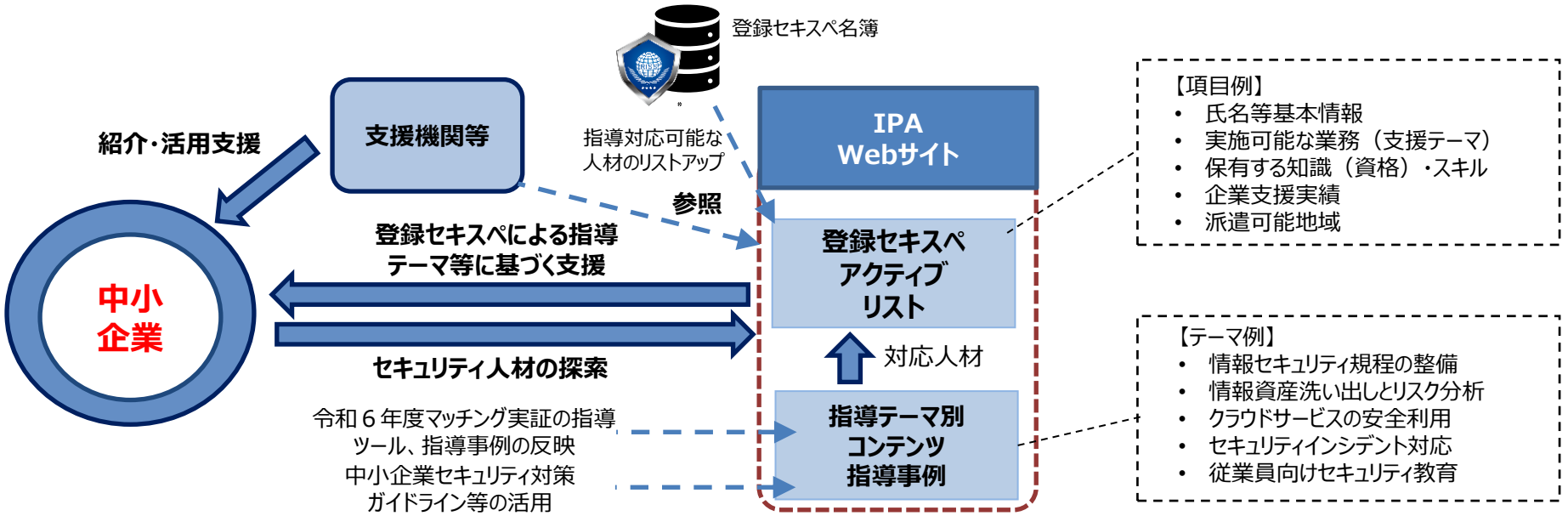
・・・企業等の内部において、経営層、IT部門、事業部門、管理部門等とのコミュニケーションや、IT／セキュリティベンダー企業との技術的調整を通じて、実施すべきセキュリティ対策を実現する場合を想定。サプライチェーン強化に向けたセキュリティ対策評価制度や投資促進施策との連携等により促進。

内製化された人材

・・・機密性の高い情報を保有する大企業、重要インフラ・基幹インフラ等の重要物資を取り扱う事業者等において、上記観点を内製化する場合を想定。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や業界基準等との連携等により促進。

登録セキスペアクティブリスト

- 中小企業は、取引先である大企業からセキュリティ対策を求められる場合もあるなど、セキュリティ対策を促進していくことは大きな課題。2024年中小企業白書の統計によると、ＤＸに取り組む中小企業は年々増加しており、ＤＸの具体的取組内容を見ても、セキュリティ対策が上位に位置付けられており、中小企業にとってもセキュリティ対策は必要性の高い項目である。
- 一方で、セキュリティ対策を行うにしても、**中小企業の中には、「コストの問題から対策を実施できない」「どのようにしてセキュリティ対策を行ったら良いか分からない」といった課題**を抱える企業が多く存在。
- また、ＩＰＡでは、登録セキスペの検索システムを整備しているが、**登録セキスペが保有している知識・スキル、企業に対する診断が可能なのかといった情報が見える化できていない**。
- そこで、令和６年度の登録セキスペと中小企業等とのマッチング実証事業を通して、**登録セキスペが実施可能な業務やスキル、企業支援実績等を可視化**し、「中小企業セキュリティ対策ガイドライン」等を活用した支援メニューとの紐づけを行い、令和７年度以降に、**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）を作成予定**。
- **活躍の場がないとする登録セキスペと、コスト及び対策手法を課題に上げる中小企業等とのミスマッチを解消**し、ビジネスベースでのマッチングを進めていく。



サプライチェーン強化に向けたセキュリティ・アーキテクチャの検討

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

- これまで「サイバーセキュリティ経営ガイドライン」や産業分野別のガイドライン等を整備し、各企業等による積極的な取組を推進してきたところ。他方、**異なる取引先から様々な対策水準を要求される**といった課題や、**外部から各企業等の対策状況を判断することが難しい**といった課題は依然として存在。
- 今後は、諸外国で議論が進んでいる、「サイバー対策」のレーティング等も参考にしつつ、**各企業等の業種・規模などのサプライチェーンの実態を踏まえた満たすべき各企業の対策のメルクマール**や、**業界間の互換性を確保しながら**その**対策状況を可視化する仕組みを検討していく。**
- 併せて、関係省庁とも連携し**政府機関・企業による活用を促す枠組みと紐付ける**ことで、**その実効性を強化**していく。

想定される検討事項

- **既存のガイドライン等をIPAが一元的に管理・体系化し、企業のセキュリティ対策基準を明確化できないか**
- 既存ガイドライン等と整合を取りつつ、**業種横断的なセキュリティ対策レベルを評価（自己評価、第三者認証）できないか**
- 政府機関等における**調達要件**や、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**を促進し、**実効性の強化**につなげられないか

※サイバーセキュリティへの取組に関し、投資家を含むステークホルダと企業経営者との対話（開示）の在り方等についても検討が必要ではないか。

対策レベルの可視化（イメージ）

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

政府調達・補助施策等への要件化

取引先からの対策要請による活用促進

利害関係者への情報開示による対話の促進

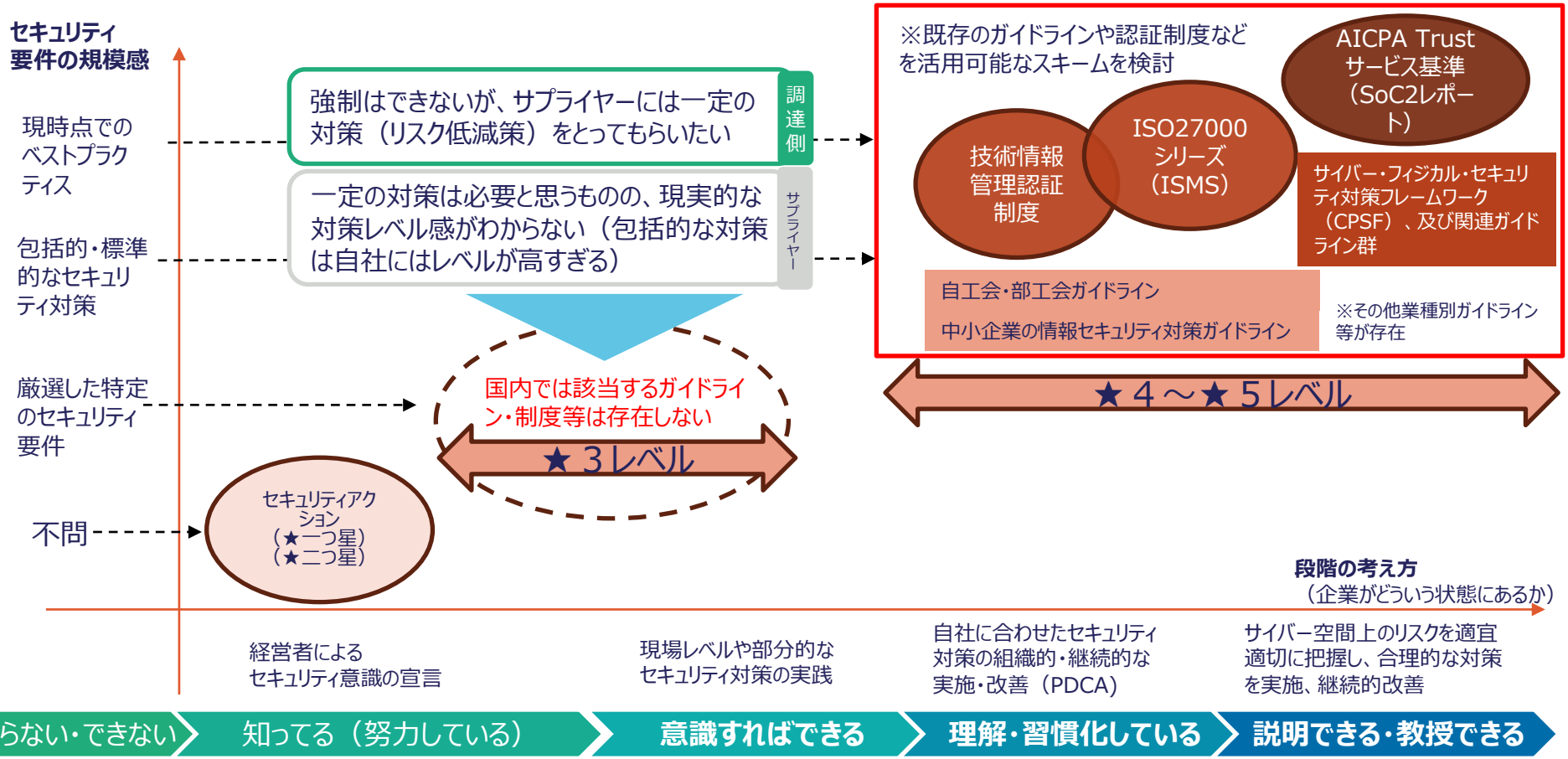
「サプライチェーン強化に向けたセキュリティ対策評価制度」構成・内容イメージ

- サイバー攻撃により、取引上共有している機微情報の漏洩や部品・サービスの供給途絶など、自社のみならずサプライチェーン全体に影響を及ぼす事態が発生しうる。このようなインシデントの予防・抑制を目的に、サプライチェーン構成企業全体のセキュリティ対策レベルの向上と、実施状況の効率的な確認ができる手法として「サプライチェーン強化に向けたセキュリティ対策評価制度」を提案。
- 中小企業を含めた多様なサプライチェーン企業が参照できるよう、三段階のセキュリティレベルを想定。

	三つ星（★３）	四つ星（★４）	五つ星（★５）
段階の考え方（企業がどういう状態にあるか）	**現場レベルや部分的なレベルでのセキュリティ対策が実践されている**	自社に合わせたセキュリティ対策の**組織的・継続的な実施・改善（PDCA)がなされている**	サイバー空間上の**リスクを適宜適切に把握し、合理的な対策を実施、継続的改善がなされている**
対象として想定する事業者	サプライチェーンを形成するすべての企業等	・産業界を代表・牽引する立場の企業等（それを目指す企業等を含む）の**サプライチェーンにおいて重要な機能・役割等を担うサプライヤー企業**	・産業界を代表・牽引する立場の企業等（それを目指す企業等を含む）の**サプライチェーンにおいて特に重要な機能・役割等を担うサプライヤー企業**等
対策セットの考え方（対策の規模感）	上記に該当する企業等が、最低限実装すべきセキュリティ対策の水準（１５項目程度）	上記に該当する企業等が、標準的に目指すべきセキュリティ対策の水準（～５０項目程度）	上記に該当する企業等が、現時点で到達点として目指すべきセキュリティ対策の水準（１００項目～）
		※既存のガイドラインや認証制度などを活用可能なスキームを検討※	
実施状況の評価・確認方法	・自己適合宣言（社内外の登録セキスペ等専門家による確認）	・自己適合宣言　（★３と同様） ・第三者評価 と二段階に分けることも考えられる（★４、★４plus）	・第三者評価

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関するSWG　資料５より抜粋

想定する企業像とセキュリティ要件の規模感



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

前回御議論いただいたこと、御指摘

- 第１回検討会においては、主に以下のような御意見をいただいた。

- 企業内でセキュリティ担当者が担うべき役割と実施すべき業務を示すことが重要。
- 規模だけでなく業種でも守るべき情報が変わり、内部で必要な人材の質は異なる。
- 自社の業務を理解の上、セキュリティ能力を獲得し、自社のビジネスを守る必要。この人材に求められる知識・スキルのレベル感や項目を国が指針を示す必要。
- 中小企業には指針を示した上で、それを実行するために具体的なガイド（How-to）を示すことも必要ではないか。
- 指針は国が示しつつ民間市場に任せるべき。民間演習を政府として認定等が有効。
- 税務について、社内経理担当を置く場合、外部の税理士を活用する場合があるのと同様に、セキュリティに関しても、内部人材の配置と外部の登録セキスペ等を活用する場合がある、といった考え方を普及させることが必要ではないか。

前回の御指摘と既存の施策との関係

- 既にサイバーセキュリティ経営ガイドラインやその付録など複数あり、社内のセキュリティ人材育成に関して、一定程度方向性を示している（詳細は次頁以降参照）。
- 他方、セキュリティ人材の充足や対策の実施が十分でない中堅・中小企業が多くみられる現状に鑑みれば、以下に掲げる**既存の施策について、どのような点が不足していると考えられるか**。

社内で実施すべき業務と外部委託可能な業務

- 「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」において記載

規模や業種の異なる企業での取り組み事例

- 「サイバーセキュリティ経営ガイドライン実践のためのプラクティス集　第４版」において、企業の規模や業種を示した上で、実際の取組事例を多数提示
- 「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、「サイバーセキュリティ体制に影響を及ぼすと考えられる要素」として業種、事業規模、事業のバリエーション等の要素を記載
- 「中小企業の情報セキュリティ対策ガイドライン」（IPA）は、経営者編と管理実践編から構成されており、管理実践編において、企業における対策についてステップごとに何をすべきか、具体的に提示

セキュリティ担当者に必要なスキル・知識

- 「ITSS＋（セキュリティ領域）」及び「サイバーセキュリティ体制構築・人材確保の手引き」において記載
  「ITSS＋（セキュリティ領域）」で示されているセキュリティに関する分野ごとに、求められる知識・スキルの概観を提示
  また、その詳細については、登録セキスペ試験シラバスとリンクさせて提示
- 知識・スキルのレベルは、主導できるレベル（セキスペ試験レベル）と経営層とコミュニケーションが取れるレベル（情報セキュリティマネジメント試験レベル）と整理
- その他、「ITSS＋（セキュリティ領域）」に含まれる分野と既存の試験、資格を紐づけて整理

サイバーセキュリティ経営ガイドラインVer 3.0

平成27年12月28日策定
令和5年3月24日第3版公表

- サイバーセキュリティ対策に当たっては、経営者がリーダーシップを取ってセキュリティ対策を推進していくことが重要。サイバーセキュリティ対策を推進するため、**経営者を対象としたサイバーセキュリティ経営ガイドラインを策定**。
- ガイドラインにおいては、**経営者が認識すべき３原則**及び**経営者が情報セキュリティ対策を実施する上での責任者（CISO等）に指示すべき１０の重要事項**をまとめている。

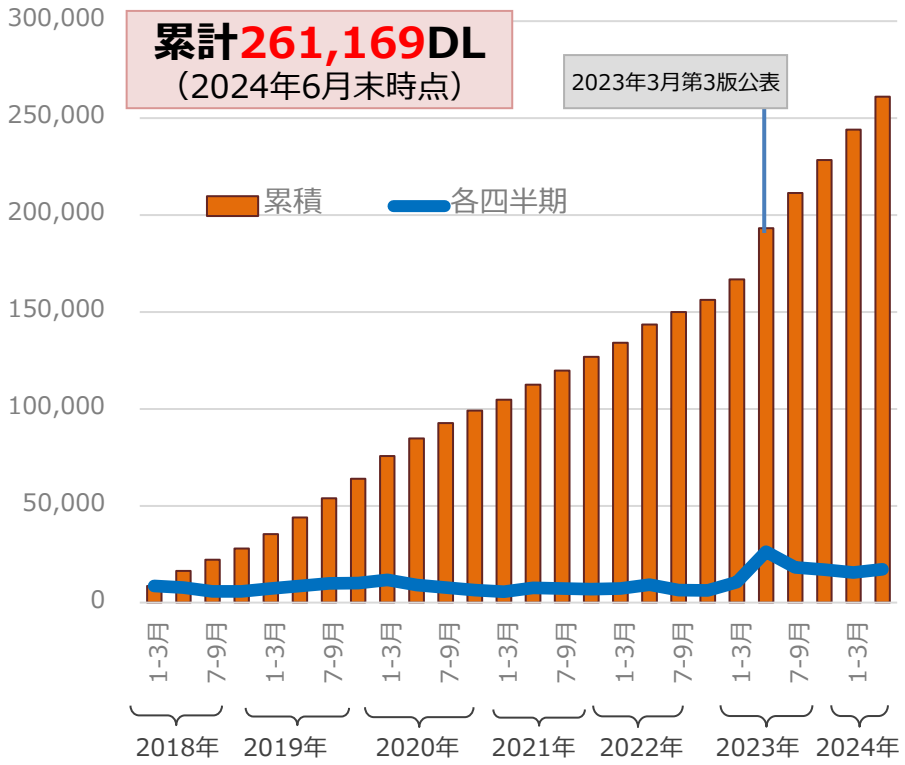
１．経営者が認識すべき３原則

（１）経営者が、**リーダーシップを取って対策**を進めることが必要
（２）自社のみならず、**サプライチェーン全体にわたる対策**への目配り
（３）平時及び緊急時のいずれにおいても、**社内外関係者との積極的なコミュニケーション**が必要

２．経営者がCISO等に指示すべき１０の重要事項

リスク管理体制の構築	**指示１** 組織全体での対応方針の策定 **指示２** 管理体制の構築 **指示３** 予算・人材等のリソース確保
リスクの特定と対策の実装	**指示４** リスクの把握と対応計画の策定 **指示５** リスクに対応するための仕組みの構築 **指示６** PDCAサイクルの実施による継続的改善
インシデントに備えた体制構築	**指示７** 緊急対応体制の整備 **指示８** 事業継続・復旧体制の整備
サプライチェーンセキュリティ	**指示９** サプライチェーン全体の状況把握及び対策
関係者とのコミュニケーション	**指示10** 情報収集、共有及び開示の促進

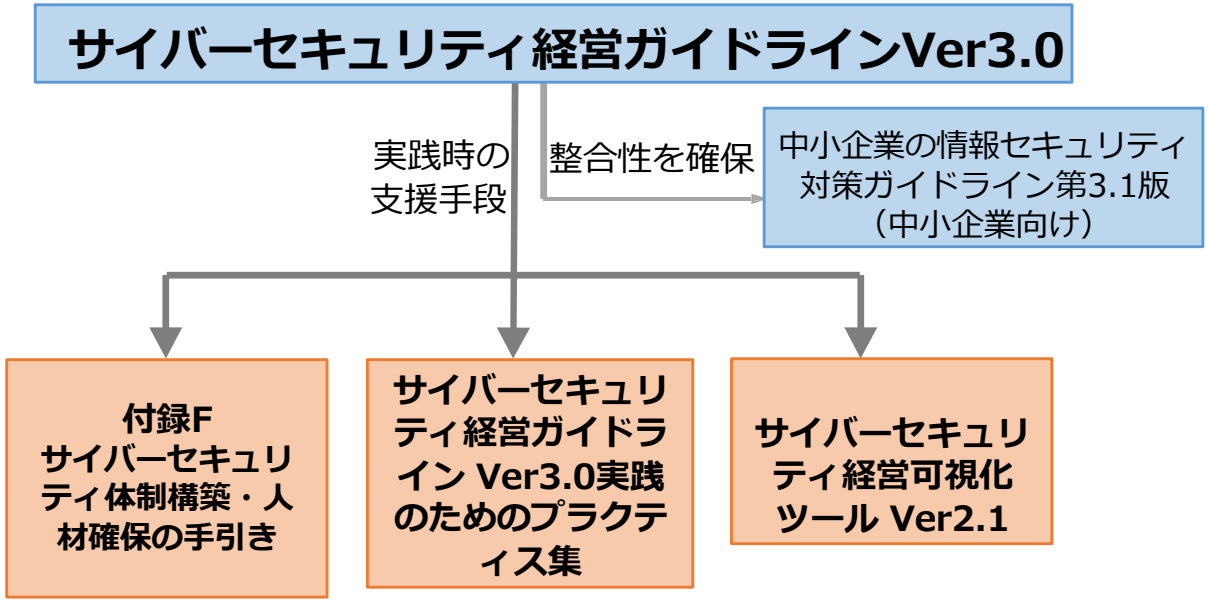
サイバーセキュリティ経営ガイドラインV2.0/V3.0のダウンロード数推移



https://www.meti.go.jp/policy/netsecurity/mng_guide.html

サイバーセキュリティ経営ガイドラインとその他関連文書等との関係性

- 「サイバーセキュリティ経営ガイドライン」を実践する際の参照文書等として、以下のように整理をしている。



資料名	発行年月日	対象読者	内容	URL
サイバーセキュリティ経営ガイドライン Ver 3.0	2023/3/24	経営者、CISO等、セキュリティ担当者	経営者のリーダーシップの下、サイバーセキュリティ対策を推進するためのガイドライン	http://www.meti.go.jp/policy/netsecurity/mn g_guide.html
中小企業の情報セキュリティ対策ガイドライン第3.1版	2023/4/26	経営者、情報管理を統括する方	重要な情報を脅威から保護　するための情報セキュリティ対策ガイドライン	https://www.ipa.go.jp/security/guide/sme/about.html
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	2022/6/15	CISO等、セキュリティ担当者、人材育成担当者	サイバーセキュリティ対策を実施するための組織作りと従事する人材の育成のための手引き書	http://www.meti.go.jp/policy/netsecurity/mn g_guide.html
サイバーセキュリティ経営可視化ツール Ver 2.1	2023/7/28	経営者、CISO等、セキュリティ担当者	セキュリティ対策実践状況の把握や事業リスク評価等に活用するための自己診断ツール	https://www.ipa.go.jp/security/economics/checktool/index.html

サイバーセキュリティ体制構築・人材確保の手引き

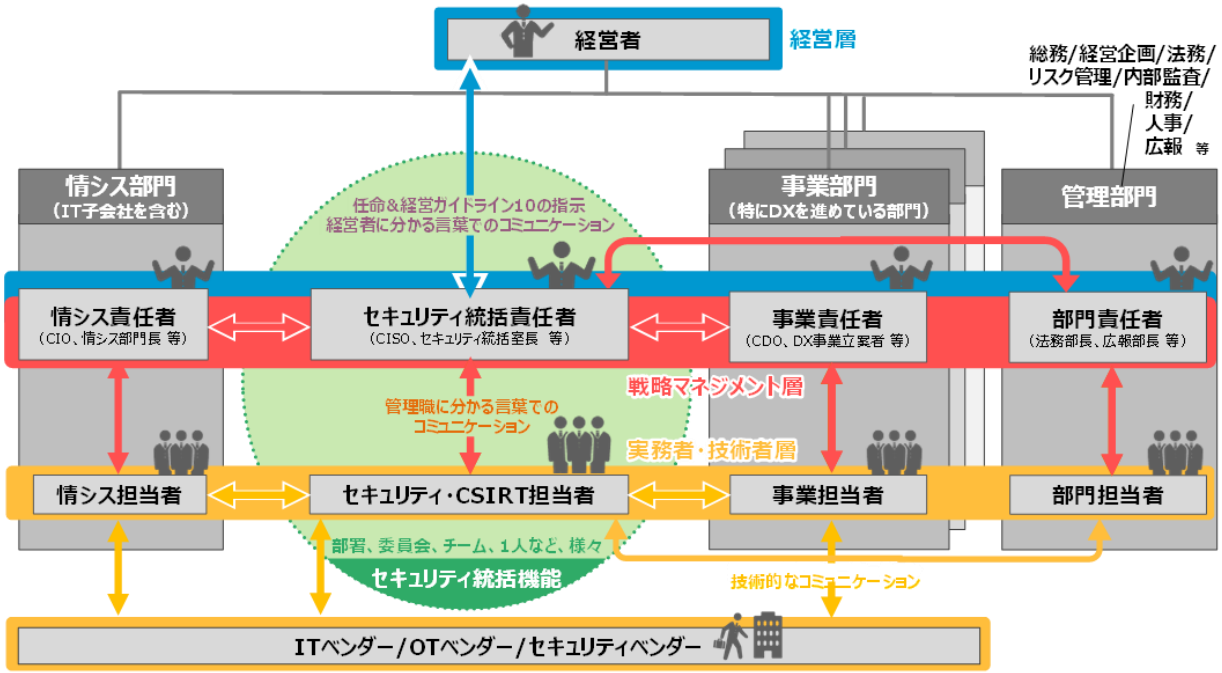
第１回 産業サイバーセキュリティ研究会 ワーキンググループ２
サイバーセキュリティ人材の育成促進に向けた検討会　資料４より抜粋

- 「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 委託先管理	サプライチェーンリスク管理		

※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）

『サイバーセキュリティ経営ガイドラインVer3.0実践のためのプラクティス集』

- サイバーセキュリティ経営ガイドラインの重要10項目を具体的に実践していくに当たり、サイバーセキュリティ経営ガイドライン実践のためのプラクティス集を公開。**実践事例に加え、セキュリティ担当者の日常業務における悩みに対する具体的対応策を提示**。
- **2023年10月、**サイバーセキュリティ経営ガイドラインVer3.0の改訂を踏まえ、**プラクティスの拡充や企業インタビュー調査で得られた事例をミニプラクティスとして追加した第４版を公表**。

＜特徴＞

サイバー攻撃対策やインシデント対応の強化に向けた体制づくりや対策は何から始めるべきか、と考えている経営者やCISO等、セキュリティ担当者を主な読者と想定し、ガイドラインの「重要10項目」を実践する際に参考となる考え方やヒント、実施手順、実践事例を掲載。

【第４版の主な改訂内容】

- 実践例として、「リテラシーにとどまらないプラスセキュリティ教育の実践」「DX推進を支える仕組みづくり」「サプライチェーンでの連携体制の構築」「『情報の共有・公表ガイダンス』に基づくCSIRTと社内外関係者との連携推進」などの事例を追加
- ミニプラクティスとして、クラウドサービスを利用する際のセキュリティ対策の強化や従業員向けのサイバーセキュリティ教育の効果を高めることなどに関する事例を追加

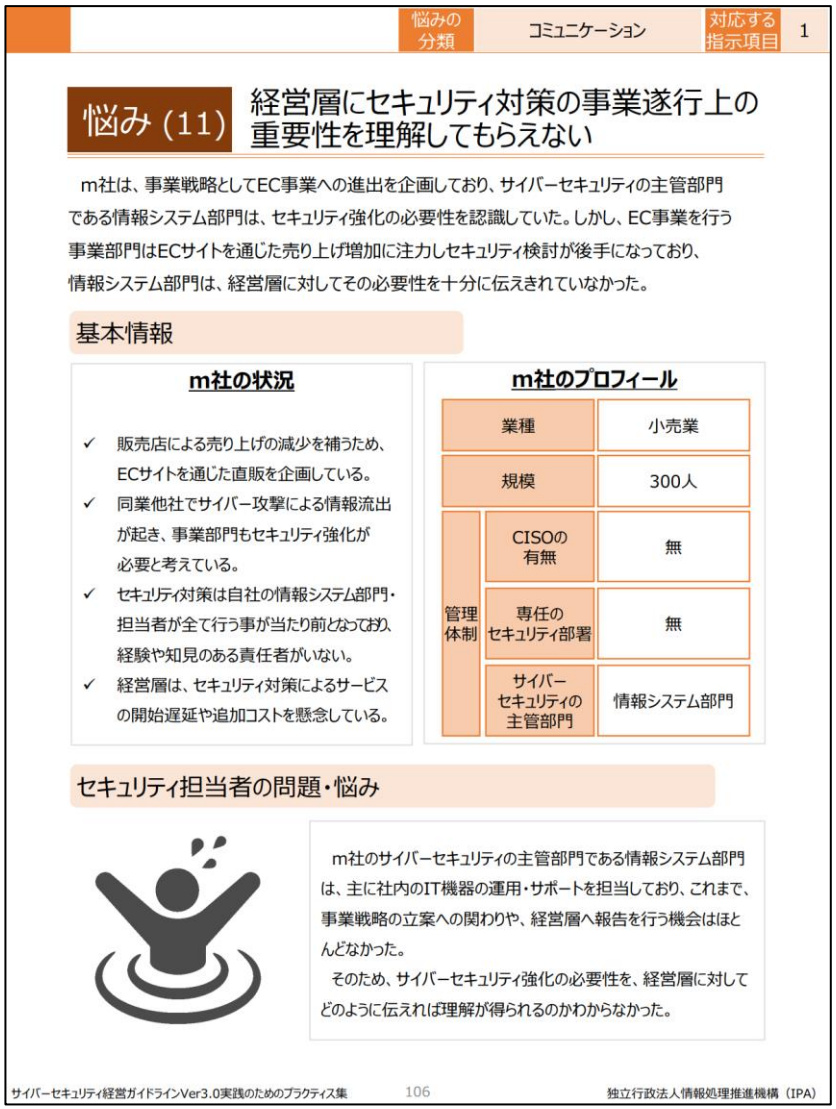
＜構成＞

はじめに
第1章　経営とサイバーセキュリティ
第2章　サイバーセキュリティ経営ガイドライン実践のプラクティス
第3章　セキュリティ担当者の悩みと取組みのプラクティス
ミニプラクティス
付録

https://www.ipa.go.jp/security/economics/hjuojm00000044dc-att/cms_practice_v4.pdf

『サイバーセキュリティ経営ガイドラインVer3.0実践のためのプラクティス集』

- サイバーセキュリティ経営ガイドライン実践のためのプラクティス集においては、企業の業種、規模、管理体制としてCISOの有無、専任のセキュリティ部署の有無、サイバーセキュリティの主管部門の有無を示した上で、悩みと取組を紹介している。



悩みの分類：コミュニケーション　対応する指示項目：1

悩み (11) 経営層にセキュリティ対策の事業遂行上の重要性を理解してもらえない

m社は、事業戦略としてEC事業への進出を企画しており、サイバーセキュリティの主管部門である情報システム部門は、セキュリティ強化の必要性を認識していた。しかし、EC事業を行う事業部門はECサイトを通じた売り上げ増加に注力しセキュリティ検討が後手になっており、情報システム部門は、経営層に対してその必要性を十分に伝えきれていなかった。

基本情報

m社の状況

- ✓ 販売店による売り上げの減少を補うため、ECサイトを通じた直販を企画している。
- ✓ 同業他社でサイバー攻撃による情報流出が起き、事業部門もセキュリティ強化が必要と考えている。
- ✓ セキュリティ対策は自社の情報システム部門・担当者が全て行う事が当たり前となっており、経験や知見のある責任者がいない。
- ✓ 経営層は、セキュリティ対策によるサービスの開始遅延や追加コストを懸念している。

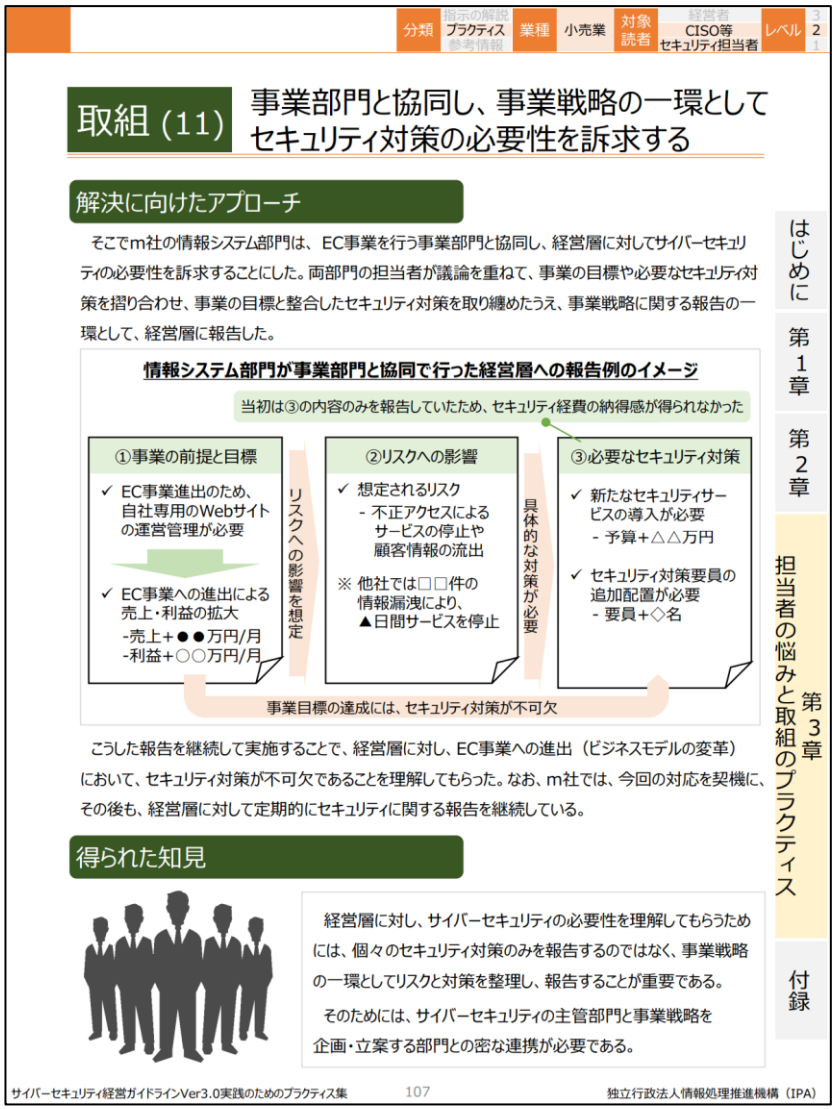
m社のプロフィール

業種		小売業
規模		300人
管理体制	CISOの有無	無
	専任のセキュリティ部署	無
	サイバーセキュリティの主管部門	情報システム部門

セキュリティ担当者の問題・悩み

m社のサイバーセキュリティの主管部門である情報システム部門は、主に社内のIT機器の運用・サポートを担当しており、これまで、事業戦略の立案への関わりや、経営層へ報告を行う機会はほとんどなかった。

そのため、サイバーセキュリティ強化の必要性を、経営層に対してどのように伝えれば理解が得られるのかわからなかった。



分類：プラクティス　業種：小売業　対象読者：経営者 CISO等セキュリティ担当者　レベル：2

取組 (11) 事業部門と協同し、事業戦略の一環としてセキュリティ対策の必要性を訴求する

解決に向けたアプローチ

そこでm社の情報システム部門は、EC事業を行う事業部門と協同し、経営層に対してサイバーセキュリティの必要性を訴求することにした。両部門の担当者が議論を重ねて、事業の目標や必要なセキュリティ対策を摺り合わせ、事業の目標と整合したセキュリティ対策を取り纏めたうえ、事業戦略に関する報告の一環として、経営層に報告した。

情報システム部門が事業部門と協同で行った経営層への報告例のイメージ

こうした報告を継続して実施することで、経営層に対し、EC事業への進出（ビジネスモデルの変革）において、セキュリティ対策が不可欠であることを理解してもらった。なお、m社では、今回の対応を契機に、その後も、経営層に対して定期的にセキュリティに関する報告を継続している。

得られた知見

経営層に対し、サイバーセキュリティの必要性を理解してもらうためには、個々のセキュリティ対策のみを報告するのではなく、事業戦略の一環としてリスクと対策を整理し、報告することが重要である。

そのためには、サイバーセキュリティの主管部門と事業戦略を企画・立案する部門との密な連携が必要である。

中小企業の情報セキュリティ対策ガイドライン　第3.1版

- 情報セキュリティ対策に取り組む際の、(1)経営者が認識し実施すべき指針、（2）社内において対策を実践する際の手順や手法をまとめたものです。経営者編と実践編から構成されており、個人事業主、小規模事業者を含む中小企業（以下「中小企業等」）の利用を想定。

- 中小企業等の経営者や実務担当者が、情報セキュリティ**対策の必要性**を理解し、**情報を安全に管理**するための具体的な手順等を示したガイドライン
- 本編2部と付録より構成
  - 経営者が認識すべき**「3原則」**、経営者がやらなければならない**「重要7項目の取組」**を記載
  - 情報セキュリティ対策の具体的な進め方を分かりやすく説明
  - すぐに使える「情報セキュリティ基本方針」や「情報セキュリティ関連規程」等の**ひな形**を付録
  - **「中小企業のためのセキュリティインシデント対応の手引き」**を追加

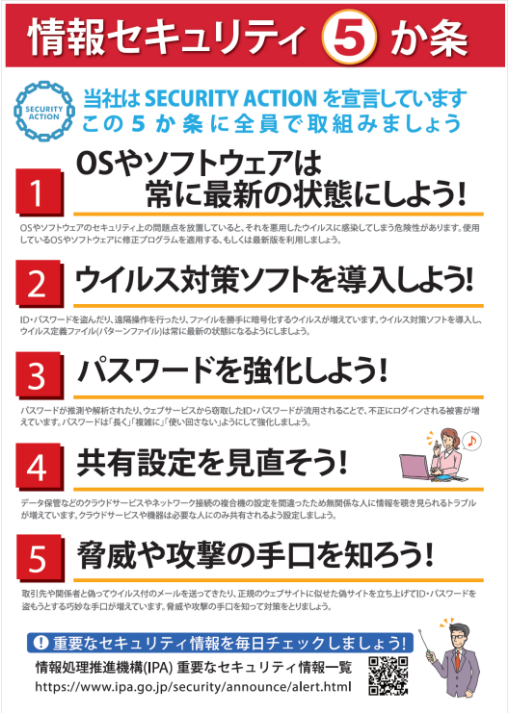
https://www.ipa.go.jp/security/guide/sme/about.html

中小企業の情報セキュリティ対策ガイドライン　実践編

- 実践編においては、４つのステップで具体的にセキュリティ対策の実践について提示。

● できるところから始めて段階的にステップアップ

Step1
できるところから始める



情報セキュリティ５か条

SECURITY ACTION ★一つ星を宣言

Step2
組織的な取り組みを開始する

５分でできる！
情報セキュリティ自社診断

SECURITY ACTION ★★二つ星を宣言

Step3
本格的に取り組む

情報セキュリティ関連規程

Step4
より強固にするための方策

- 情報収集と共有
- ウェブサイトの情報セキュリティ
- クラウドサービスの情報セキュリティ
- 情報セキュリティサービスの活用
- 技術的対作例と活用
- 詳細リスク分析の実施方法

より強固にするため方策

SECURITY ACTION制度

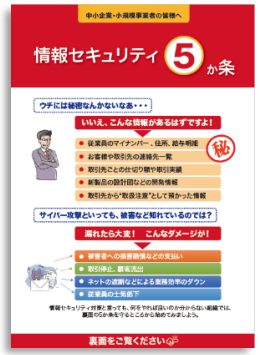
- 中小企業自らが情報セキュリティ対策に取り組むことを**自己宣言**する制度（※）
  - 「中小企業の情報セキュリティ対策ガイドライン」の実践をベースに**２段階の取組目標**を用意
- 本自己宣言は、IT導入補助金等の補助金の要件となっている。

※IPAが各企業等の情報セキュリティ対策状況等を認定する、あるいは認証等を付与する制度ではない

１段階目（一つ星）

●情報セキュリティ５か条に取り組む

★一つ星



【情報セキュリテイ５か条】

- □OSやソフトウェアは常に最新の状態にしよう！
- □ウイルス対策ソフトを導入しよう！
- □パスワードを強化しよう！
- □共有設定を見直そう！
- □脅威や攻撃の手口を知ろう！

2段階目（二つ星）

●情報セキュリティ自社診断を実施
●基本方針を策定

★★二つ星

【基本方針の記載項目例】

- □管理体制の整備
- □法令・ガイドライン等の順守
- □セキュリティ対策の実施
- □継続的改善

など

(SECURITY ACTIONサイト)
https://www.ipa.go.jp/security/security-action/

今後の政策対応の方向性（案）

- 「サイバーセキュリティ経営ガイドライン」や「中小企業の情報セキュリティ対策ガイドライン」によって、企業の経営者に対し、企業内でのセキュリティ人材育成・確保の必要性を訴えてきた。また、「サイバーセキュリティ体制構築・人材確保の手引き」により、セキュリティ人材育成の具体的取組の手順を提示してきた。しかしながら、実態として、**多くの中堅・中小企業でセキュリティ人材が充足されず、対策が進んでいない状況**にある。

- 中堅・中小企業と言っても、売上、従業員規模、業種、情報資産やIT依存度、サプライチェーン上の重要度等が多種多様であるところ、これら企業に対し**一律で対策を求めていくことは現実的ではない**。大まかに大別して、**内部でセキュリティ対策を①専任で推進する人材の確保が可能な企業・目指すべき企業**(※)と**②専任で推進する人材の確保が困難な企業（他の業務との兼任でしか人材の確保が困難な企業）が存在するのではないか。**
  （※）ただし、自社の経営判断によって兼任として確保することを排除するものではない。

- **①専任で推進する人材の確保が可能な企業・目指すべき企業**については、仮に、当該企業が適切にサイバーセキュリティに係るリスクを理解し、企業内部でセキュリティ人材を確保・育成することの必要性を理解したとしても、**既存のどの成果物を参照すればよいか分からない、または具体的にどのように取組を実践すればよいかが分からず**、**人材育成・確保に取り組む方法等についての十分な理解が浸透していない可能性が考えられる**。

- そこで、①**専任で推進する人材の確保が可能な企業・目指すべき企業**については 、「サイバーセキュリティ体制構築・人材確保の手引き」に示される「セキュリティ統括機能」の考え方をどのように適用できるかについて検討し、実践的指針を示した上で、当該機能**を遂行するために必要な**内部人材に求められる**スキル・知識の水準**やその**考え方を提示する**ことを検討したい。

- **②専任で推進する人材の確保が困難な企業**についても、「セキュリティ統括機能」の考え方を適用し、セキュリティ人材を確保すべきであるが、人的・金銭的リソースの観点から、現実的には困難であると考えられる。そこで、当該企業に対しては、**スキルや知識の有無を問わず、兼任であっても、まずは内部にセキュリティ担当者をアサインする必要性を示すとともに**、そのような立場を前提に、当該企業が「**行うべき業務**」や「**最低限知っておくべき知識**」、「**セキュリティ対策の考え方**」**を示すこと**（**外部人材の活用の在り方を提示**することも含む。）に重点を置くこととしてはどうか。

- 上述した成果物が広く活用されるように、既存施策との連携などの政策的手段を検討することとしたい。

内部でセキュリティ対策を専任で推進する人材の確保が可能・目指すべき企業/兼任であっても推進する人材の確保を目指すべき企業のイメージ

- 内部でセキュリティ対策を①専任で推進する人材の確保が可能な企業・目指すべき企業と②兼任であっても推進する人材の確保を目指すべき企業について、**一概に従業員数や売上等の要素で線引きすることは困難**である。他方で、具体的なイメージを持って議論することが重要であるため、本検討会においては、以下のような想定で整理したい。

①専任で推進する人材の確保が可能な企業・目指すべき企業

- **組織としてある程度の大きさがあり、セキュリティ体制の構築、人材育成が組織のセキュリティ向上に有効な企業**。
- サイバー事案によって、**サプライチェーンへの影響が大きいと考えられる企業**。

例：製造業、従業員規模は２００名程度、資本金１億円程度。
本社工場以外に複数の分工場を有する。
社内にCSIRTは無いが、発注元企業側はCSIRTを配置している
生産管理情報として以下を扱う製造業である
特定社会基盤事業者の設備評価対象（経済安保推進法関連）
重要経済安保情報を扱う事業者（経済安保推進法関連）
社内に営業秘密「生産に関わる製造レシピ情報」を保有

②兼任であっても推進する人材の確保を目指すべき企業

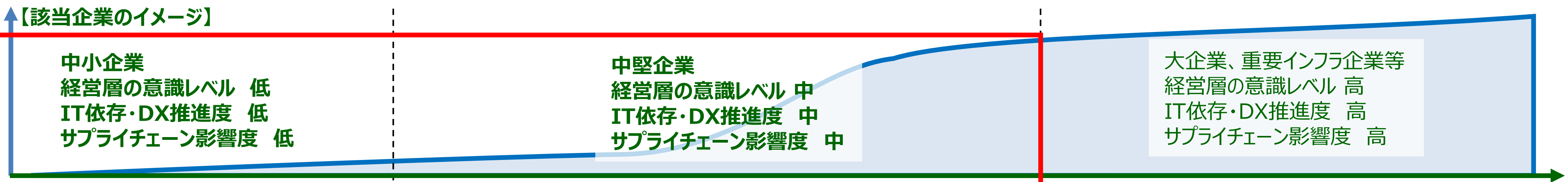
- 現状の業務遂行に手一杯であり、**新たな業務負担を許容するリソースがない**。
- 能力の有無を問わず、兼任であっても、まずは社内にセキュリティ担当者をアサインし、情報セキュリティ５か条のような基本的対策を実施することが優先。
- サイバー事案によって、**サプライチェーンへの影響が小さいと考えられる企業。**

例：建設業、従業員２０名程度、資本金２０００万円程度。
事務所が一つ。パソコンは５台程度
社員の多くが現場業務、もしくは営業と現場業務を兼務する。
事務員が３名程度

セキュリティ統括機能と人材関係整理

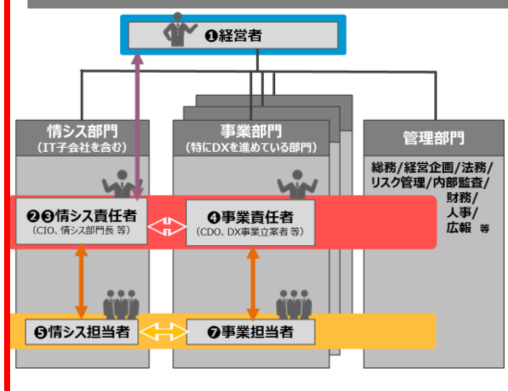
第4回 産業サイバーセキュリティ研究会 ワーキンググループ2
資料3より抜粋・加工

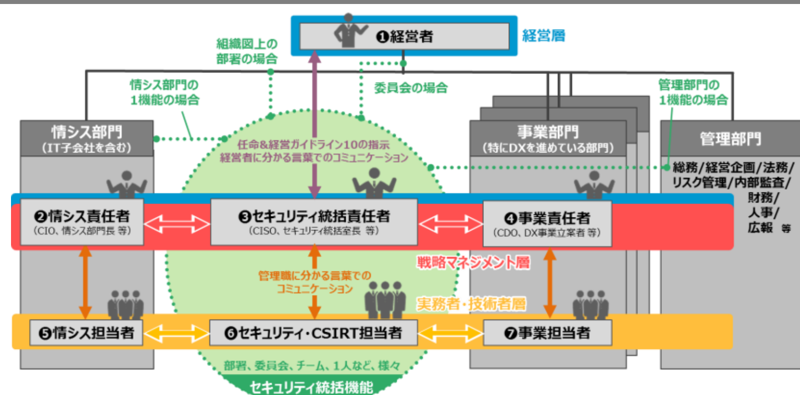
- セキュリティ体制・人材と、セキュリティ成熟度の間には、概ね以下のような関係が認められるのではないか。

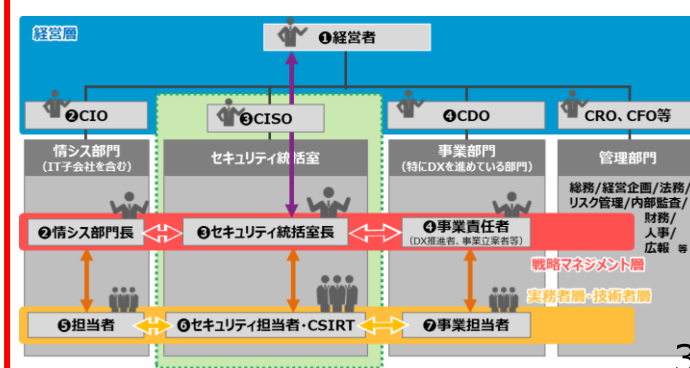


中小企業	中堅企業	大企業、重要インフラ企業等
CSIRT機能の設置・確立状況		
△ (→ 窓口の設置を目指す)	○ (→ CSIRTの設置を目指す)	◎ (→ CSIRT機能の確立を目指す)
セキュリティ統括責任者（CISO等）の設置状況		
△ (→ 兼務による担当者設置を目指す)	○ (→ 専任による部課長級の設置を目指す)	◎ (→ 役員級のCISOの設置を目指す)
セキュリティ統括機能の設置・確立状況		
×	○ (→ 設置を目指す)	◎ (→ 機能の確立を目指す)
事業部門・管理部門のセキュリティ意識・能力		
×	△ (→ セキュリティ統括機能との連携を目指す)	○ (→ 事業部門・管理部門の意識・能力の向上を目指す)

体制のイメージ







中堅・中小企業における「セキュリティ統括機能」の有効性

- サイバーセキュリティ経営ガイドラインの付録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、企業内に「セキュリティ統括機能」を設置することの有効性が示されているが、この「セキュリティ統括機能」は、中堅・中小企業にとっても必要な機能であるか検討したい。

セキュリティ統括機能が担うタスク

① 経営層（CISO等）が行う意思決定等の補佐（図中「方針策定」） CISOや経営層が担う業務のうち、一定の専門的な知見が必要となるものについて支援し、意思決定や判断の補佐を行う。

② 自らが主体となって実施する実務（図中「実務」） 組織横断的対応が必要な業務を自らが主体となって実施する。

③ 他部署が主体となって実施する実務の支援（図中「支援」「実務支援」） 事業部門や管理部門が主体となって行う実務を、一定の専門的な知見を用いて支援する。

内部でセキュリティ対策を専任で推進する人材の確保が可能・目指すべき企業の例示①

- 「セキュリティ統括機能」の有効性を議論すべく、製造業における例を提示。従業員数の違い、専任のセキュリティ部署の有無についての違いが見られるが、**IoT機器の利用や機密性の高い情報の保有等**の要素を鑑みれば、「セキュリティ統括機能」としての役割を担う専任人材の配置を目指すべきではないか。

業種：製造業
規模：300人
CISOの有無：有 (CIOが兼任)
専任のセキュリティ部署：無
サイバーセキュリティの主管部署：情報システム部門

✓ 製品製造ラインの一部にIoT機器を導入している。
✓ 通常、製造部門がシステムを導入する際には、情報システム部門が関与するルールである。
✓ 製造部門で製造に使用する制御システムは通常外部ネットワークに接続しない。

業種：製造業
規模：2,000人
CISOの有無：有 （IT担当取締役が兼任)
専任のセキュリティ部署：有
サイバーセキュリティの主管部署：サイバーセキュリティ部門

✓ 全国各地に営業所を構え、各拠点で機密性の高い情報を保有している。
✓ 全社セキュリティ委員会を設置し、 各拠点のセキュリティ責任者・担当者と逐次情報連携を行っている。
✓ 本社にて各拠点でのサイバーセキュリティ管理状況の実態を正しく把握できているか自信がない。

内部でセキュリティ対策を専任で推進する人材の確保が可能・目指すべき企業の例示②

- 製造業に限らず、**流通業や通信業などインフラを支えるような業種であり、サプライチェーンに対する影響が大きい企業**については、従業員規模の大小を問わず、「セキュリティ統括機能」としての役割を担う専任人材の配置を目指すべきではないか。

業種：流通業
規模：600名程度
CISOの有無：有 (コンプライアンス担当役員が兼任)
専任のセキュリティ部署：無
サイバーセキュリティの主管部署：情報システム部門

✓ 情報保護の観点からコンプライアンス部がセキュリティリスクを管理しているが、情報システムに対する技術的な実装が多いサイバーセキュリティ対策は、暗黙のうちにIT統括部が担当している。

業種：通信業
規模： 1,800人
CISOの有無：有 (コンプライアンス担当役員が兼任)
専任のセキュリティ部署：有
サイバーセキュリティの主管部署：サイバーセキュリティ部門

✓ 仮想現実（VR）を利用したゲームやSNS、非代替性トークン（NFT）応用など、最新技術を活用したサービスの提供に積極的であり、将来的にはメタバースでの事業展開も視野に入れて積極的な研究開発を行っている。

本日議論いただきたい点

本日議論いただきたい点①（登録セキスペの活用及び制度の見直し）

【果たすべき役割】

- セキュリティ人材は、ITSS＋（セキュリティ領域）において、「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」の各分野を担う人材と定義されており、個々人によって扱う分野も多種多様である。
- 一方、昨今のサイバー空間を取り巻く情勢を鑑みれば、企業内部において、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の必要性が増加している。
- こうした状況において、**登録セキスペについても**、「企業等の外部から専門的なセキュリティ対策を実施できる人材」としてのみならず、**「企業等の内部に置かれるべき人材」としての役割を果たす期待が高まっているのではないか**。
- また、「企業等の内部に置かれるべき人材」と「企業等の外部から専門的なセキュリティ対策を実施できる人材」とで、**必要な知識・スキルはどのように異なるか**。
- 例えば「企業等の内部に置かれるべき人材」にとっては、「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」が持ち合わせているスキル（マルウェアの解析等）までは必ずしも求められてはいないのではないか。その上で、**企業内部セキュリティ人材にとっての資格更新の在り方について、現在の講習体系とは異なる方法を取る余地はあるか**。
- また、こうした議論の前提となる**情報処理安全確保支援士試験の在り方（試験科目・試験制度等）はどうあるべきか**。

本日議論いただきたい点①（登録セキスペの活用及び制度の見直し）

【実務経験等を通じた更新負担軽減】

- 兼業等を通じた中小企業等の支援、企業内部におけるセキュリティ対策の実施等を促進する観点から、更新費用負担の軽減のために、既存の講習体系は維持しつつも、**実務経験等を通じた更新講習受講義務の軽減（講習のみなし受講）をするのはどうか**。
- **講習のみなし受講については**、登録セキスペの責務や倫理等の国家資格として全登録セキスペが共通的に受講すべき内容であるオンライン講習は対象外とし、**特定講習又は実践講習のみを対象とするのはどうか**。また、講習を提供する事業者や講習内容は多種多様であること、運用との費用対効果等を踏まえると、**講習によって得られる知識・能力と同等の学習及び実務経験を一定以上行った者については、特定講習又は実践講習をすべて受講したとみなすこととするのはどうか**。
- **実務経験等の基準の設定に際して、**当該基準の更新及び運用のコスト、登録セキスペとして望ましい活動（兼業等を通じた中小企業等の支援、企業内部におけるセキュリティ対策の実施等）を促進するなどの観点から、**どのような方策が現実的と考えられるか**。
- **実務経験等の基準については、**具体的かつ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が、**具体的にどのような学習や実務経験等が考えられるか**。

本日議論いただきたい点①（登録セキスペの活用及び制度の見直し）

【活用促進】

- ユーザー企業における登録セキスペの活用を進めるにあたって、**規模、業種、情報資産・IT依存度、サプライチェーン上の重要度等が様々であることを踏まえると、企業ごとに登録セキスペの活用方法は異なるのではないか**。例えば、リソース等の観点で、自社に登録セキスペを配置することが困難な企業については、登録セキスペを外部人材として活用していくことが必要ではないか。
- 「サプライチェーン強化に向けたセキュリティ対策評価制度」との連動や、支援機関（商工会議所等）と連携した登録セキスペアクティブリストの活用を通じた企業支援、IT関連製品のセキュリティ機能の適切性・確実性等を確認するための第三者評価を行う人材としての活用等を検討しているが、**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**。

【その他】

- すべての登録セキスペを対象として更新コストを低減するための方策（例：オンライン講習（責務や倫理等に係る内容の講習）の簡素化・回数見直し等）は必要であると考えられるか。

本日議論いただきたい点②

（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・中小企業と言っても、規模、業種、情報資産・IT依存度、サプライチェーン上の重要度等が様々であり、これら企業に対し一律で対策を求めていくことは現実的ではない。
- **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を育成・確保するとの目的に照らした際に、内部でセキリュティ対策を①専任で推進する人材の確保が可能な企業・目指すべき企業と②兼任であっても推進する人材の確保を目指すべき企業それぞれに対して効果的な施策は異なるのではないか**。
- **①専任で推進する人材の確保が可能な企業・目指すべき企業**については、サイバーセキュリティ対策の必要性を理解していることを前提とすれば、次の段階として、**内部でセキュリティ対策を推進するための人材を確保・育成するために参考となる具体的方法の提示が必要**。この点、**既存の成果物ではどのような点に不足があるか（どのような成果物があると良いか）　。**
  - 内部でセキュリティ対策を推進する者を育成・確保するにあたって、既存の成果物で示される事例等には十分に具体性・網羅性があり、①の対象となる企業にとって実践可能な取組手法が示されているか。
  - 「サイバーセキュリティ体制構築・人材確保の手引き」で示される「セキュリティ統括機能」は、①の対象となる企業にとって、適切な考え方（そのまま適用できる考え方）であるか。
  - ①の対象となるいくつかの企業サンプルを示し、それぞれの企業サンプルについて「セキュリティ統括機能」の考え方を適用した体制構築の在り方や人材確保の方法(How-to)をケーススタディ的に示すことが有効ではないか。

本日議論いただきたい点②

（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）

- **②兼任であっても推進する人材の確保を目指すべき企業**については、**人的・金銭的リソースの確保に限界があることを前提に当該企業がセキュリティ対策の観点から行うべき業務・当該業務を遂行するために必要な役割を明確化することが必要ではないか**。また、当該業務を遂行するには、まずは能力や兼務に関わらず、セキュリティ担当者をアサインした上で、**外部人材も活用することが不可欠**であるため、（人材政策的アプローチとして）**外部人材の活用のあり方**（How-to）**を提示することも有効ではないか**。その観点から、**既存の成果物ではどのような点に不足があるか**（**どのような成果物があると良いか**）**。**
  - 中小企業の情報セキュリティ対策ガイドラインにおいて、実践すべき業務、外部人材の活用について示しているが、十分に具体性・網羅性があり、実現可能な取組の手法を示しているか。
  - （仮に外部人材の水準として登録セキスペも有用である場合には、）登録セキスペの活用（アクティブリストの活用等）推進施策とも連動させる必要があるのではないか。

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３回	令和６年９月～11月	
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）