経済産業省

第11回
産業サイバーセキュリティ研究会
ＷＧ２（地域・中小企業支援）
事務局説明資料

令和７年４月15日

商務情報政策局　サイバーセキュリティ課

産業サイバーセキュリティ研究会の体制及び関連会議の実績

産業サイバーセキュリティ研究会

第１回：平成29年12月27日		
第２回：平成30年　5月30日	アクションプラン（４つの柱）を提示	
第３回：平成31年　4月19日	アクションプランを加速化する３つの指針を提示	
第４回：令和　2年　4月17日	（電話開催）	産業界へのメッセージを発信
第５回：令和　2年　6月30日	サイバーセキュリティ強化運動の展開	
第６回：令和　3年　4月　2日	アクションプランの持続的発展と、新たな課題へのチャレンジへ	
第７回：令和　4年　4月11日	産業界へのメッセージを発信	
第８回：令和　6年　4月　5日	新たなサイバーセキュリティ政策の方向性を提示	

＜構成員＞　※2025年5月開催時点

伊藤　栄作	三菱重工業株式会社取締役社長
遠藤　信博	日本経済団体連合会サイバーセキュリティ委員長、 日本電気株式会社特別顧問
片野坂真哉	日本情報システム・ユーザー協会会長、 ANAホールディングス株式会社　取締役会長
澤田　純	日本電信電話株式会社取締役会長
寺田　航平	経済同友会副代表幹事、 寺田倉庫株式会社　代表取締役社長
東原　敏昭	株式会社日立製作所取締役会長　代表執行役
船橋　洋一	公益財団法人　国際文化会館 グローバル・カウンシル チェアマン
村井　純(座長)	慶應義塾大学教授
渡辺　佳英	日本商工会議所特別顧問、大崎電気工業株式会社取締役会長

＜オブザーバー＞

NISC、サイバー安全保障体制制度準備室、警察庁、金融庁、総務省、外務省、
文部科学省、厚生労働省、農林水産省、国土交通省、防衛省、デジタル庁

WG１（実効性強化・国際連携）

第１回：平成30年　2月　7日
第２回：平成30年　3月29日
第３回：平成30年　8月　3日
第４回：平成30年12月25日
第５回：平成31年　4月　4日
第６回：令和　2年　3月（書面開催）
第７回：令和　2年10月（書面開催）
第８回：令和　3年　3月15日
第９回：令和　4年　4月　4日
第10回：令和 6年　3月14日
第11回：令和 7年　4月14日

- ガイドライン等の実効性強化
- 国際的な制度調和に向けた連携

WG２（地域・中小企業支援）

第１回：平成30年　3月16日
第２回：平成30年　5月22日
第３回：平成30年11月　9日
第４回：平成31年　3月29日
第５回：令和　2年　1月15日
第６回：令和 2年8月25日
第７回：令和 3年2月18日
第８回：令和 4年3月23日
第９回：令和 5年3月27日
第10回：令和6年3月25日
第11回：令和7年4月15日

- 地域・中小企業等における対策支援

WG３（産業振興・人材育成）

第１回：平成30年4月　4日
第２回：平成30年8月　9日
第３回：平成31年1月28日
第４回：令和 元年8月　2日
第５回：令和2年3月（書面開催）
第６回：令和3年3月10日
第７回：令和4年4月　6日
第８回：令和6年4月　3日

- セキュリティ産業振興、研究開発
- 人材育成・確保

＜新たなサイバーセキュリティ政策の全体像及び今後の方向性＞

1．サプライチェーン全体での対策強化
2．セキュア・バイ・デザインの実践
3．政府全体でのサイバーセキュリティ対応体制の強化
4．サイバーセキュリティ供給能力の強化

目次

１．サイバーセキュリティを巡る状況

- 最近国内外で発生した主な事案
- 情報セキュリティ10大脅威の10年間の変遷（2016～2025)
- 中小企業に対するサイバー攻撃の現状
- 中小企業のセキュリティ対策投資に対する現状
- セキュリティ人材 リソース不足の状況
- ガイドライン・各種施策の普及状況

最近国内外で発生した主な事案

①機微技術情報等の窃取

- 2019年以降、中国の関与が疑われるグループ「MirrorFace」による、**日本の安全保障や先端技術に係る情報窃取を目的とした攻撃キャンペーン**が実行されている。（2025年1月 警察庁及びNISCが注意喚起を発出）
- 2024年後半、中国背景と指摘されるグループ「Salt Typhoon」による、米国の通信事業者のネットワークに侵入して**政府関係者等の通話記録等、安全保障に関する情報等の窃取**を狙うような活動が報告されている。

②金銭等資産の窃取

- 2024年5月、北朝鮮を背景とする攻撃グループ「TraderTraitor」が、**ソーシャルエンジニアリング等の手法を用いて**、㈱DMM Bitcoinから**約482億円相当の暗号資産を窃取**。（2024年12月 警察庁、NISC及び金融庁が注意喚起を発出）

③事業活動の停止

- 2024年6月、㈱KADOKAWAが**ランサムウェアを含む大規模サイバー攻撃を受け、Webサービス等が停止**。大量の個人情報や企業情報が漏えいしたうえ、SNS等を通じて拡散される二次被害も発生。

④重要インフラの機能停止等

- 2024年12月～2025年１月の年末年始にかけて、航空事業者、金融機関、通信事業者等が**相次いでDDoS攻撃を受け、サービスの一時停止**等の被害が発生。（2025年2月 NISCが注意喚起を発出）
- 2024年2月、米国政府機関（CISA、NSA、FBI等）が、ファイブアイズ諸国の関係機関と合同で、中国を背景とするグループ「Volt Typhoon」による米国の重要インフラを標的とした活動について注意喚起。同グループは、**有事の際に重要インフラに対するサイバー攻撃を行うため、事前に重要インフラ事業者等のネットワークへのアクセス権限を確保してOT機器に対する侵害を可能としている**旨が指摘されている。

情報セキュリティ10大脅威の10年間の変遷（2016～2025)

- 「ランサムウェアによる被害」と「サプライチェーンの弱点を悪用した攻撃」はここ数年上位を占めている状況であり、WG2において中小企業対策の議論をより一層深耕させて、対策の検討を進めていかなければならない。

脅威の種類		順位の変遷									
		2025	2024	2023	2022	2021	2020	2019	2018	2017	2016
1	ランサムウェアによる被害	1	1	1	1	1	5	3	2	2	7
2	サプライチェーンの弱点を悪用した攻撃	2	2	2	3	4	4	4	-	-	-
3	システムの脆弱性を突いた攻撃	3	7	8	6	10	-	9	4	-	6
4	内部不正による情報漏えい等	4	3	4	5	6	2	5	8	5	2
5	機密情報を狙った標的型攻撃	5	4	3	2	2	1	1	1	1	1
6	リモートワーク等の環境や仕組みを狙った攻撃	6	9	5	4	3	-	-	-	-	-
7	地政学リスクに起因するサイバー攻撃	7	-	-	-	-	-	-	-	-	-
8	分散型サービス妨害攻撃（DDoS攻撃）	8	-	-	-	-	10	6	9	4	4
9	ビジネスメール詐欺	9	8	7	8	5	3	2	3	-	-
10	不注意による情報漏えい等の被害	10	6	9	10	9	7	10	-	-	10

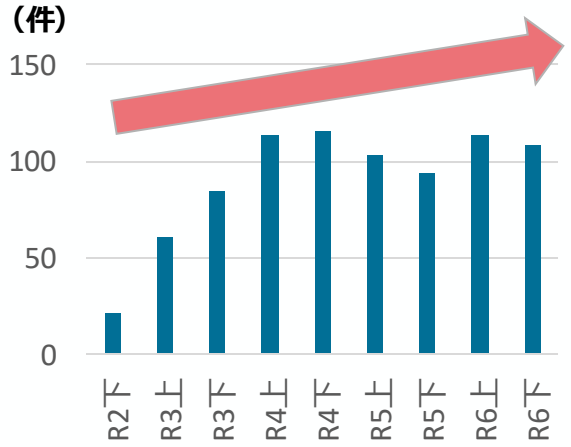
中小企業に対するサイバー攻撃の現状

- 近年、大企業を標的としたサイバー攻撃のみならず、サプライチェーン全体の中で対策が相対的に遅れている中小企業を対象とするサイバー攻撃により、**中小企業自身**及びその**取引先である大企業等への被害が顕在化**している。
- 特に**中小企業に対するサイバー攻撃が増加しており、**警察庁公表資料によると、令和6年におけるランサムウェア被害件数を令和５年と比較すると、大企業の被害件数が減少する一方、**中小企業の被害件数は37%増加している。**
- また、**サイバー攻撃被害に遭った中小企業の７割が、サイバーインシデントにより取引先にまで影響を及ぼしている。**

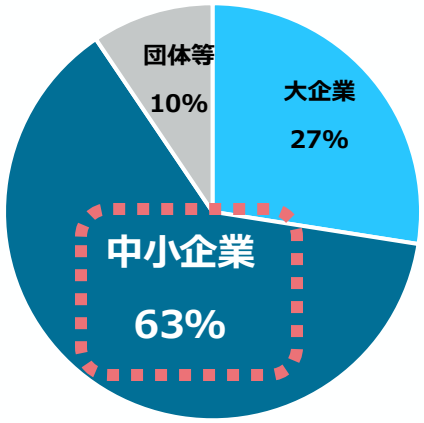
中小企業に対するランサムウェア攻撃が増加

- サイバー被害（ランサムウェア被害件数）は**高止まりしている。**
- 被害件数222件の内訳は、大企業が61件（26%）に対して、**中小企業は140件（63%）と6割を占める。**

企業・団体等における ランサムウェア被害の報告件数



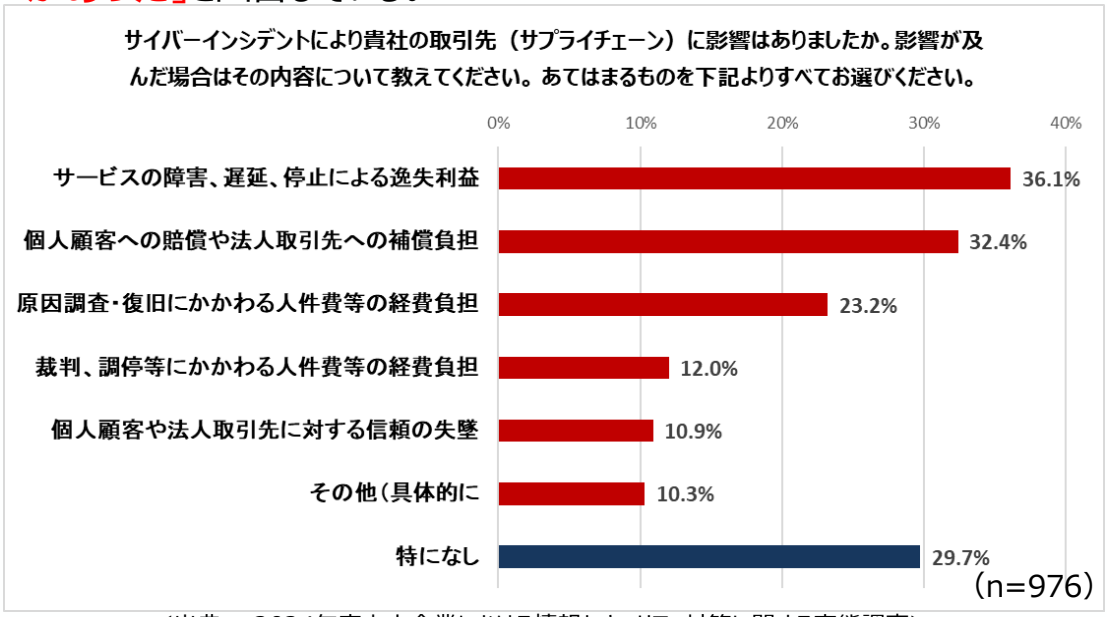
ランサムウェア被害企業等の 規模別件数



<出典：令和6年におけるサイバー空間をめぐる脅威の情勢等について>

取引先等を経由したサイバー攻撃被害の経験

- サイバーインシデントの被害を受けたと回答した企業（n=976）のうち、**約7割（70.3%）が「サイバーインシデントにより取引先に 影響があった」**と回答している。

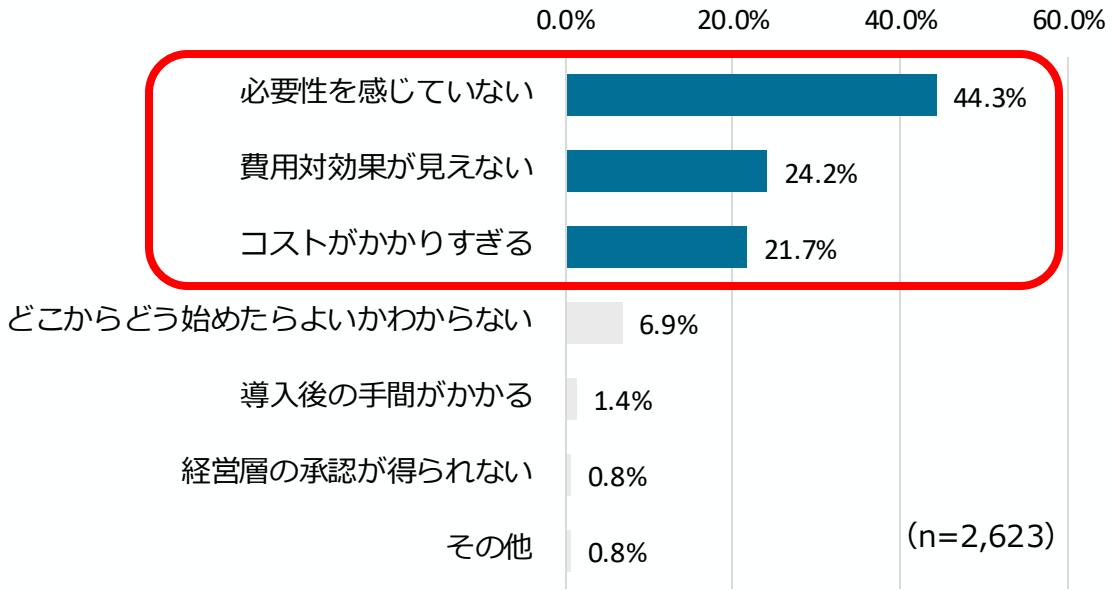


<出典： 2024年度中小企業における情報セキュリティ対策に関する実態調査>

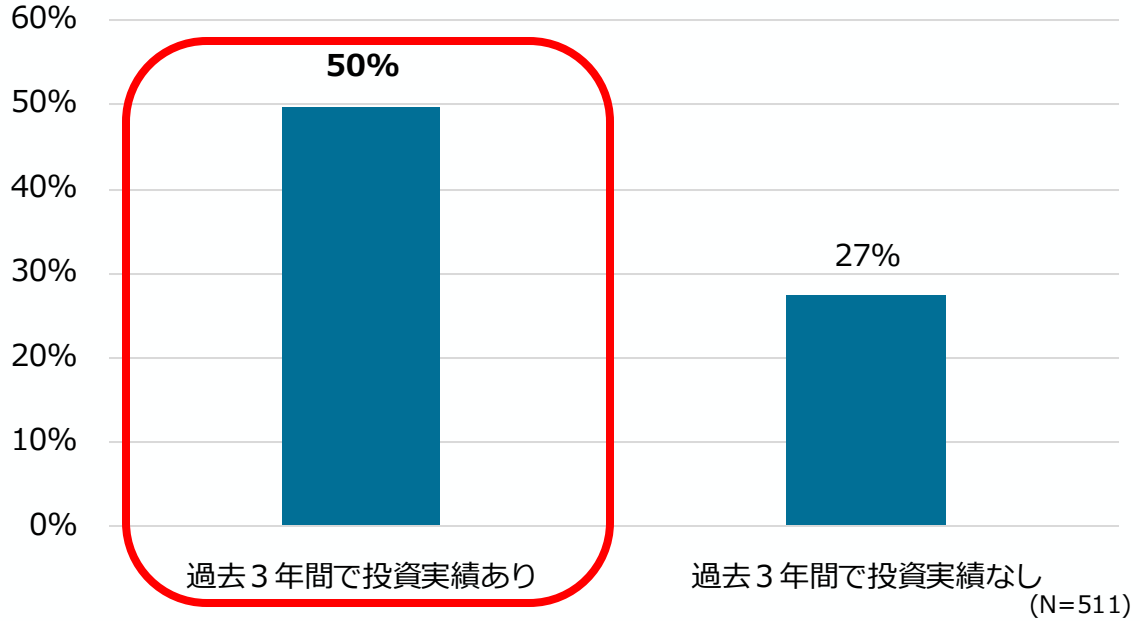
中小企業のセキュリティ対策投資に対する現状

- IPAが2024年度に行った中小企業実態調査では、中小企業が情報セキュリティ投資を行わなかった理由として、**４割の企業が「必要性を感じない」、2割が「費用対効果が見えない」、「コストがかかりすぎる」**と回答。
- 他方で、**サイバーセキュリティ対策投資をより行っている中小企業等の方が、取引につながったと考える割合が高い。**
- 引き続き、**中小企業への普及・啓発を促進し、中小企業にセキュリティ対策の必要性を訴えていくとともに、「サイバーセキュリティお助け隊サービス」など低コストでも実施できる対策の導入を促進する必要がある。**

2024年度中小企業における情報セキュリティ対策に関する実態調査



セキュリティ対策によって取引につながったと考える企業の割合



出典：独立行政法人情報処理推進機構「2024年度 中小企業における情報セキュリティ対策に関する実態調査」を基に経済産業省作成

セキュリティ人材 リソース不足の状況

- 令和５年の調査（2024年版中小企業白書）においても、**第３段階（デジタル化による業務効率化やデータ分析に取り組んでいる状態）の中小企業のうちセキュリティ対策の強化に取り組んでいる企業は46.2%**であるなど、中小企業のセキュリティ対策状況は低い水準となっており、更なるセキュリティ対策の向上が必要。
- また、NRIセキュアの調査によると、日本企業は**9割がセキュリティ対策人材が「不足している」**と回答しているが、**セキュリティ人材不足を補うために人材確保の施策を実施している企業は12.5%**であるなど、セキュリティ人材が育成されていない実態がある。

ＤＸに向けた取組内容(取組状況別)(上位５項目を抜粋)

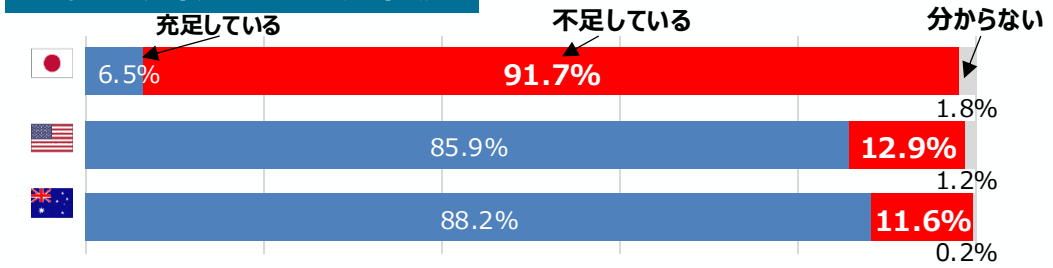
	段階１ (n=1,637)	段階２ (n=1,877)	段階３ (n=1,429)	段階４ (n=366)
紙書類の電子化・ペーパレス化	21.4%	63.8%	79.1%	79.8%
自社ホームページの作成	25.2%	55.3%	70.3%	77.9%
web会議・ビジネスチャットなどのコミュニケーションツール導入	11.4%	41.7%	64.9%	78.7%
セキュリティ対策の強化	8.2%	26.3%	46.2%	66.1%
クラウドサービスの活用	7.3%	27.2%	45.6%	65.6%

段階４	デジタル化によるビジネスモデルの変革や競争力強化に取り組んでいる状態 （例）システム上で蓄積したデータを活用して販路拡大、新商品開発を実践している
段階３	デジタル化による業務効率化やデータ分析に取り組んでいる状態 （例）売上・顧客情報や在庫情報などをシステムで管理しながら、業務フローの見直しを行っている
段階２	アナログな状況からデジタルツールを利用した業務環境に移行している状態 （例）電子メールの利用や会計業務における電子処理など、業務でデジタルツールを利用している
段階１	紙や口頭による業務が中心で、デジタル化が図られていない状態

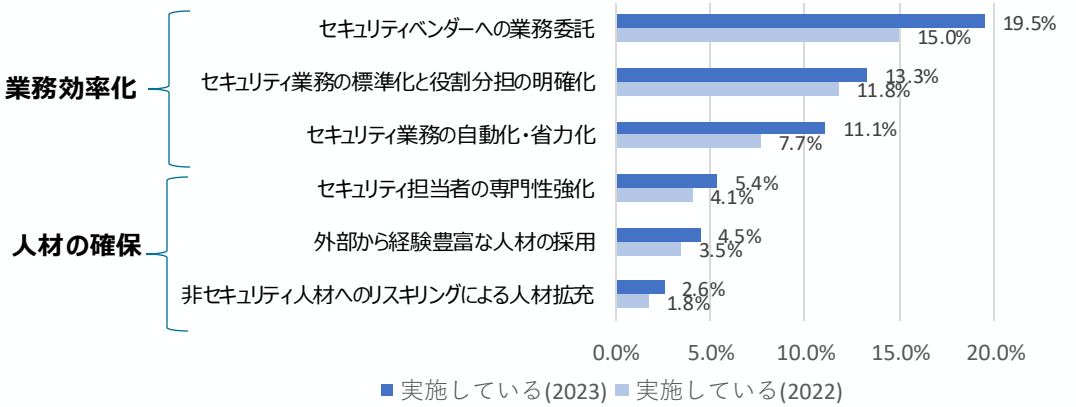
- 第２段階（アナログな状況からデジタルツールを利用した業務環境に移行している）の企業のうちセキュリティ対策に投資している企業は26.3%、第３段階（デジタル化による業務効率化やデータ分析に取り組んでいる状態）の企業のうちセキュリティ対策に投資している企業は46.2%と、中小企業のセキュリティ対策取組状況は低い水準となっており、更なる取組状況の向上が必要である。

出典：2024年版　中小企業白書

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



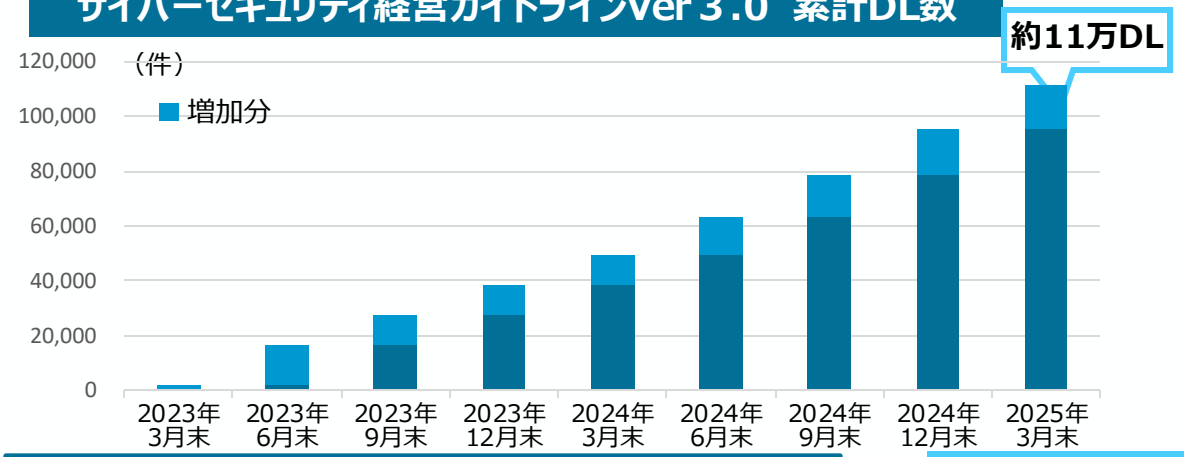
- 実施率が最も高い業務委託でも回答が２割弱に留まっている理由として、セキュリティ関連予算の不足、現場が常時繁忙で検討や実行の時間が取れないことが考えられる。

出典：NRI セキュア　企業における情報セキュリティ実態調査2023

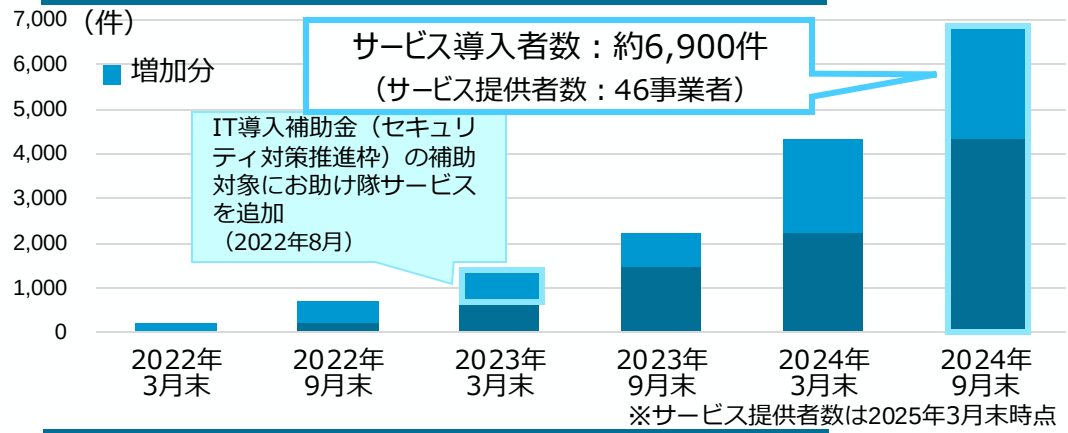
ガイドライン・各種施策の普及状況

- 「サイバーセキュリティ経営ガイドラインVer3.0」（2023年３月改訂）のダウンロード数が**10万件**に到達
- 補助金の申請要件化を通じてSECURITY ACTION宣言数が拡大。宣言数は**約40万件**まで到達。
- お助け隊サービス導入件数は**約7,000件**にまで到達。**足下で急速に導入が進んでいる。**
- IPAを通じた施策等により、**継続的にサイバーセキュリティ人材を育成**。地域での経営者向け演習、地域団体への講師派遣、セキュリティ担当者向けセミナー等を通じて**セキュリティ・コミュニティ（地域SECUNITY）の形成・活動を促進**。

サイバーセキュリティ経営ガイドラインVer３.0　累計DL数

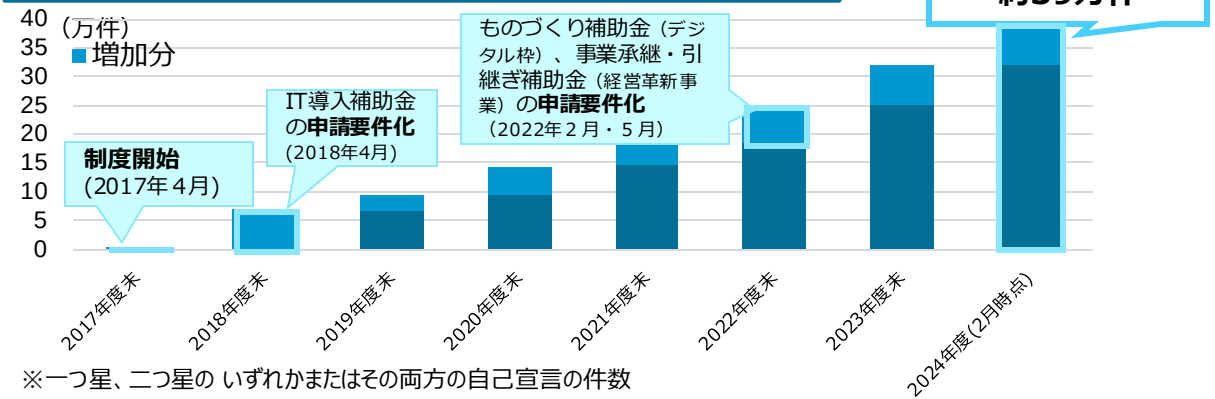


サイバーセキュリティお助け隊導入実績（累計）



※サービス提供者数は2025年3月末時点

SECURITY ACTION宣言の実績（累計）



※一つ星、二つ星の いずれかまたはその両方の自己宣言の件数

人材育成及び地域ワークショップの実績

中核人材育成プログラム修了者数	492名(2017年～2024年)
情報処理安全確保支援士	22,845名(2024年10月時点)
セキュリティ・キャンプ参加者数	全国大会：1232名(2004年～) ネクストキャンプ：53名(2019年～) ジュニアキャンプ：11名(2023年～)
IPA　セキュリティ講演者派遣	84件(2024年度)
IPA　セキュリティセミナー支援	セミナー開催支援：26件 経営者向けインシデント机上訓練：18件 (2024年度)

２．令和６年度の主な施策の取組状況

新たなサイバーセキュリティ政策の全体像及び今後の方向性

中小企業のセキュリティ対策の課題・対策・今後の方向性

（１）サプライチェーン対策強化

（２）中小企業への対策強化

（３）人材育成

（４）国際的なプレゼンスの強化

新たなサイバーセキュリティ政策の全体像及び今後の方向性

- NISCをはじめ関係省庁との連携の下、サイバーセキュリティ市場における**需要拡大と供給力強化に向けた取組**や、**国際的な制度調和と国内での調達要件化促進**、**サイバー情勢分析能力強化**を図っていく。

①サプライチェーン全体での対策強化

- サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の具体化・実装
- 我が国半導体関連産業におけるセキュリティ対策水準の向上を通じた競争力確保
- 地域における中小企業支援の拡大（サイバーセキュリティお助け隊サービスの普及促進等）
- サプライチェーン対策評価制度の構築（対策水準の可視化）等　**⇒政府調達・補助金の要件化等を通じた実効性強化**

②セキュア・バイ・デザインの実践

- IoT適合性評価制度の検討、国際制度調和に向けた調整
- SBOM（Software Bill of Materials）の活用促進、安全なソフトウェアの開発に向けた指針の整備
- サイバーインフラ事業者の責務の明確化

⇒国際連携を前提とした制度構築と政府調達等要件化を通じた制度の普及

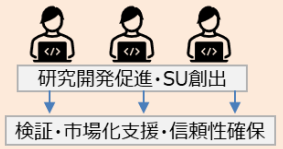
③政府全体でのサイバーセキュリティ対応体制の強化

- IPAのサイバー情勢分析能力強化
- 改正保安３法を踏まえたサイバー事故調査体制の構築
- サイバー攻撃技術情報の共有促進　等

⇒官民のサイバー状況把握力・対処能力向上と関係省庁との連携

④サイバーセキュリティ供給能力の強化

- サイバーセキュリティ産業振興のための政策パッケージの推進
- 先進的サイバー防御機能・分析能力の強化
- 重要インフラ等を守る高度セキュリティ人材の育成（中核人材育成プログラム）、若手人材発掘機会（セキュリティ・キャンプ）の拡大　等



IPA 産業サイバーセキュリティセンター
Industrial Cyber Security Center of Excellence（ICSCoE）

⇒セキュリティ市場の拡大に向けたエコシステムの構築

中小企業のセキュリティ対策の課題・対策・今後の方向性

	①中小企業の対策不足	②サプライチェーンへの影響	③セキュリティ人材不足
課題の認識	中小企業の約４割が必要性を感じていないとの認識があり、４割の企業がコストの課題がある。 中小企業のセキュリティに対する意識を変革させるとともに、コスト負担軽減策が必要。	中小企業に対するサイバー攻撃により、取引先企業の７割に影響が及んでいる。 サプライチェーン全体としてセキュリティ対策を強化できる環境整備が必要。	企業の約９割がセキュリティ人材不足が深刻と認識。 社内外を問わず、セキュリティ対策を適切に助言、判断、評価等ができる人材の育成等が必要。
現状の対策	SC3の活用も含め幅広くセミナー等を開催し地域企業のセキュリティ対策意識を向上。 企業規模等に応じたセキュリティ対策事例作成、お助け隊サービス普及とIT導入補助金の要件見直し。	サプライチェーン全体でセキュリティ対策の可視化のためSC対策評価制度の検討。 監査制度の活用促進のためガイドラインの見直し。 取引先とのパートナーシップ構築に向けた具体的検討の開始。	人材の手引きの策定、共通語彙集の策定などの基本枠組みの整備。 セキュリティ支援が可能な専門家と中小企業とのマッチング実証を実施。
目指す方向性	・ガイドラインの普及促進により自発的にセキュリティ対策に取組む中小企業の増加。 ・お助け隊サービス導入企業が飛躍的に伸びて、中小企業のセキュリティ対策レベルの底上げが実現。	・サプライチェーン全体でセキュリティ対策状況が可視化され取引の信頼性を高める。 ・取引先企業への対策の支援・要請に係る関係法令を整理し共助の関係が実現。	・登録セキスペのアクティブリストやセキュリティ人材育成の手引き等のサポート基盤が整備され、中小企業のセキュリティ人材不足を補完する仕組みが立ち上がっていく。

２．令和６年度の主な施策の取組状況

（１）サプライチェーン対策強化

- サプライチェーン対策評価制度
- （参考）セキュリティ要求事項・評価基準
- 取引先へのセキュリティ対策の要請に係る関係法令の適用関係の整理
- 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）の組織強化
- ＳＣ３の活動と今後の方針
- 情報セキュリティ監査・システム管理制度　関連基準等の全体像
- 情報セキュリティ監査・システム監査に関する令和６年度の動き

サプライチェーン対策評価制度

～制度の目的～

【現状認識（制度検討の背景）】

- 近年、**サプライチェーンを通じた情報漏えい・事業継続に関するインシデントが頻発**。その対策として、政府や重要インフラ企業のみならずその取引先に対しても適切なセキュリティ対策を課す必要があるが、**複雑なサプライチェーン下で、様々な取引先から様々な要求事項を求められている**状況。**発注企業にとっては、正しいセキュリティ対策が取引先でなされているか不明確／受注企業にとっては（特に中小企業を中心に）過度な負担につながっている**。結果として、サプライチェーン全体のセキュリティ底上げにつながっていない。

【制度趣旨】

- **ビジネスサプライチェーン・ITサービスサプライチェーン**における、**取引先へのサイバー攻撃を起因とした情報セキュリティリスク／製品・サービスの提供途絶リスク/取引ネットワークを通じた不正侵入等のリスクに対するセキュリティ対策の成熟度を確認する**。
- **2社間の契約における発注企業が、受注側に適切な段階（★）を提示し取得を促す**（**再委託先は発注者から見た対象にはならない**（※））。

（※） **再委託先のセキュリティ対策は、委託先を通じて必要に応じて管理**（一部要求項目において、「重要な取引先におけるセキュリティ対策状況の把握」を求めることを盛り込み）

【目指す効果】

- **サプライチェーンにおけるリスクを対象**にした上で（※）、その中での立ち位置に応じて必要な対策を提示することで、**企業の対策決定を容易・適切なものにする**。すべてのサプライチェーン企業が対象となるが、特に**サプライチェーンを構成する中小企業は、セキュリティ対策におけるリソースが限られていること／自社のリスクを踏まえてセキュリティ対策を行うことはハードルが高いことから、活用による効果が大きい。**

（※）**本来は各企業が自社のリスクを特定して必要なセキュリティ対策を個別に検討・実施することが望ましい**が、リソースに限りのある**中小企業を中心にただちにこれを実現できていない企業が一定数存在**する。本制度は、**包括的なリスク分析に基づき共通して求められる対策を示す**もの。将来的には、こうした企業も**より自社のリスク分析に基づいたさらなる対策の強化をしていくことが望ましい**。

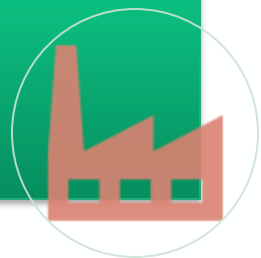
サプライチェーン対策評価制度

～制度の目的～

- 発注者・受注者双方にとって、適切なセキュリティ対策の決定や対策状況の説明が容易・適切となることが期待される。
- また、取引先のセキュリティ対策が適切に実装されることで、発注企業のサプライチェーン・リスクの低減や、経済・社会全体でのサイバーレジリエンスの強化が期待される。

受注企業への効果

- 自社がどの程度のセキュリティ対策を実施するべきか明確になる。
- 発注企業等に対して、セキュリティ対策に係る説明が容易になる。
- 対策に要する費用や効果の可視化
- セキュリティサービスの標準化による選択肢拡大やコスト低減（中長期）



発注企業への効果

- 取引先に求めるセキュリティ対策の内容や水準の決定や、実施状況の把握が容易・適切になる
- 取引先におけるセキュリティ対策の適切な実装により、サプライチェーンに起因する自社セキュリティリスクの低減

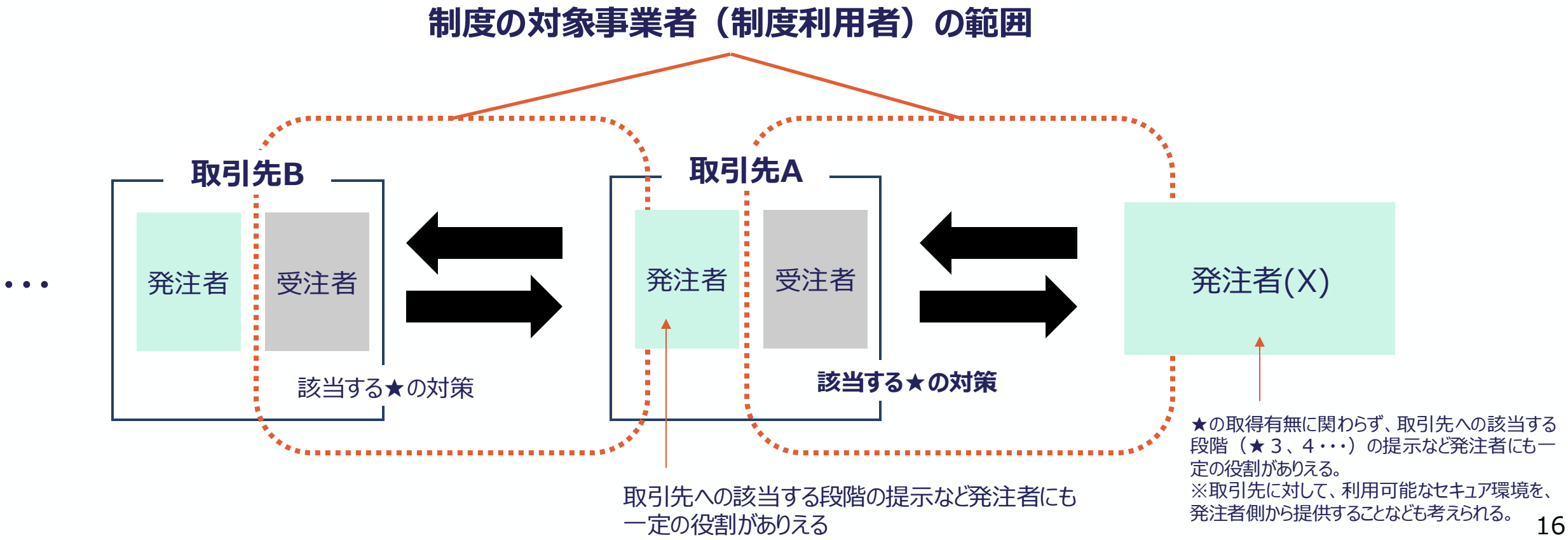
社会全体での効果

- サプライチェーン全体での底上げを通じた経済・社会全体のサイバーレジリエンス※の強化
- サイバー攻撃への備えのある企業等への適切な評価
- セキュリティ製品やサービスの市場拡大・競争力向上（中長期）

※サイバーレジリエンス(Cyber resiliency)
サイバー資源を使用する、またはサイバー資源によって実現するシステムに対する不利な状況、ストレス、攻撃、侵害を予測し、それらに耐え、回復し、適応する能力 https://csrc.nist.gov/glossary/term/cyber_resiliency

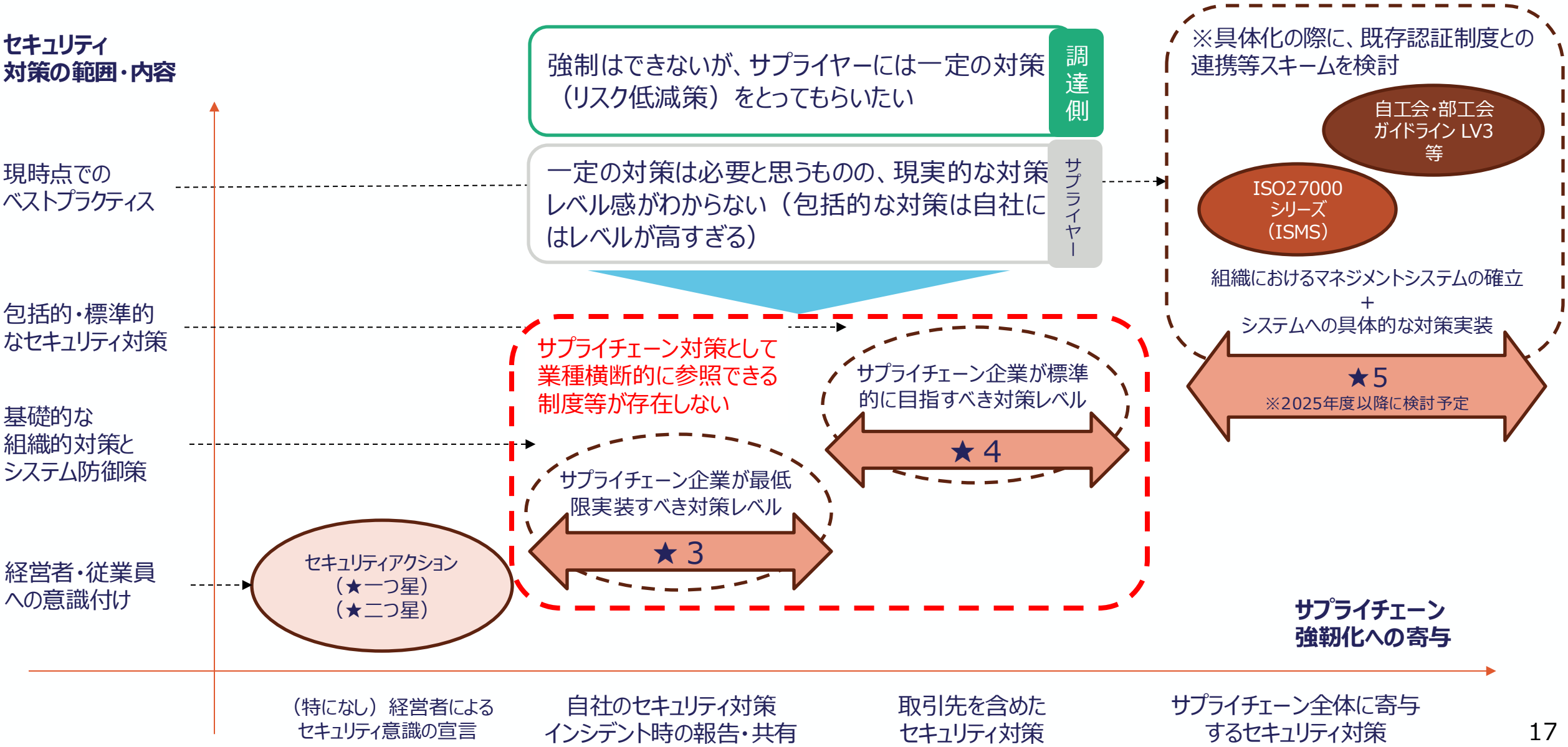
サプライチェーン対策評価制度
～制度の対象とする組織～

- 本制度で定めるセキュリティ対策の実施主体として想定するのは、サプライチェーン企業（２社間の契約における受注者側）。サプライチェーン企業が対策を実施するに当たって、発注者による協力が必要な場合があることから、制度が想定する対象事業者（制度利用者）の範囲は、赤枠囲いとする。なおサプライチェーン企業は、取引によっては発注者にもなりえる。
- 評価取得の申請主体は、自社IT基盤を中心とした自社のセキュリティ対策の向上に責任を有する単位（基本的には法人単位又は企業グループ単位）とする。



サプライチェーン対策評価制度

～要求事項・評価基準～



（参考）セキュリティ要求事項・評価基準

- レベルごと達成すべき「経営の責任」、「サプライチェーンの防御」、「IT基盤の防御」に資する対策を提案。

※1 以下は必ずしも全要求を網羅しているわけではない点に留意されたい。
※2 資料2の大分類のうち、ガバナンスの整備、リスクの特定、インシデントへの対応、インシデントからの復旧は「経営の責任」に、取引先管理は「サプライチェーンの防御」に、攻撃等の防御、攻撃等の検知は「IT基盤の防御」に該当

	★3（Basic）	★4（Standard）
経営の責任	**企業として最低限のリスク管理体制構築** • 自社のセキュリティ担当の明確化 [No.1] • セキュリティ対応方針の策定 [No.3] **インシデント発生に備えた対応手順の整備** • インシデント対応手順の作成 [No.25] **自社IT基盤や資産の現状把握** • 情報資産やネットワークの一覧化 [No.7,8] • 取引先等とのネットワーク接続の管理 [No.9]	**継続的改善に資するリスク管理体制の構築** • 定期的な見直しの実施 [No.6] • 定期的な経営層への報告、不備の是正等 [No.7] **インシデントからの復旧手順等の整備** • 復旧ポイント、復旧時間を満たす手順等の整備[No.44] **脆弱性など最新状況の把握と反映** • 脆弱性管理体制、管理プロセスの明確化 [No.17] • 定期的な見直しの実施「No.6」（再掲）
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明確化** • 接続している外部情報システムの一覧化 [No.5] • 他社との機密情報の取扱い明確化 [No.6]	**サプライチェーンにおける対策状況の把握** • 機密情報共有先の一覧化 [No.8] • 重要な取引先等の対策状況把握 [No.10] **取引先等との役割と責任の明確化** • インシデント発生時の他社との役割等の明確化 [No.11]
IT基盤の防御	**不正アクセスに対する基礎的な防御** • 基礎的なID管理手続き、アクセス権限の設定 [No.11,12,17] • パスワードの安全な設定及び管理 [No.15,16] • 内外ネットワーク境界の分離・保護 [No.23] **端末やサーバーの基礎的な保護** • ソフトウェアの適時のアップデート適用、不要なソフトウェアの削除 [No.20,21] • 端末等へのマルウェア対策 [No.22]	**多層防御による侵入リスクの低減** • 重要な保管データの暗号化 [No.29] • 社内システムにおける適切なネットワーク分離 [No.38] • 社外への不正通信の遮断(出口対策) [No.39] • 情報機器等の状態や挙動の監視・対応 [No.41] **迅速な異常の検知** • ログの収集・定期的な分析の実施 [No.35] • ネットワーク接続やデータ転送の監視 [No.40] • 情報機器等の状態や挙動の監視・対応 [No.41]（再掲） • 監視活動で検知された事象の分析 [No.42]

取引先へのセキュリティ対策の要請に係る関係法令の適用関係の整理（暫定）

- 令和４年10月に公表したガイドラインについて、関係省庁と連携し**更なる具体化に向けた検討**を実施中。

サプライチェーン全体のサイバーセキュリティの向上のための取引先とのパートナーシップの構築に向けて（概要）

【背景】

（令和４年10月28日 経済産業省・公正取引委員会）

■ 昨今、サイバーセキュリティ対策が不十分な**中小企業がサイバー攻撃に狙われ、サプライチェーン全体に問題が波及**する事態が発生。

■ 令和４年４月、「原油価格・物価高騰等に関する関係閣僚会議」（内閣総理大臣、内閣官房長官、関係大臣、公正取引委員会委員長が出席）において、**コロナ禍における「原油価格・物価高騰等総合緊急対策」**を決定。

「サイバーインシデントによってサプライチェーンが分断され、物資やサービスの安定供給に支障が生じることのないよう、**中小企業等におけるサイバーセキュリティ対策を支援**するとともに、**取引先への対策の支援・要請に係る関係法令の適用関係について整理**を行う。」

【内容】

■ 発注者側となる事業者は、以下を参考に、サプライチェーンの保護に向けて、取引先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み、取引先とのパートナーシップの構築を目指していただきたい。

①サイバーセキュリティ対策に関する支援策

■ **サイバーセキュリティお助け隊サービス**（中小企業に対するサイバー攻撃への対処として不可欠なサービスをワンパッケージで提供）の利用促進

■ **セキュリティアクション**（中小企業がセキュリティ対策に取り組むことを宣言）の推進

■ **中小企業の情報セキュリティ対策ガイドライン**（中小企業を対象に、情報セキュリティ対策に取り組む際の、経営者が認識し実施すべき方針、対策を実践する際の手順や手法をまとめたもの）の活用

■ **パートナーシップ構築宣言**（発注側企業が取引先との間でパートナーシップを構築することを宣言）の中で、取引先にサイバーセキュリティ対策の助言・支援を行うことを取組例として記載

②サイバーセキュリティ対策の要請に係る独占禁止法・下請法の考え方

■ サイバーセキュリティ対策の必要性が高まる中、**サプライチェーン全体のセキュリティ対策強化は重要**な取組。サイバーセキュリティ対策を要請すること自体が直ちに問題となるものではない。

■ ただし、要請の方法や内容によっては、問題となることもあるため、そのようなケースを例示。

<問題となるケースの例>

① 取引上の地位が優越している事業者が、サイバーセキュリティ対策の要請を行うことで、取引の相手方に生じるコスト上昇分を考慮することなく、一方的に著しく低い対価を定める場合

② 取引上の地位が優越している事業者が、取引の相手方に新たなセキュリティサービスを利用する必要がないにもかかわらず、自己の指定する高価なセキュリティサービスを利用させる場合

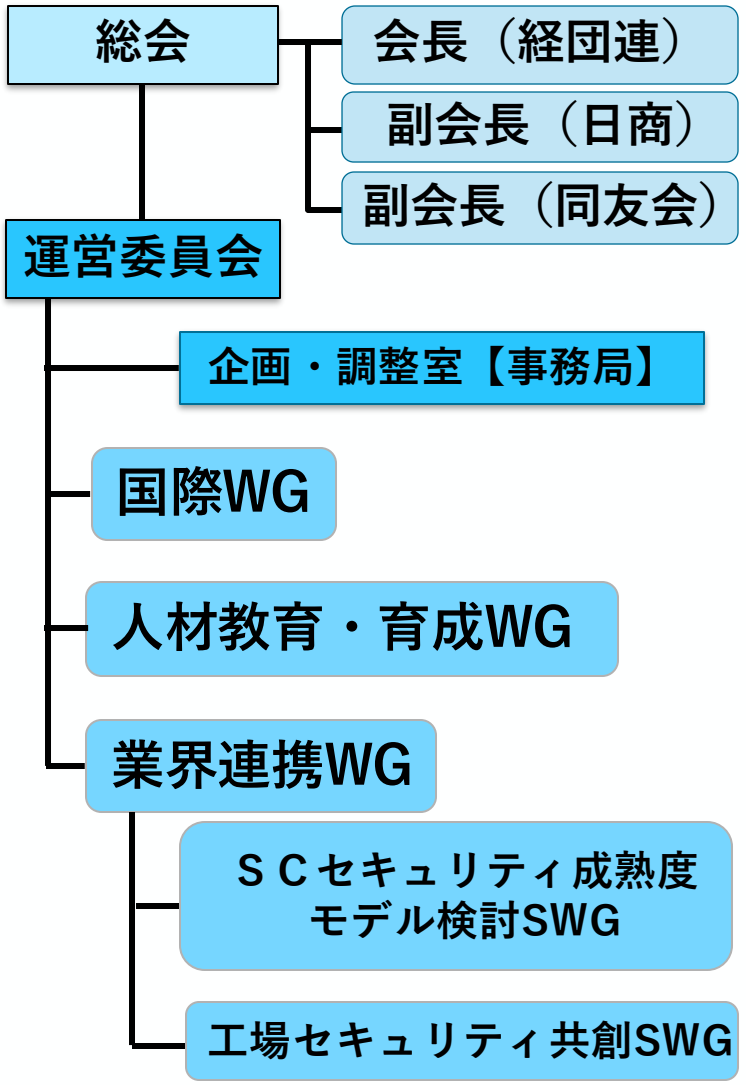
サプライチェーンサイバーセキュリティコンソーシアム（ＳＣ３）の組織強化

ＳＣ３は「産業界主導による業界連携のプラットフォーム」として、サプライチェーン上のステークホルダーとの対話や政策提言を主導し、施策の実効性を高めることを目指し令和２年に任意団体からスタート。

今後サイバー攻撃が益々増化していく中、サイバー空間の安定性、安全、繁栄を推進するため、対話、協業、イノベーションを通じて、日本のサプライチェーンの強靭性を構築する取り組みを開拓し、国家全体のレジリエンス力を強化する必要がある。

そのために、産業界横断、地域企業、中小企業の観点で幅広い会員基盤を有するSC3は法人化により体制を強化し、令和6年度、経産省・IPAの支援を経て、企画運営機能の強化、ワーキンググループの再編を進め、経済三団体からの支持、従来会員の参加の継続を維持した形で一般社団法人サイバーリスク情報センターとの一体連携の経営に移行。『民民連携・産官連携の連携プラットフォーム』として機能強化を図り、令和７年度より本格的に活動を開始する。

＜新組織体制＞



＜新組織＞
ＣＲＩＣ－ＳＣ３：一般社団法人サイバーリスク情報センター
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

・令和６年１０月より、企画運営機能の強化、ワーキンググループを再編し業界連携、国際連携、人材育成の課題にフォーカス。
・令和７年１月よりＣＲＩＣとの一体連携により法人化。
・経済三団体（経団連・日商・同友会）主導で、会員数は令和７年１月現在で９６業界団体と７５企業が参加。

HP：https://sc3.jp/　　問合せ先：info@sc3.jp

ＳＣ３の活動と今後の方針

従来	現在	今後
• 十分なリソースを割けない中小企業での対策強化 • 情報不足により対策が進まない地域や地方にある団体／企業への情報提供 • 多重下請け構造の業界における、対応標準化やTierNへの浸透	• 国際的なサプライチェーンでの課題検討 • 産学連携による人材育成活用環境整備 • 企業のセキュリティ対策評価制度検討 • 工場システムにおける企業の協力体制 • 企業/業種の垣根を越えた、システム/サービスの連携	• 独禁法/下請法対応の政策提言 • 業界で異なる各種ガイドラインの見直し • 企業間契約とインシデント時の責任分界点 • 企業のセキュリティに関わる情報公開の在り方 • 地域SECUNITYの活性化

今後の検討テーマ
課題の抽出と優先順位を検討

① 各種ガイドラインの在り方の検討（業界間相違、共有化／個別性のバランス）
② SBOM等の普及啓発
③ サプライチェーン先との独禁法・下請法対応の具体的なガイドの検討
④ サプライチェーン先への利益供与問題
⑤ 企業のセキュリティに関わる情報公開の在り方と情報共有におけるベンダー・ユーザ間契約
⑥ サイバー保険
⑦ 地域SECUNITYと連携した活動の展開

活動形態

	開催頻度	開催形式/利用システム	概要
全体会議	年2回開催	ハイブリッド形式	• SC3全体活動報告 • 関心の高いトピックスの講演
フォーラム	最大年2回	会場開催形式	• 1つのWG/SWGから詳細な活動報告を実施 • **外部専門家を招聘し、サイバーの状況を共有**
勉強会	別途決定	会場開催形式/ハイブリッド形式	• 特定トピックスについて取り上げ議論を実施 • 必要に応じて、SWGを設置
外部連携	連携組織による	連携組織の形式	• **IPA地域関連活動など外部組織との連携・コラボレーション**

情報セキュリティ監査・システム監査制度　関連基準等の全体像

凡例：民間にて規定　経済産業省にて規定

情報セキュリティ監査制度

情報セキュリティ監査基準
（全5ページ）
2003年策定
監査人の行動規範のみ

実施基準ガイドライン（全11ページ）
2003年策定
実施上の留意事項と手順を示す

報告基準ガイドライン（全15ページ）
2003年策定
報告上の留意事項と報告書雛形を示す

情報セキュリティ管理基準
（全84ページ）
2015年改訂
マネジメント基準と管理策基準で構成

個別管理基準（監査項目）策定ガイドライン
（全5ページ）
2003年策定
個別基準策定の手順を示す

システム監査制度

システム監査基準
（全44ページ）
2023年改訂
実施基準や報告基準に相当する内容を含む

システム監査基準ガイドライン
（全65ページ）
2023年改訂
基準の趣旨等を具体的に説明、例示

ITガバナンス編とITマネジメント編で構成

システム管理基準
（全89ページ）
2023年改訂

追補版
IT統制ガイダンス
（全150ページ）
2024年改訂

システム管理基準ガイドライン
（全288ページ）
2023年改訂
具体的な着眼点等を例示

情報セキュリティ監査・システム監査に関する令和６年度の動き

情報セキュリティ監査基準・管理基準各ガイドライン

情報セキュリティ監査基準・管理基準並びに各ガイドラインは、情報セキュリティマネジメントに関わる国際規格（ISO/IEC 27001、27002）が改正され、また情報セキュリティ監査制度を取り巻く環境に変化があったことを受け、外部有識者の意見も踏まえ、改訂作業を実施中。

＜主な改訂＞

・国際規格の改正に基づいた改訂
・条項番号*の付記方法の見直し

*情報セキュリティ管理基準に付されているJIS Q 27001/27002に基づき付記している番号。

監査人が適正かつ円滑な監査業務を遂行出来るよう、より分かりやすい内容にするための改訂作業が進行中。

システム管理基準追補版（IT統制ガイダンス）

システム管理基準追補版（財務報告に係るIT統制ガイダンス）は、令和５年４月に「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の改訂について（意見書）」が公表され、また、同月に「システム管理基準」及び「システム監査基準」（システム管理基準等）が改訂されたことを受けて、これらの改訂部分との差異を点検し、整合がとれたものとなるよう所要の見直しを実施。

令和６年12月に改訂版を公表。

➢ **今後も、これらのガイドラインが活用されるよう、普及・啓発を行っていく。**

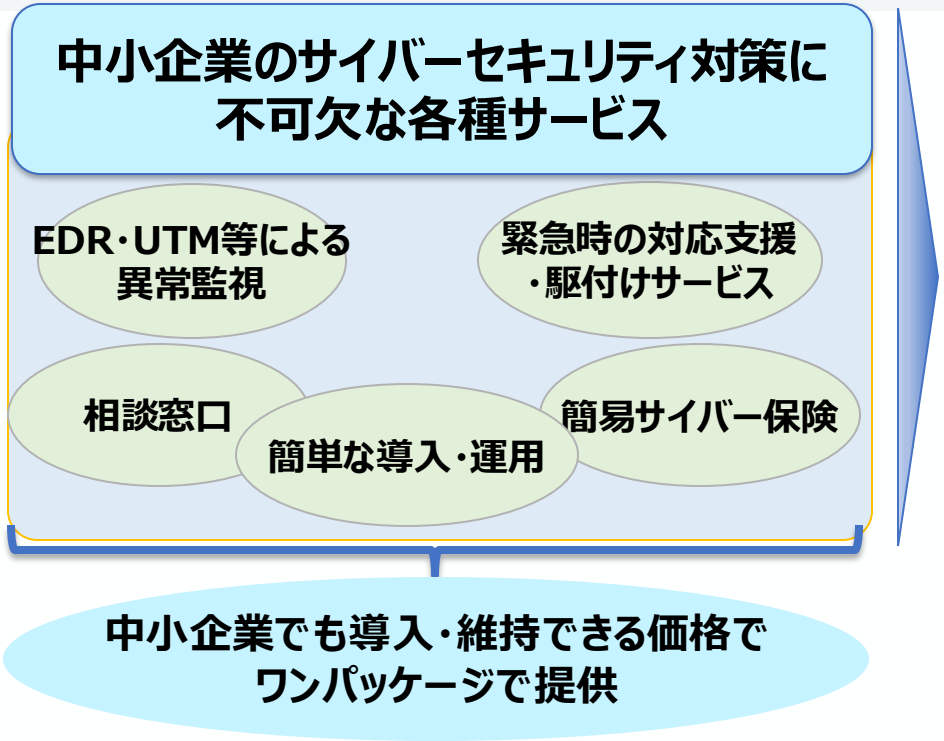
２．令和６年度の主な施策の取組状況

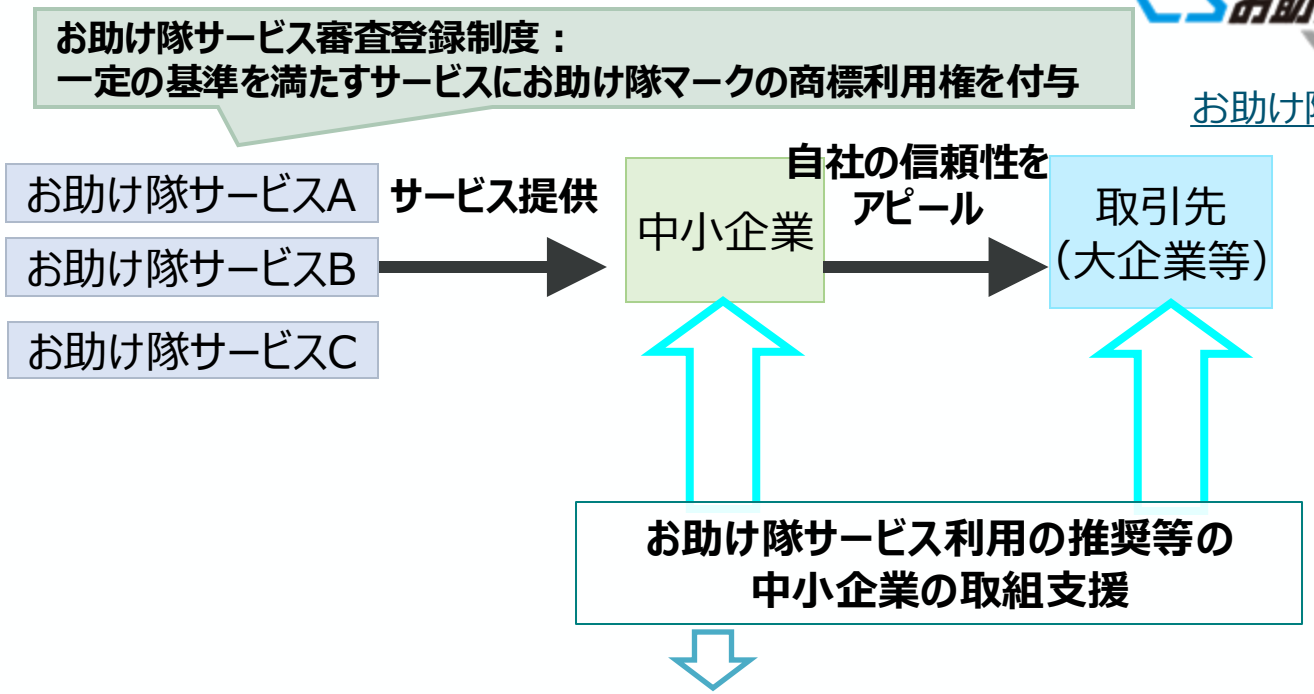
（２）中小企業への対策強化

- サイバーセキュリティお助け隊サービス概要
- IT導入補助金セキュリティ対策推進枠の要件変更
- サイバーセキュリティお助け隊サービスの普及の取組
- サイバーセキュリティお助け隊サービスの現状と課題
- 中小企業実態調査　企業の規模・業種別の費用対効果ある対策事例（速報）
- 地域のITベンダの能力向上にかかる手引きの整備
- 地域のセキュリティ対策活性化の取組

サイバーセキュリティお助け隊サービス概要

- サイバーセキュリティお助け隊サービスは、**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（例：月額1万円以内）に提供するサービス。**
- **全国46事業者がサービスを提供**しており、**約7,000件の利用実績**（2024年９月末時点）がある。
- IT導入補助金「セキュリティ対策推進枠」を活用することで、**最大150万円まで、導入費用の1/2（小規模事業者は2/3）の補助を受けられる。**





お助け隊マーク

サイバーセキュリティお助け隊サービスの利用はこちらから
⇒ https://www.ipa.go.jp/security/otasuketai-pr/

IT導入補助金セキュリティ対策推進枠の要件変更

- **サイバーセキュリティへの投資は**直接売り上げ増加につながらない（投資効果が見えにくい）ため、**中小企業にとって他のIT投資と比較しても投資へのインセンティブは極めて低いのが現状。**
- サイバーセキュリティお助け隊サービスの提供事業者10社へのヒアリングによると、**申請コストに比較して補助金によるインセンティブが低い**との実態が明らかになるとともに、**補助率の引き上げの要望が多数**寄せられた。
- そこで、IT導入補助金2025から、**補助率・補助上限を引き上げる要件変更を実施。**

小規模事業者の補助率引き上げ

とりわけ小規模事業者については、サイバーセキュリティ対策にコストをかけられない実態がある。
そうした者については、現在の要件（補助率及び５万円との補助下限額）では補助対象とならない場合もあることから、**小規模事業者の補助率を２／３に引き上げた。**

補助上限の引き上げ

お助け隊サービスの価格要件が撤廃された新たなサービス「お助け隊２類サービス」の提供が開始されたことにより、今までサービスの導入ができなかった相対的に規模の大きい中小企業についても本サービスを導入できるようになったところ、**中小企業における２類サービスの導入を促進するために、補助上限を150万円に引き上げた。**

IT導入補助金セキュリティ対策推進枠見直しの概要

※赤字が見直し部分

	要件見直し前	要件見直し後
補助上限	5万円～100万円	5万円～**150万円**
補助率	中小企業：１/２	**小規模事業者：2/3** 中小企業：1/2
その他見直し		**事業全体における**労働生産性（※）について、以下の要件を全て満たす３年間の事業計画を策定し、実行すること。 一　事業計画期間において労働生産性を年平均成長率１パーセント以上向上させること。 二　労働生産性の向上に向けた計画が実現可能かつ合理的であること。 **（※）　補助により軽減された負担分を振り向けた投資による効果、サイバー攻撃リスクの低減に伴う売上損失の期待値減少効果、その他の経営努力による効果を含む。**
対象経費	サイバーセキュリティお助け隊サービス利用料（最大2年分）	

サイバーセキュリティお助け隊サービスの普及の取組

- お助け隊サービスの更なる普及に向けては**中小企業における認知度が課題**であるところ、政府広報を活用して**日経ビジネスの記事掲載**や**ラジオ番組への出演**、**新聞広告**等を実施。
- 中小企業におけるサイバーセキュリティ対策の必要性への理解とサイバーセキュリティお助け隊サービスの活用を促す**リーフレットを作成**し、全国の中小企業支援機関等に展開。
- また、特定の業界等における身近な事例が有効であることから、**医療機関での導入事例を作成**し、周知を実施。引き続き、様々な事例の作成を実施する予定。

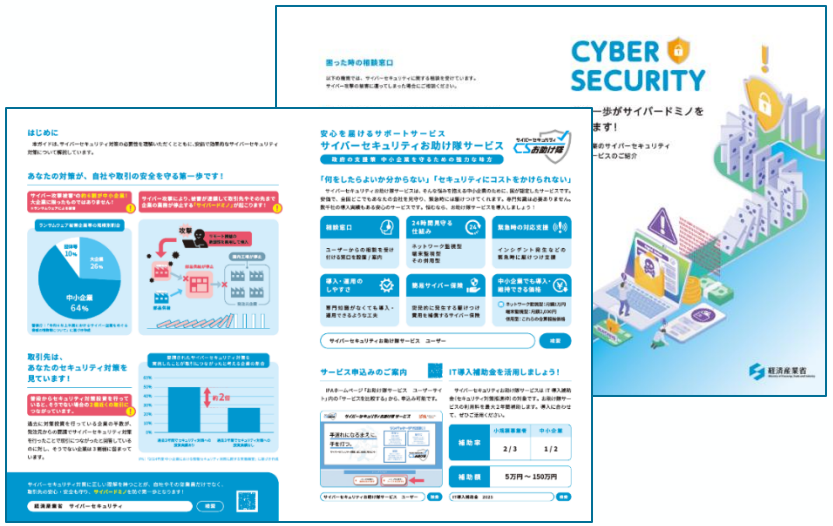
政府広報を通じた対外発信

<2025年2月14日発刊
「日経ビジネス」>

2025.02.16
備えて安心！中小企業のサイバーセキュリティお助け隊サービス

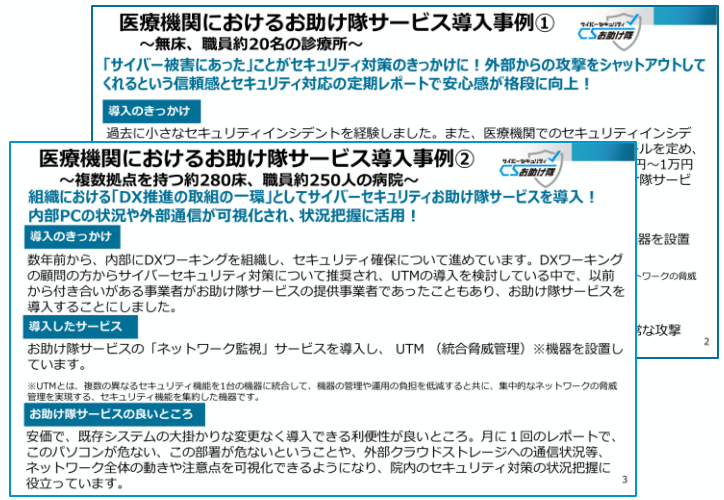
<2025年2月16日放送FM
TOKYO「日曜まなびより」>

中小企業向けリーフレットの作成



関係省庁や業界団体の御協力を得て、全国の経済産業局、総合通信局、都道府県警察、金融機関（地方銀行、信用組合等）、中小企業支援団体（商工会議所等）、士業団体（税理士会、行政書士会等）、業界団体等に広く展開。

導入事例の作成

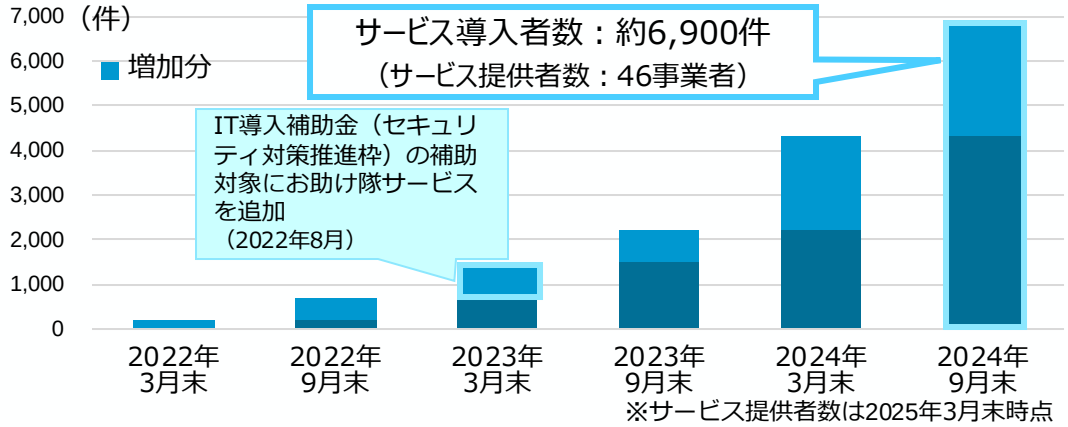


医療機関の協力を得て、医療機関における導入事例を作成。厚労省の協力をのもと、医療機関等への情報提供を強化。

サイバーセキュリティお助け隊サービスの現状と課題

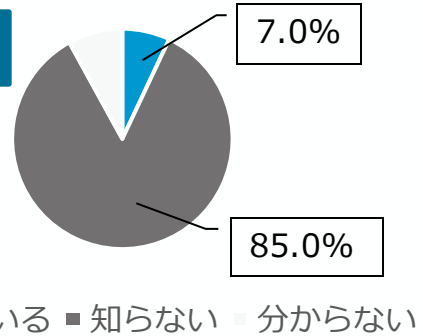
- お助け隊サービス提供事業者数及びサービス導入者数は右肩上がりで増加を続けているが、セキュリティ対策を必要とする中小企業への浸透度合いはまだまだ不十分であり、普及に向けた取組強化は喫緊の課題である。
- お助け隊サービスの導入数は増加傾向にあるが、2024年にIPAが実施した中小企業等実態調査の結果によると、「サイバーセキュリティお助け隊」を認知している企業は全体の１割弱にとどまる。
- サービス提供事業者、ユーザ双方が使いやすい制度となるように、基準の見直しを含めて検討する必要がある。

サイバーセキュリティお助け隊導入実績（累計）



中小企業における認知度

調査期間：2024年10月25日～11月6日
調査方法：ウェブアンケート
調査対象：中小企業の経営層
回収数：4,191件



２類サービスの認定状況

- 2024年度、2回のお助け隊サービス適合性審査を実施し、計12サービスを認定。
- 2類サービスは、1類サービスに比べ、価格要件が緩和され、より多くの中小企業が対象となることから、中小企業が選びやすいサービスとするめたに更なるにサービス数が増加を目指す。

その他の課題等

お助け隊サービス提供事業者に対するヒアリングでは、以下のような指摘があった。

- お助け隊サービス登録の審査期間が非常に長く、必要書類も多いことから、審査基準が不透明でコストがかかる。
- 物価高騰、人件費高騰により、価格要件を維持したサービス展開が困難。

中小企業実態調査　中小企業等における費用対効果のある対策（速報）

1. 中小企業4,191社に対するアンケート調査、更にその中から21社に対するインタビュー調査を実施した。
2. 調査結果から、**SECURITY ACTION 二つ星の対策を実施している企業ほどインシデント被害の低減が見られ**、また**第三者認証の取得や社内セキュリティ体制の整備をしている企業ほど取引先からの信頼獲得および取引につながる要因になったと回答している企業が多く見られた**。

全ての中小企業で効果のある対策

※アンケート調査結果より

✓SECURITY ACTION 二つ星 の実施

SECURITY ACTION 二つ星の対策を実施している企業ほど、インシデント被害が少なく、被害額も少ないと回答していることが明らかになった。

25項目の対策実施によりインシデント被害の低減（発生割合・被害額）が期待される。

✓第三者認証の取得・社内セキュリティ体制の整備

ISMS認証やPマークの取得はもちろんのこと、第三者認証以外にも社内のセキュリティ体制整備を実施している企業ほど、取引先からの信頼獲得につながり、取引につながっていると回答していることが明らかになった。

第三者認証の取得や体制整備により取引先からの信頼獲得、取引の拡大が期待される。

企業が取り組んでいる対策とその効果

※インタビュー調査結果より

業種（従業員数）	対策	効果
複合サービス業（51～100名以下）	**業務終了時にオフィス内ネットワークを完全に遮断する**ことで、不正アクセスによる**被害の低減とともに安心感を得られた。**	**被害の低減**
製造業（21～50名以下）	**「サイバーセキュリティお助け隊サービス」**を導入したことで、**社員による情報漏えいなどの事故が未然に防げるといった安心感を得られた。**	**被害の低減**
情報サービス業（21～50名以下）	**全社的な情報セキュリティ対策を行い、ISMS認証を取得**したことで**全社的なセキュリティ意識が向上し、新規取引のきっかけになった。**	**経営基盤の強化 信頼の獲得**
教育・学習支援業（5名以下）	大手塾の情報漏洩事案を受けて個人塾についても顧客等から情報管理に不信感が抱かれたため、**ISMS認証を取得**し、**情報管理の意識向上と顧客からの信頼獲得を図った。**	**経営基盤の強化 信頼の獲得**
製造業（6～20名以下）	**月額５万円程度の、民間の総合セキュリティ（UTM）を導入**しており、個別にセキュリティ機器を導入するよりもコストを抑えられた。また**地元の商工会議所が開催する講習会に参加して情報収集している**。これにより、**セキュリティ意識が向上し25年近くもウイルス感染が起きていない。**	**被害の低減**

「効果」の具体的内容

- 信頼の獲得　… 第三者認証の取得や、取引先（発注元）からのセキュリティ要請に応じて対策を実施したことが取引につながった等
- 被害の低減　… セキュリティ対策の実施によってインシデント被害の発生割合、被害額の低減につながった等
- 経営基盤の強化　… セキュリティ体制整備や第三者認証の取得により社内のセキュリティ意識向上につながった等

地域のITベンダーの能力向上にかかる手引きの整備

- 中小企業において、**セキュリティで困ったことがあった際の相談先として、「社外のIT関連業者」がもっとも多く**、特に身近なIT関連業者が重要な役割を担っている。他方、サイバー攻撃の被害にあった事案の中には、ベンダーの知識や対応不足等が起因するなど、**地元企業に対してITシステムを納入する地域のITベンダーの強化が不可欠**であり、ITベンダーの強化を図っていく必要がある。
- こうした現状を踏まえ、**地域のITベンダーのセキュリティに対する意識や知識の向上に向けて、ITベンダとしてセキュリティに関して認識しておくべき事項をまとめた手引きの作成に向けて検討を進めている。**
- 別途検討がなされている「サイバーインフラ事業者に求められる役割等に関するガイドライン」との整合性も確保しつつ本手引を作成し、**地域SECUNITYやお助け隊提供事業者等を通じた広報周知を進めていく。**

地域ITベンダー状況調査

- **ITベンダーの約2割が、サービス導入後に顧客と運用保守契約を締結しておらず、**その後の対応を中小企業側に全て委ねるケースも見られ、中小企業のセキュリティが十分に確保されないまま放置されている状況が判明。中小企業のコスト制約や人材不足等の課題がある状況下において、**ITベンダーの利益確保に直結しにくい**という事情も明らかとなった。
- また、**ITベンダーの約７割が社内のセキュリティ技術者が１～５名**であり、**セキュリティ技術者がいないITベンダーも約１割存在**することが判明。ITベンダー自社のリソース確保についても課題が明らかとなった。
- 一方で、一部ITベンダーの中には、**セキュリティ要件の優先付け、リスク説明と責任の明確化**を行うなど、中小企業の課題に対応するための取組を進めている事例も確認された。

地域ITベンダー向け手引の全体構成【案】

	構成	概要
本編	第１部　中小企業のお客様が抱えるセキュリティ対応上の課題	中小企業のお客様が抱えるセキュリティ対応上の課題やそれに伴うさまざまな問題点を明らかにし、中小企業のお客様向けシステムのセキュリティ担保の重要性について説明
本編	第２部　中小企業のお客様システムをサイバー攻撃から守るために地域のITベンダーに求められるもの	地域ITベンダーの自社の事業領域において、中小企業のお客様システムのセキュリティ確保・向上のために必要となる取組について説明
本編	第３部　地域のITベンダーが中小企業のお客様の良き相談相手となるための取組ヒント	中小企業のお客様のセキュリティ対応において、地域ITベンダーが中小企業のお客様から信頼される良き相談相手となるための取組ヒントについて説明
付録	付録1　中小企業のお客様システムにおけるセキュリティ対応の重要ポイントがよくわかるチェックリスト	セキュリティに不安がある中小企業のお客様システムに対して、セキュリティの観点から採り得る対応がよくわかるチェックリストを提供
付録	付録2　中小企業のお客様のセキュリテ対応支援に役立つ情報	地域ITベンダーにとって、中小企業のお客様のセキュリティ対応支援に役立つ情報を紹介

出典：中小企業のセキュリティ対応におけるITベンダーの役割に関するアンケート・ヒアリング調査（IPA）（2024年12月～2025年2月実施）

地域のセキュリティ対策活性化の取組

- 地域SECUNITY活動を進めるために、セキュリティとＤＸとセットで推進することの必要性を、関連団体・地域企業との更なる連携を目的として、全国の９つの経産局を回り、関連団体に協力を要請。
- IPAにおいて、2025年2月に「地域SECUNITY連絡会」を立ち上げ、取組の報告会を開催し情報の共有を図った。
- 地域SECUNITY連絡会で報告された内容は、地域SECUNITY活動促進のためのプラクティス集として2025年３月に公開した。

地域SECUNITY連絡会

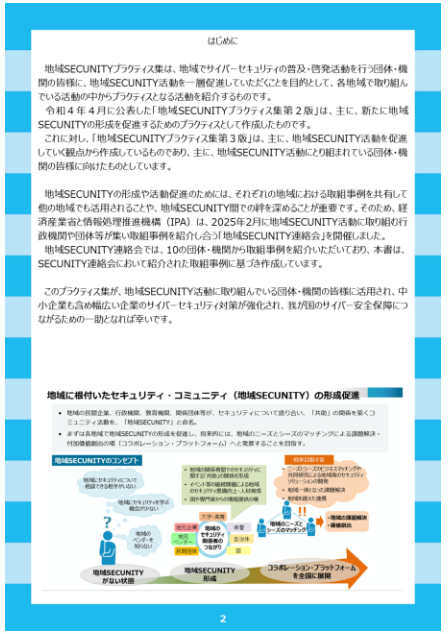
各地域SECUNITYの関係者を集め、各団体の課題や問題意識の共有を行う、「地域SECUNITY連絡会」を実施。他の団体の取組みを参考とすることで、各地域SECUNITYの活動を活性化。

開催概要

・開催日時：2025年2月12日
・開催形態：オンライン開催
・発表団体：10団体
・参加団体：22団体
・御講演：SC3企画調整室長　武智洋様

プラクティス集の作成

地域セキュリティコミュニティ【地域ＳＥＣＵＮＩＴＹ】
活動促進のためのプラクティス集　第３版



地域セキュリティコミュニティ【地域ＳＥＣＵＮＩＴＹ】
活動促進のためのプラクティス集　第３版

２．令和６年度の主な施策の取組状況

（３）人材育成

- サイバーセキュリティ人材の育成・確保に向けた令和６年度の取組概要
- 登録セキスペの活用促進・活躍の場の拡大
- 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
- 【参考】登録セキスペアクティブリストの基本設計（案）
- 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）（全体像）

中小企業のサイバーセキュリティ対策における人材の育成・確保に向けた令和６年度の取組概要

- サイバーセキュリティ**人材の育成促進に向けた検討会**において、**既存施策の拡充や改善などを基本**として、**登録セキスペの活用及び制度の見直し**や、**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**について議論。
- 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等）や支援機関等の意見から得られた課題を踏まえ、**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中小企業等の内でサイバーセキュリティ人材を育成し、又は外部の人材を活用するための実践的な方策を示したガイドブックの策定及び活用・普及策を中心に検討を実施。

	必要性	内 容	活用・普及策
登録セキスペアクティブリスト	• 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**自社の課題を特定**するために、また、ひな形や　要求事項を**自社にカスタマイズ**して落とし込むために、**専門家と相談**できる機会を**探索コストをかけずに確保**する必要。	• 相談者のニーズに応じた登録セキスペを選定できるよう、実証事業での声を踏まえ、 **支援実績テーマ／得意な業界／所属形態／登録セキスペ以外の保有資格など** を記載メニュー化したリストを作成・公表。 • **定型的な支援テーマ**（規程整備・リスク分析・クラウドサービス・インシデント対応・従業員教育）について、引き続き**ニーズ把握しつつ拡充を検討**。	• 中小企業の**直接利用（プル型）**のみならず、支援機関やITベンダー等の中小企業の**相談先を介した活用（プッシュ型）**も想定。 • 支援機関の**指導員への周知・研修**、支援機関の**窓口・専門家派遣事業**における利用。 • **専門家団体との連携**も検討。
人材確保・育成策の実践的方策ガイド	• **長尺なガイドを読むのが難しい**、人材育成のための**適切な演習が　分からない**などの声や企業の　**セキュリティ課題**は成熟度・課題領域が**多様**であることを踏まえ、**各所に散らばった対策の内容**や　**人材確保・育成策のエッセンス**を**段階的・コンパクト**に示す必要。	• 経営者の意識向上につながるよう、**経営者向けのメッセージ**も収録。 • 相談各社の**セキュリティ課題は多様**であることを踏まえ、実施すべきセキュリティ対策をSECURITY ACTION★１レベルから**段階的に提示**。 • 段階ごとに**提示したタスクを実施する人材の確保・育成策**を**具体的な教育コンテンツ**等とともに提示。	• 中小企業の**経営者・セキュリティ　担当者**を読者とするだけでなく、**中小企業の支援機関による活用**も想定。 • 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、セミナーコンテンツ、**映像コンテンツ**等による普及も検討。

登録セキスペの活用促進・活躍の場の拡大

- **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。

企業等類型

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

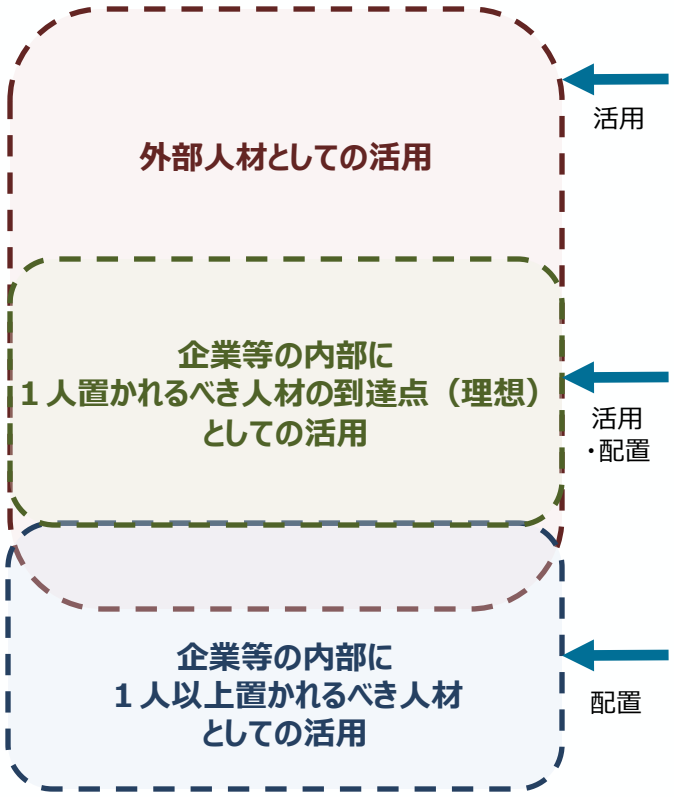
（例）「セキュリティ統括機能」として セキュリティ対策を推進する 専任人材を置くべき企業

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

政府機関・地方公共団体

登録セキスペの活用像



企業側（活用側）への働きかけ

サイバーセキュリティ対策促進制度における活用
（サプライチェーン対策評価制度、IoTセキュリティ適合性評価制度 等）

DX施策との連動
（デジタルガバナンス・コードへの紐付け 等）

各種投資促進施策における要件化

公的機関・重要インフラ事業者等における配置促進

登録セキスペ側への働きかけ

登録セキスペとのマッチングの枠組みの整備

登録セキスペアクティブリスト整備

連携・反映

デジタル人材育成・DX推進プラットフォームの整備

活用

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）

登録促進

監査スキル強化機会の提供

戦略マネジメント層向け講習の拡大

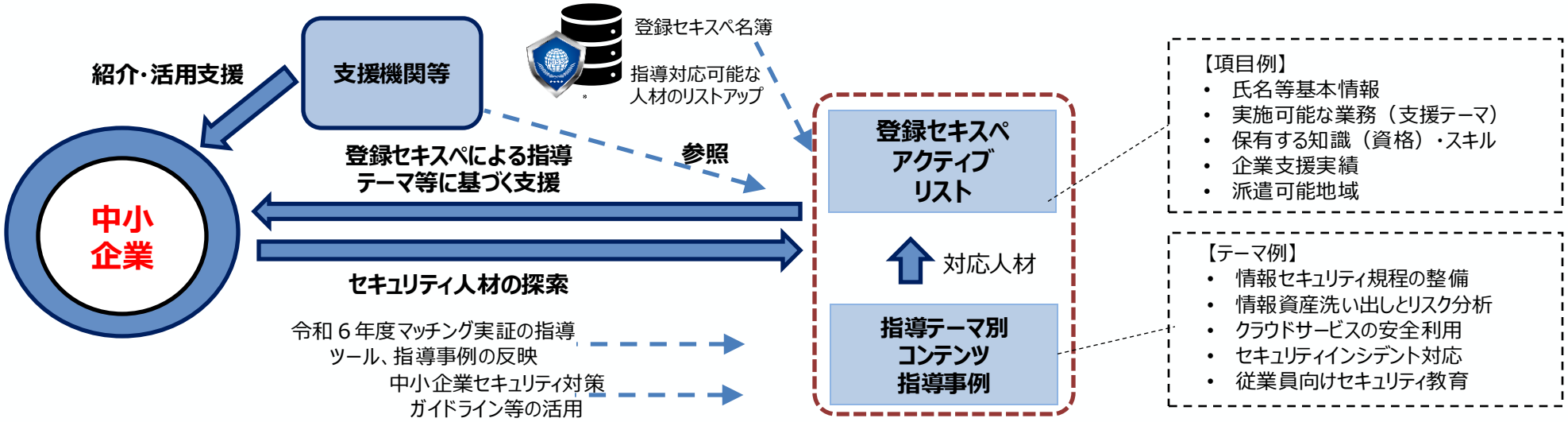
登録セキスペアクティブリストを活用した中小企業支援

サイバーセキュリティ人材の育成促進に向けた検討会第４回資料を一部加工

- 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**マネジメント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した「登録セキスペアクティブリスト」を整備する**とともに、リスト掲載項目の一つである**マネジメント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するとともに、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】登録セキスペアクティブリストの基本設計（案）

- 令和５年度補正予算事業の実施状況を踏まえ、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マネジメント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。

Ⅰ　リストの内容

掲載対象者	• 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	• 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（マネジメント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。

Ⅱ　リストの管理運用

管理運用主体	• マネジメント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	• 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、同事業のマネジメント指導の実績がある者を中心に掲載することを想定。令和７年度以降は、対象者を拡充することを想定。

Ⅱ　リストの管理運用（続き）

更新方法	• **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「マネジメント指導」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	• 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が有効であることを検証中。 （※２）令和５年度補正予算事業の地域ベンダー向け手引書において、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に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。

Ⅲ　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。

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）（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。

※ ガイドの整理に当たっては既存の公表文書との整合を確保。

４つのStepを提示

Step1	Step2	Step3	Step4
取組の開始	組織的な取組	本格的な取組	継続的な改善 より強固な対策
兼務の担当者を一人確保	兼務の担当者を増員	専任担当者の確保 兼任担当者の増員	必要な人材・体制の 見直しと確保

Step1の取組は、規模や業種に関わらず、全ての企業が実施。

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/jinzai/riss/index.html

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/security/otasuketai-pr/

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。

２．令和６年度の主な施策の取組状況

（４）国際的なプレゼンスの強化

- ●産業制御システム・サイバーセキュリティ演習
- ●日ASEANサイバーセキュリティ能力構築センター（AJCCBC）との連携
- ●ASEAN向け企業対策支援
- ●サプライチェーン上の国際連携の取組強化

産業制御システム・サイバーセキュリティ演習

- 経済産業省とIPA産業サイバーセキュリティセンター(ICSCoE)が、**米国・EU政府等と連携し、毎年開催するインド太平洋地域向けの1週間の研修プログラム**。これまで2018年度より７回開催。
- 本演習は、**インド太平洋地域の重要インフラ事業者、製造業者等のICSセキュリティの向上を目的**に、**産業用制御システム（ICS）のサイバーセキュリティに焦点**を当て、**ハンズオン演習**や、**日米欧専門家による講演**、**参加者間のネットワーキング**等を実施。

2024年度 演習の概要

- **日時**：2024年11月12日～15日
- **場所**：IPA文京キャンパス、IPA秋葉原キャンパス、EU代表部
- **主催**：経済産業省、IPA産業サイバーセキュリティセンター、米国政府（国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁、国務省）及びEU政府（通信ネットワーク・コンテンツ・技術総局）
- **参加者：**ASEAN加盟国、インド、バングラデシュ、スリランカ、モンゴル、台湾の重要インフラ事業者、製造業者、ナショナルCSIRT、政府機関等

ハンズオン演習

日米欧専門家による講演

インド太平洋地域参加者間のネットワーキング

日ASEANサイバーセキュリティ能力構築センター（AJCCBC）との連携

- ASEAN地域でのサイバーセキュリティ能力の向上と各国との連携強化を目指して、2024年11月にICSCoE(IPA)は、AJCCBC及びオランダ政府と協働し、同地域の政府関係者を対象に、**OTセキュリティを含む重要情報インフラ保護に関する人材育成プログラムを提供**。
- 5日間のプログラムのうち、1-4日目はオランダ政府からのセオリー中心の講義、最終日にICSCoE講師によるサプライチェーン　リスクマネジメントを主題とした講義およびワークショップを提供。

  - 日程：2024年11月25-29日　　※ICSCoEが提供したワークショップ：11月29日
  - 開催地：タイ・バンコク
  - 主催:AJCCBC、タイNational Cyber Security Agency(NCSA)、JICA
  - プログラム提供者：ICSCoE(IPA)、オランダ国家サイバーセキュリティセンター(NCSC)
  - 参加者：22名（タイ、フィリピン、インドネシア、マレーシア、カンボジア、ラオス、ブルネイ、シンガポール、東ティモール）

ワークショップの様子

参加者集合写真

ASEAN向け企業対策支援

- 経済産業省では産業界のサイバーセキュリティ向上に向け、**対象者ごとに具体的な対策を記載したガイドラインを展開している。**そのうち一部は**英語版も発行しているが、国外企業における認知度は低い。**
- サイバーセキュリティ対策は、サプライチェーン全体での対策が必要であり、 我が国とサプライチェーンの多くを共有するASEAN地域でのサイバーセキュリティ能力の向上が重要であることから、**ASEAN地域に向けて、施策の情報発信を強化。具体的には、日・ASEANサイバーセキュリティ政策会議や英語版HPにて情報発信。**

ASEAN地域へのガイドラインの展開

◆全事業者向け

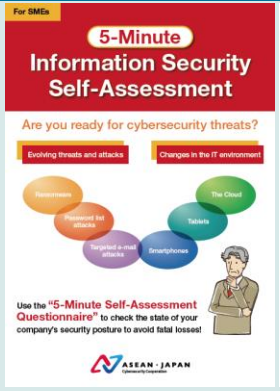
- サイバーセキュリティ経営ガイドライン
- ５分でできる！情報セキュリティ自社診断

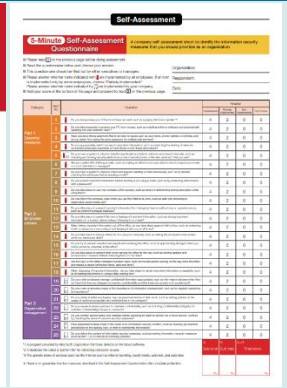
◆産業分野別

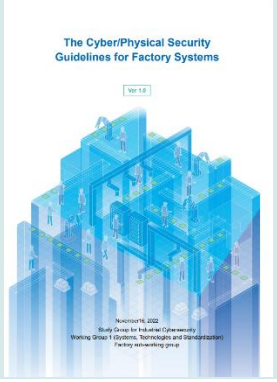
- 工場、自動車産業向けガイドライン

◆IT、ソフトウェア企業向け

- SBOMの導入に関する手引き　　等







英語版HPの更新

効果的に施策を発信するため、英語版HPを大幅リニューアル。必要な政策情報に簡単にアクセスできるよう、再構成。

Cybersecurity / METI Ministry of Economy, Trade and Industry

サプライチェーン上の国際連携の取組強化

ＳＣ３国際ＷＧの活動で国を超えたサプライチェーンのセキュリティ問題を検討

・2024年6月：台湾工業技術研究院 (ITRI) と MoU締結し、半導体製造業等のセキュリティに関して協力関係を構築

・2025年1月17日「半導体業界標準SEMI E187セミナー」開催

ITRIとのMoUの締結式

ITRI Ares Cho 博士のSEMI-E187のプレゼン

３．前回ＷＧで御指摘いただいた事項の対応状況

前回のＷＧ２ご意見への対応状況整理

前回のWG2ご意見への対応状況整理（１／２）

項目	前回の主なご意見	令和６年度の対応と成果	今後の対応
経営・中小企業（サプライチェーン対策）	・中小企業におけるセキュリティの底上げは、対面で実施しなければ広がらないと考えられる。どんな事例や被害額を見せても、**そのインシデントが自分のところでも起こると感じてもらわなければ、対策する気にはならない**のではないか。	・中小企業が**システムの脆弱性を攻撃された場合どの程度の額の被害が想定されるかを示し、中小企業にセキュリティ対策の必要性を理解してもらい**、自発的な対策ができる仕組みを検討する。そのために、**セキュリティ対策の実態調査を実施。**	・中小企業に対し、**ASMツールを用いた調査を実施**する。診断結果を企業規模別費用対効果対策やお助け隊サービスの活用と紐づけ、実施するべき**必要な対策をまとめたプラクティス集を作成**し、各地で啓発・広報を通じて中小企業が必要なセキュリティ対策の実施を促していく。 ・実態調査に基づき、**より実効性・継続性のあるSAの対策基準を見直す**。
	・セキュリティに馴染みのない方が多い印象で、380万社あるアクティブな中小企業のうち大半がそのような状況。**キャンペーン不足と思われる**ので、もう少し踏み込んで対応されるとよい。	・お助け隊サービスの認知度向上のため**政府広報を活用し、専門誌、ラジオ、リーフレット配布を展開。**ホームページ改修、支援機関等と連携した普及展開等を実施。	・お助け隊サービスを利用する**中小企業への普及啓発施策の検討を継続**すると共に、**サービスを提供する事業者の登録数の維持・増加を推進する**ための新たな施策を検討する。
	・中小企業のセキュリティ対策は、**企業の規模や位置づけに応じた施策が必要**。セキュリティ対策の解像度を上げ、業種や規模に応じた具体的な施策を検討することが求められる。 ・大企業が取引先と一緒に取り組めるような土壌があるとよい。**セキュリティ対策の成熟度を可視化する取組は評価**できる。	・サプライチェーンの実態を踏まえた**セキュリティ対策水準を評価する制度の検討を開始。**業種や規模に応じたレベルの設定、関連制度との整合性、対策推進のための企業支援のあり方等を**有識者によるSWG検討会で議論。**	・実証事業を通じて**要求事項・評価基準を確定**し、評価スキーム等の検討を進め、**令和７年度の運用開始を目指す。**併せて、**制度の導入促進**(お助け隊サービスとの連動、下請法等に係る課題の整理、関連ガイドラインへの記載等)**のための施策について検討を行う。**
	・大企業が取引先に対して**セキュリティ対策を要請するためのガイドラインが必要。**サプライチェーン全体のセキュリティ向上に向けたパートナーシップの構築が重要。	・取引先への**セキュリティ対策の要請に係る関係法令の適用関係の整理を開始。**	・サイバーセキュリティ対策の取引先への実施要請について、**ＳＣ３と勉強会を立ち上げて検討。**関係省庁と調整を進めて、**令和7年度に実施要請の想定事例を作成**を目指す。

前回のWG2ご意見への対応状況整理（２／２）

項目	前回の主なご意見	令和６年度の対応と成果	今後の対応
経営・中小企業（サプライチェーン対策）	・中小企業に対するセキュリティ対策の説明が重要であり、**具体的な事例を示すことで経営陣に理解を促す**べき。	・地域SECUNITY活動を通じて中小企業に対し**セミナー・机上演習等により普及・啓発を実施。**全国の**経産局を行脚し普及啓発の取組を共有**、関連団体、産業界とも連携しながら、施策を全国の企業に普及、拡大できる団体の増加を推進。	・地域のベストプラクティスの共有、**セキュリティ対策強化の活動を自発的に継続していくための更なる施策**を検討していく。 **・普及・啓発活動を行う支援機関が少ない地域において地域SECUNITY活動を活性化させるための方策**を検討する。
人材育成	・有資格者というよりも**能力ある人材の確保が重要**であり、**資格取得の需要を喚起する工夫**が必要。**既存の資格制度を活用し、民間資格との連携を図る**ことが求められる。 ・専門人材の育成において、受講者を増やすための**多様なプログラムが求められる。**人材の雇用状況に関するデータ収集が必要であり、育成された人材のキャリアパスをフォローアップすることが重要。	・セキュリティ対応において**支援が必要な中小企業とその支援が可能な専門家（登録セキスペ）とのマッチング実証を実施。** ・資格維持コストを低減するため、**資格更新時の講習の受講みなし制度を導入等の具体化**を検討。 ・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のβ版を作成。**	・実証の結果を踏まえ、**登録セキスペの得意分野・専門領域を可視化する「登録セキスペアクティブリスト」を整備。**支援テーマの拡充など、継続的なリストの掲載内容・運用改善を行い、併せて、マッチング主体・仲介者（支援機関やITベンダー）の役割や中小企業との関わり方を踏まえたアクティブリスト活用方法について検討を行う。 ・実践的方策ガイドの策定において、**取組事例の収集、有効性の確認、普及方法などの改善活動**を行っていく。
国際連携	・日本におけるサイバーセキュリティの取り組みについて、**海外であまり理解が進んでいない。取組や現状を国際発信できていない**のは国益上問題である。	・日本のサイバーセキュリティ対策の国際的な理解を促進するために、**ＡＳＥＡＮ向け施策情報発信を実施。（英語版ＨＰ更新、英語ガイドの掲載、日ASEAN会議にて取組紹介）**	・日本企業の取組紹介、汎用的なプラクティスの共有のための**情報発信を継続的に進めていく**と同時に**英語のコンテンツを充実**させていく。

４．今後の取組の方向性と本日ご議論いただきたい論点

今後の取組の方向性
　＜中小企業・サプライチェーン対策の強化＞
　＜人材育成＞
　＜国際連携＞

本日ご議論いただきたい論点
　＜中小企業・サプライチェーン対策の強化＞
　＜人材育成＞
　＜国際連携＞
　＜その他＞

今後の取組の方向性（１／２）

＜中小企業・サプライチェーン対策の強化＞

①サプライチェーン対策評価制度の構築に向けた更なる検討

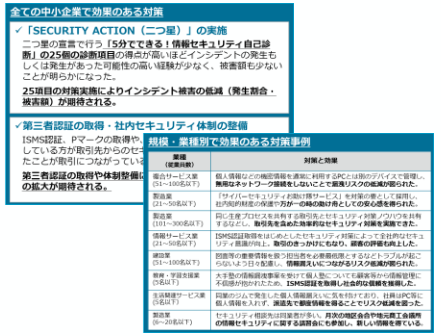
令和８年度の制度開始を目指し、実証事業等を通じて評価基準や評価スキーム等の具体化や制度整備を引き続き実施するとともに、同制度の活用促進に向けて、サイバーセキュリティお助け隊サービス等の利用促進や登録セキスペ等の外部専門家と中小企業のマッチングスキームの検討、セキュリティ対策の要請に係る関係法令の整理（具体的事例の整理）など関連施策の一体的な推進を図っていく。

②サイバーセキュリティお助け隊サービスの基準の見直し

お助け隊サービスの活用は徐々に広まる一方、価格上限や対象機器が限定されていること等により提供事業者が利益を上げられず撤退の動きが出始めていること、また境界防御モデルからゼロトラストへサイバーセキュリティ対策の軸が移っているなど技術動向の変化があることから、現行の基準などの見直しの必要性を今後検討。

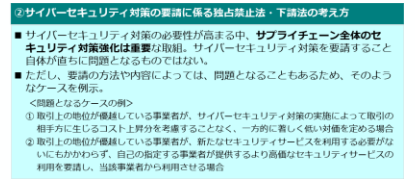
③中小企業のセキュリティ対策の実態調査

中小企業がサイバー攻撃に対する当事者意識を持っていただくために、現状のシステムの脆弱性の箇所と攻撃を受けた場合の想定被害額を可視化して、対策の必要性を認識していただくことが重要。そこで令和７年度ＡＳＭツールを用いた調査を実施して、診断結果を基に実施するべき必要な対策をまとめたプラクティス集を作成し、各地で啓発・広報を通じて中小企業が必要なセキュリティ対策の実施を促す。



④取引先とのパートナーシップの構築を目指す取り組み

サプライチェーン全体でサイバーセキュリティ対策の強化を促進していくため、大企業が取引先に対してセキュリティ対策を要請するためのガイドラインが必要という声がある中で、取引先とのパートナーシップの構築を目指す取り組みを進めている。今後、セキュリティ対策の要請に係る関係法令の整理を行い、関係省庁と連携し、また関係団体の意見も踏まえて、対策実施の想定事例としてまとめる。



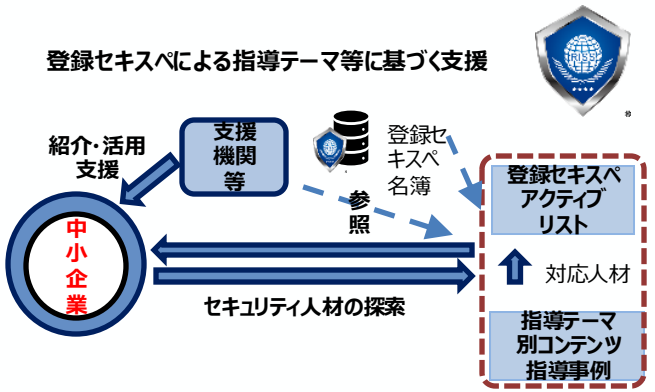
今後の取組の方向性（２／２）

＜人材育成＞

①登録セキスペの活用促進

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」の整備の実施と活用促進に向けた方策の具体化を図る。

※資格更新制度の見直しについても検討。



②中堅・中小企業内部のセキュリティ人材育成

「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」 の更なる改善を図る。

ＩＰＡの人材育成プラットフォーム等を活用しつつ、中小企業の人材育成に資する教育コンテンツの拡充。

＜国際連携＞

日本におけるサイバーセキュリティの取り組みについて、海外であまり理解が進んでおらず、取組や現状を国際発信できていない。その中でも、ASEAN地域は我が国企業が多く進出する重要なサプライチェーンであるため、セキュリティ体制の強靭化が重要。

このため、ASEAN地域に対する我が国政策の普及促進を進めるべく、日本国内で整備するガイドライン等を英語化のうえ、日ASEAN政府間会合にて展開を検討していく。

本日議論いただきたい論点（１／２）

＜中小企業・サプライチェーン対策の強化＞

サプライチェーン対策評価制度

論点１：サプライチェーン企業のセキュリティ向上を図るために構築中の本制度が有効活用されるために、今後、どのような点を意識して制度の具体化や制度普及に向けた取組・関連施策（サイバーセキュリティお助け隊サービス活用や外部専門家の助言等）と連携などを図っていくべきか。

サイバーセキュリティお助け隊サービス

論点２：本サービスの更なる普及や提供事業者の拡大、中小企業へのより効果的なサービスの提供などの観点から今後どのような対応が考えられるか。

中小企業のセキュリティ対策の実態調査

論点３：実証後に作成した事例集を中小企業に浸透させ、継続的に活用していただくための効果的な方法として、どのような対応が考えられるか。

取引先とのパートナーシップの構築

論点４：想定事例が大企業及び中小企業に活用されるために、考慮すべき点はどのようなことか。

本日議論いただきたい論点（２／２）

＜人材育成＞

登録セキスペ

論点１： アクティブリストの整備に際し、企業や組織が実際に活用しやすいものとするために必要な検討事項は何か。
論点２： 登録セキスペ制度の維持・発展のための産業界へ働きかけとして、どのような施策が有効と考えられるか。

実践的方策ガイド

論点３：中堅・中小企業向けの実践的方策ガイドを改善するために、どのようなコンテンツを取り入れていくのが有効か。
論点４：ガイドの普及促進のために、どのような組織と連携していくのが有効か。

＜国際連携＞

ガイドラインの海外情報発信

論点１：効果的にASEAN内で各種ガイドラインを浸透させるには、ASEANへの働きかけとしてどのような方策が有効と考えられるか。
論点２：ガイドラインの普及促進のために、どのような組織と連携していくのが有効か。

＜その他＞

ＷＧ２において今後取り組んでいくべき事項、議論していくべき論点についてのご意見。

METI
Ministry of Economy, Trade and Industry

経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html