経済産業省

第１２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８年３月3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検討体制及びWG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
第３回：平成31年　4月19日
第４回：令和　2年　4月17日※
第５回：令和　2年　6月30日
第６回：令和　3年　4月　2日
第７回：令和　4年　4月11日
第８回：令和　6年　4月　5日
第９回：令和　7年　5月23日

※電話開催

＜構成員＞　※2026年4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

星野　理彰　NTT株式会社　代表取締役副社長、副社長執行役員 CTO

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＞
国家サイバー統括室、警察庁、金融庁、デジタル庁、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、防衛装備庁

WG１（実効性強化・国際連携）

- 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

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

WG２（地域・中小企業支援）

- 地域・中小企業等における対策支援

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
第12回：令和8年3月　3日

WG３（産業振興・人材育成）

- セキュリティ産業振興、研究開発
- 人材育成・確保

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
第９回：令和 7年4月17日

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
- サイバー対処能力強化法
- サイバーセキュリティ戦略（中小企業関係）
- サイバーセキュリティ政策に関する国際的な動向
- 中小企業実態調査結果と中小企業に対するサイバー攻撃の現状

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

- 2021年以降、中国を背景とするグループ「Salt Typhoon」による、**政府や軍事インフラを含む世界中のネットワークを標的に、公開された脆弱性等を利用してアクセスし、データ窃取**等を行う活動が観測されている。（2025年8月 国家サイバー統括室及び警察庁が国際アドバイザリーに共同署名）

② 事業活動の停止

- 2025年9月、英自動車大手ジャガー・ランドローバー社において、**サイバー攻撃の影響により生産・小売活動が停止**。英国非営利団体は「約3,900億円以上の経済損失が生じた、英国史上最も被害の大きいサイバー攻撃である」と報告。
- 2025年9月、アサヒグループホールディングス㈱において、**ランサムウェア攻撃の影響により**国内の酒類や飲料、食品の**受注・出荷業務が停止。主要工場での製造も一時停止**するとともに、情報漏えいの可能性も確認。
- 2025年10月、アスクル㈱において、**ランサムウェア攻撃の影響により受注・出荷業務が停止**。ネット通販の配送をアスクルのグループ会社に委託する良品計画㈱等においてもネットストアでの受注・出荷業務が停止。情報漏えいも確認。

③ 重要インフラの機能停止等

- 2025年12月、ポーランドの**風力・太陽光発電所、熱電併給プラント等を標的とした、冬季の電力高需要期を狙ったとみられる大規模なサイバー攻撃キャンペーン**が行われた。攻撃者についてはロシアが支援するAPTグループとの関連が指摘されている。

④ サプライチェーン・委託先等への攻撃を起点とした情報漏えい

- 2025年3月、日鉄ソリューションズ㈱において、**ネットワーク機器へのゼロデイ攻撃を原因とした不正アクセス**を受け、同社のサーバー内に保存されていた、過去の**業務委託元などの取引先の個人情報を含む情報の漏えい**可能性を確認。

（参考）情報セキュリティ10大脅威の10年間の変遷（2017～2026）

- 近年、「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」が１位・２位 を占めている状況であり、**中小企業にとってサイバー攻撃は他人事ではない**状況にある。

脅威の種類		順位の変遷									
		2017	2018	2019	2020	2021	2022	2023	2024	2025	2026
1	ランサム攻撃による被害	2	2	3	5	1	1	1	1	1	1
2	サプライチェーンや委託先を狙った攻撃	-	-	4	4	4	3	2	2	2	2
3	AIの利用をめぐるサイバーリスク	-	-	-	-	-	-	-	-	-	3
4	システムの脆弱性を悪用した攻撃	-	4	9	-	10	6	8	7	3	4
5	機密情報を狙った標的型攻撃	1	1	1	1	2	2	3	4	5	5
6	地政学リスクに起因するサイバー攻撃（情報戦を含む）	-	-	-	-	-	-	-	-	7	6
7	内部不正による情報漏えい等	5	8	5	2	6	5	4	3	4	7
8	リモートワーク等の環境や仕組みを狙った攻撃	-	-	-	-	3	4	5	9	6	8
9	DDoS攻撃（分散型サービス妨害攻撃）	4	9	6	10	-	-	-	-	8	9
10	ビジネスメール詐欺	-	3	2	3	5	8	7	8	9	10

連続選出

初選出

サイバー対処能力強化法及び同整備法の全体像

- 国家安全保障戦略（令和４年12月16日閣議決定）では、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるとの目標を掲げ、①**官民連携の強化**、②**通信情報の利用**、③**攻撃者のサーバ等への侵入・無害化**、④**NISCの発展的改組・サイバー安全保障分野の政策を一元的に総合調整する新たな組織の設置** 等の実現に向け検討を進めるとされた。
- これら新たな取組の実現のために必要となる法制度の整備等について検討を行うため、令和６年６月７日からサイバー安全保障分野での対応能力の向上に向けた有識者会議を開催し、同年１１月２９日に提言を取りまとめ。
- この提言を踏まえ、令和7年2月7日に**「サイバー対処能力強化法案」及び「同整備法案」**を閣議決定。国会での審議・修正を経て、**同年５月16日に成立、同月23日に公布**。

概　要

総　則
- 目的規定、基本方針等（第１章）

官民連携（強化法）
- 基幹インフラ事業者による
  - 導入した一定の電子計算機の届出
  - インシデント報告

  （第２章）
- 情報共有・対策のための協議会の設置（第９章）
- 脆弱性対応の強化（第42条）

（その他、雑則（第11章）、罰則（第12章））

通信情報の利用（強化法）
- 基幹インフラ事業者等との協定（同意）に基づく通信情報の取得（第３章）
- （同意によらない）通信情報の取得（第４章、第６章）
- 自動的な方法による機械的情報の選別の実施（第22条、第35条）
- 関係行政機関の分析への協力（第27条）
- 取得した通信情報の取扱制限（第５章）
- 独立機関による事前審査・継続的検査 等（第10章）

→ 分析情報・脆弱性情報の提供等（第８章）←

アクセス・無害化措置（整備法）
- 重大な危害を防止するための警察による無害化措置
- 独立機関の事前承認・警察庁長官等の指揮 等（警察官職務執行法改正）
- 内閣総理大臣の命令による自衛隊の通信防護措置（権限は上記を準用）
- 自衛隊・日本に所在する米軍が使用するコンピュータ等の警護（権限は上記を準用）　等（自衛隊法改正）

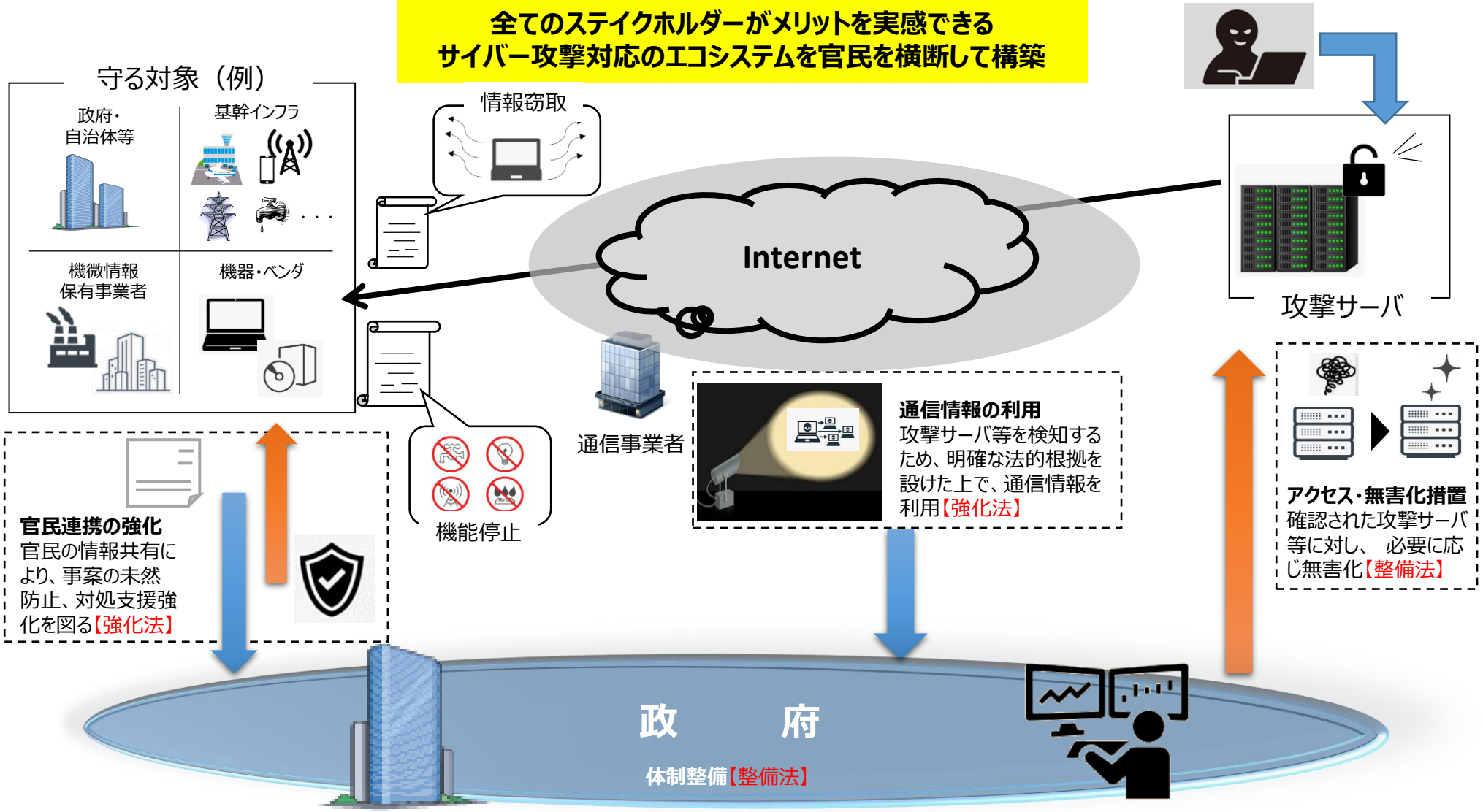
組織・体制整備等（整備法）
- サイバーセキュリティ戦略本部の改組、機能強化（サイバーセキュリティ基本法改正）
- 内閣サイバー官の新設（内閣法改正）　等

施行期日　公布の日（令和7年5月23日）から起算して1年6月を超えない範囲内において政令で定める日　等

（参考）サイバー対処能力強化法及び同整備法の全体イメージ

「国民生活や経済活動の基盤」と「国家及び国民の安全」をサイバー攻撃から守るため、能動的なサイバー防御を実施する体制を整備する。

全てのステイクホルダーがメリットを実感できる
サイバー攻撃対応のエコシステムを官民を横断して構築



サイバーセキュリティ戦略の全体像

- 令和７年12月23日に閣議決定された「サイバーセキュリティ戦略」には、**中小企業を含めたサプライチェーン全体のレジリエンス確保が重要な方向性の一つ**として位置づけられている。
- 経済産業省では、本戦略に基づき、中小企業を始めとした個々の民間企業等における対策の強化に向け、**サイバーセキュリティお助け隊サービスの制度拡充やセキュリティ専門家の活用促進などの中小企業支援策**を企画・実行していく。

「国家安全保障戦略」及び**サイバー対処能力強化法等**に基づく取組を含め、サイバー空間上の脅威に対応するための取組を一体的に推進するため、中長期的な視点から、**今後５年の期間を念頭に**、実施すべき諸施策の目標や実施方針を内外に示す。

情勢	厳しさを増す国際情勢と国家を背景としたサイバー脅威の増大	社会全体のデジタル化の進展とサイバー脅威の増大	AI、量子技術等の新たな技術革新とサイバーセキュリティに及ぼす影響
施策の方向性	**1. 深刻化するサイバー脅威に対する防御・抑止**	**2. 幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上**	**3. 我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成**

1. 深刻化するサイバー脅威に対する防御・抑止

- ✓ 厳しいサイバー安全保障環境に対応するため、官民連携・国際連携の下、事案対処等の従来の施策に能動的サイバー防御を含む多様な手段を組み合わせることで、攻撃者側にコストを負わせ、脅威を防御・抑止
- ✓ 政府から民間への積極的な情報提供

国が要となる防御・抑止

官民連携エコシステムの形成

国際連携の推進・強化

2. 幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上

- ✓ 様々な主体に求められる対策及び実効性確保に向けた方策の明確化・実施（政府機関等が範となり対策）
- ✓ デジタル化とセキュリティ確保の同時推進

政府機関等の対策強化

重要ｲﾝﾌﾗ事業者・地方公共団体等の対策強化

サプライチェーン全体のﾚｼﾞﾘｴﾝｽ確保（中小企業・ベンダー等）

全員参加によるサイバーセキュリティ向上

ｻｲﾊﾞｰ犯罪対策を通じた安全・安心の確保

3. 我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

- ✓ 産学官を通じたサイバー人材の確保・育成
- ✓ 国産を核とした、新技術・サービスの創出

効率的・効果的な人材の育成・確保

新たな技術・サービスのエコシステム形成

先端技術(AI、量子技術等)への対応・取組

官民連携・国際連携の下、広く国民・関係者の理解を得て、国が対策の要となり、官民一体で我が国のサイバーセキュリティ対策を推進
これにより、厳しさを増すサイバー空間を巡る情勢に切れ目無く対応できる、世界最高水準の強靱さを持つ国家を目指す。

サイバーセキュリティ政策に関する国際的な動向

- 欧米を中心に、①セキュア・バイ・デザイン*の概念に基づく**製品のサイバーセキュリティ対策に対する要請**や、②**企業のサイバーセキュリティ対策**水準の整備・可視化、③国内のサプライチェーン全体をカバーする**中小企業向けサイバー対策促進支援**の取組が進展。

＊ IT 製品（特にソフトウェア）が、設計段階から安全性を確保されていることを指す。

①IoT・ソフトウェア製品に対するセキュリティ要件

EU サイバーレジリエンス法

- デジタル要素を備えた製品（ソフトウェア含む）の製造者に対し、**①セキュリティ特性要件に従った上市前の設計製造、②上市後に積極的に悪用された脆弱性・インシデントの報告等を義務付け**。
- 報告義務の運用開始は2026年9月、その他は2027年12月開始予定。

PSTI法

- 英国内で主に消費者向けIoT機器の製造や流通、販売を行う事業者に対し、**3つのセキュリティ要件※を含むセキュリティ対策の遵守を義務付け**。
- 2024年4月に適用開始。

※共通パスワード設定の禁止、脆弱性情報の提供、セキュリティサポート期間の明示。

②企業のサイバーセキュリティ対策水準の整備・可視化

サイバー・エッセンシャルズ

- 英国NCSCが全ての**企業を対象に**一般的なサイバー攻撃への防御策を提供することを目的として設計した、自己適合、第三者診断の**二段階で構成される認証制度**。
- 一部政府及び公的機関の調達において必須要件として課される場合がある。

※豪州においても、すべての組織を対象とする４段階の基準（エッセンシャル・エイト）が存在。
※米国においても、米国防省がその請負業者等と共有する機密性の高い情報の保護を目的に設計したサイバーセキュリティ成熟度モデル認証（CMMC。2023年12月に2.0版が発効。）が存在。

③中小企業向けサイバーセキュリティ対策促進支援

サイバー・アクション・ツールキット

- 英国NCSCが**個人事業主・小規模組織向けにサイバーセキュリティ対策支援ツールを無料で提供**。（2025年10月公表）

サイバー・エッセンシャルズ取得支援

- 英国NCSCがサイバー・エッセンシャルズの**認証取得を支援するツール**（準備計画策定支援、自己評価質問票等）を提供。

小規模事業者サイバーセキュリティパイロットプログラム

- 米国中小企業庁が州政府を通じて、サイバーセキュリティ対策が困難な**中小企業向けにサイバーセキュリティ対策の研修やコンサルティングを提供**。

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（IPA調査）

- IPAは、中小企業4,191社を対象に情報セキュリティ対策に関する実態調査を実施。
- 業種問わずに効果的なサイバーセキュリティ対策として、**①SECURITY ACTION自己宣言（SA宣言）の 二つ星に掲げる対策項目を多く実施（→インシデント被害の低減が期待）、②第三者認証（ISMS認証、Pマーク）を取得するなどサイバーセキュリティ対策の実施状況を可視化（→取引先の信頼獲得・取引につながることが期待される）**が挙げられる。
- また、中小企業が実施している**具体的な対策事例**や企業が実感した**具体的な効果（生声）を紹介**。業種に応じてサイバーセキュリティ対策の目的（期待される効果）も異なることから、それぞれの業種において多くの企業が実施している取組を参考とすることも有用（認証の取得、機器の導入、教育の実施、保険への加入等）。

1 SECURITY ACTION 二つ星に掲げる対策項目を実施することの効果

➡ 実態調査の結果によれば、**SECURITY ACTION 二つ星に掲げる対策項目を多く実施**している企業ほど、**サイバーインシデント被害が少なく、被害額も少ない**ことが明らかとなった。

2 第三者認証（ISMS認証、Pマーク）を取得することの効果

➡ 実態調査の結果によれば、**第三者評価制度（ISMS認証、Pマーク）を取得している企業**は、取得していない企業よりも、取引先からのセキュリティ対策要請に応じたことが**取引につながった**大きな要因と考える割合が約2倍であった。

※セキュリティ体制の整備、リスク認識の有無についても同様の結果となった。

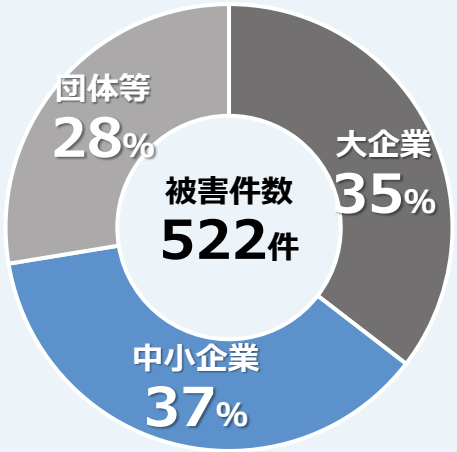
企業が実施している主な対策と具体的効果の例

業種	主な対策	主な効果
建設業	セキュリティ体制の整備	**「取引先からの信頼を得て受注が増えた」**
製造業	セキュリティ体制の整備、「サイバーセキュリティお助け隊サービス」などセキュリティ機器の導入	**「顧客からの信頼獲得による受注増や特命発注の獲得」**
情報通信業	ISMSの取得、セキュリティ体制の整備、セキュリティ教育の実施	**「お客様からの信頼感が違うのと、業界全体では当たり前だという認識を社内で共有できた」**
小売業	セキュリティ教育の実施	**「顧客情報の漏洩を防ぐことができるという安心感を得られた」**
金融業 保険業	セキュリティ体制の整備、セキュリティ教育の実施、サイバー保険への加入	**「従業員の意識が変わり、サイバーに関しての情報を認知し事前対策を講じるようになった」**

中小企業のサイバー被害状況とサプライチェーンへの影響

- 大企業に限らず**中小企業も相当数のサイバー攻撃の被害を受けており**、その影響として**取引先・サプライチェーンにも影響を及ぼしている場合が多い。**

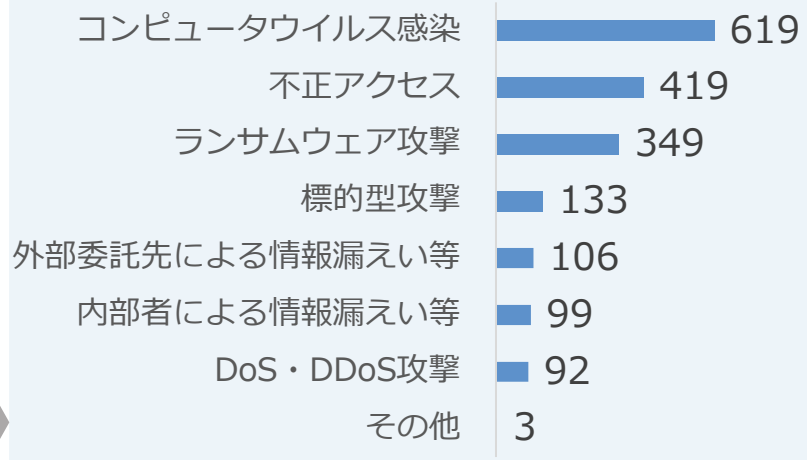
サイバー攻撃の被害組織の規模別割合（2022年７月～2024年6月）



直近２年間のサイバー攻撃による被害の**約４割**を中小企業が占めているという結果から、大企業に限らず、多くの中小企業においてもサイバー攻撃の被害が現実に発生している状況

出典：JNSA「インシデント損害額調査レポート別紙 2025年版」を基に経済産業省作成

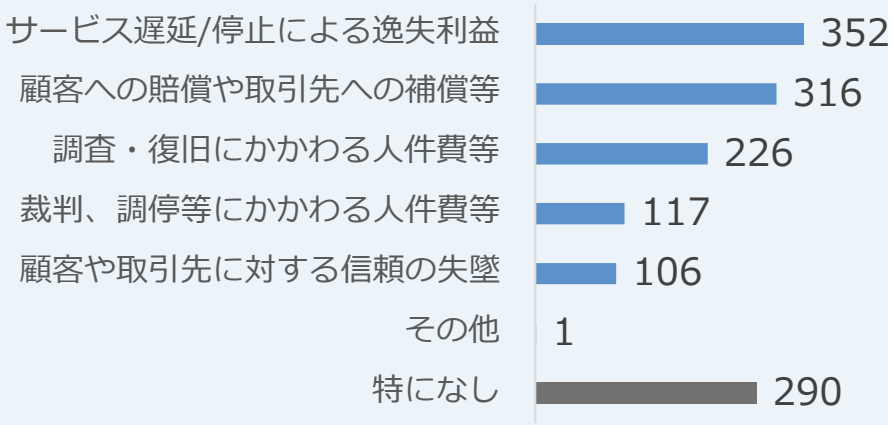
中小企業が実際に受けたサイバーインシデント（複数選択可、回答企業975社）



約1/4の中小企業が1年間（2023年4月～2024年3月）にサイバーインシデントの被害を受けたと回答
その内訳は、コンピュータウイルス感染や不正アクセス、ランサムウェア攻撃など**形態は様々**

出典：IPA「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

サイバーインシデントによるサプライチェーンへの影響（複数選択可、回答企業975社）



サイバーインシデントの被害を受けたと回答した975社のうち、**685社**がサイバーインシデントにより取引先（サプライチェーン）に影響があったと回答
その割合は**70.3%**

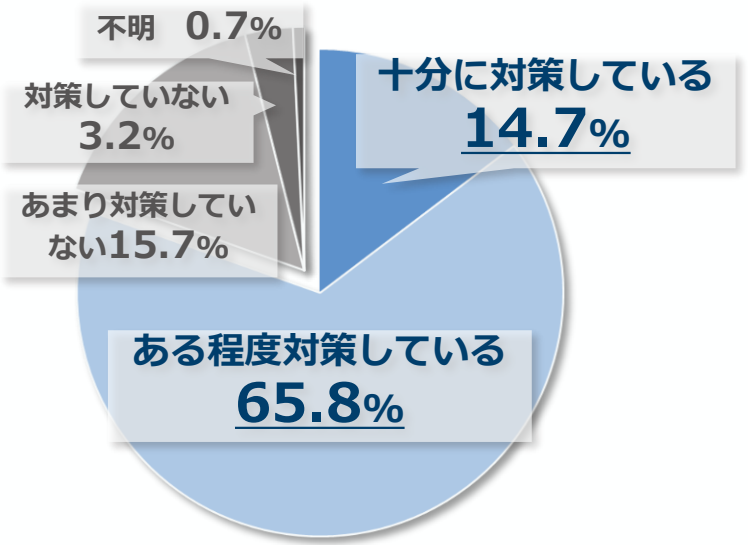
出典：IPA「2024年度中小企業における情報セキュリティ対策に関する実態調査」を基に経済産業省作成

中小企業によるサイバーセキュリティ対策の状況と課題

- 東京商工会議所による調査では、中小企業の**約８割がサイバーセキュリティ対策を行っている**と回答。
- 一方、対策の内訳を見ると、「ウイルス対策ソフトのインストール」「OS／ソフトウェアの定期的なアップデート」など**基礎的な内容が中心**で、「サイバーセキュリティ訓練の実施」「サイバーセキュリティ専門人材の雇用・育成」などの**組織的な対策は低水準に留まる**。

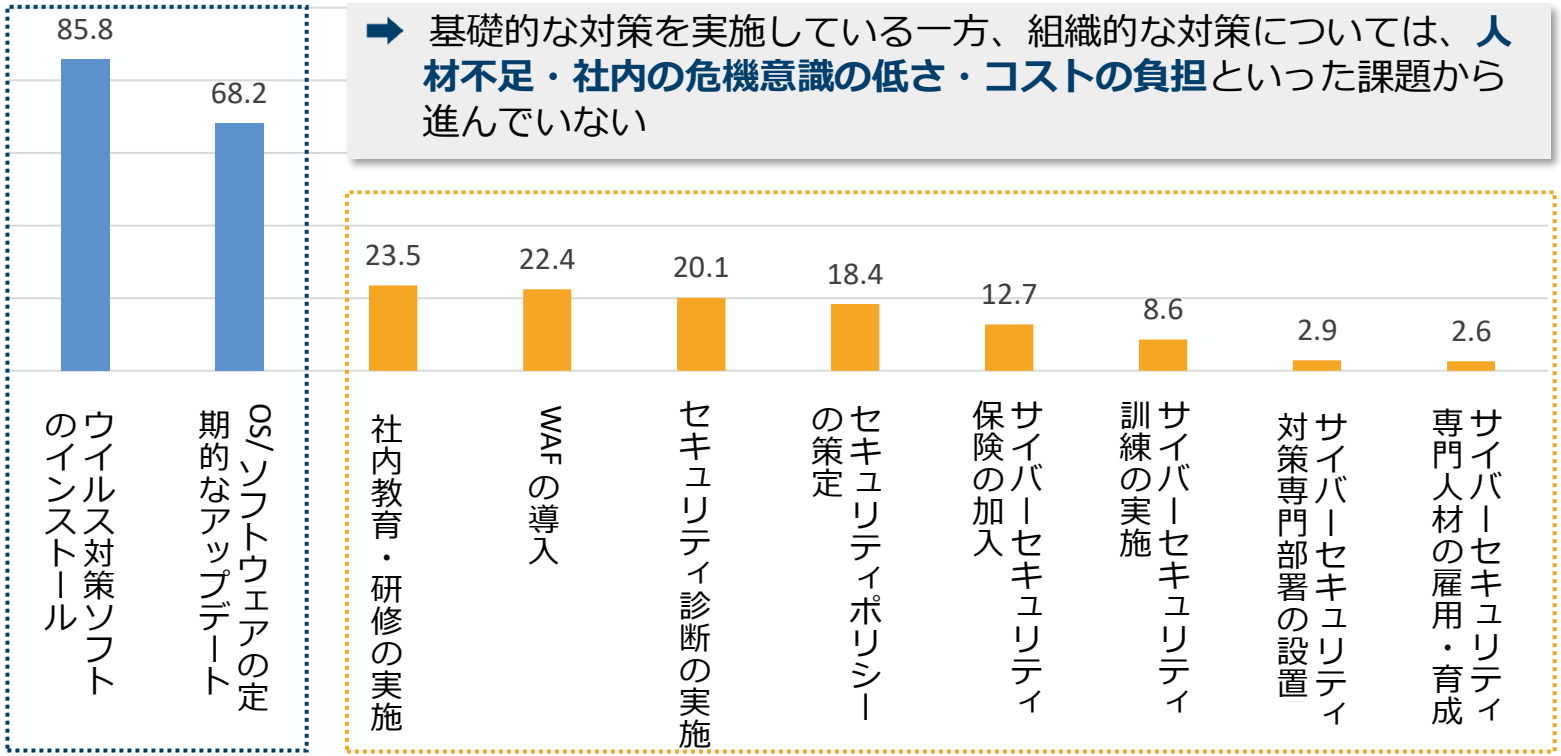
サイバーセキュリティ対策の状況

n＝1,218社(中小企業)



➡**80.5%がサイバーセキュリティ対策を実施**していると回答

サイバーセキュリティ対策の内訳



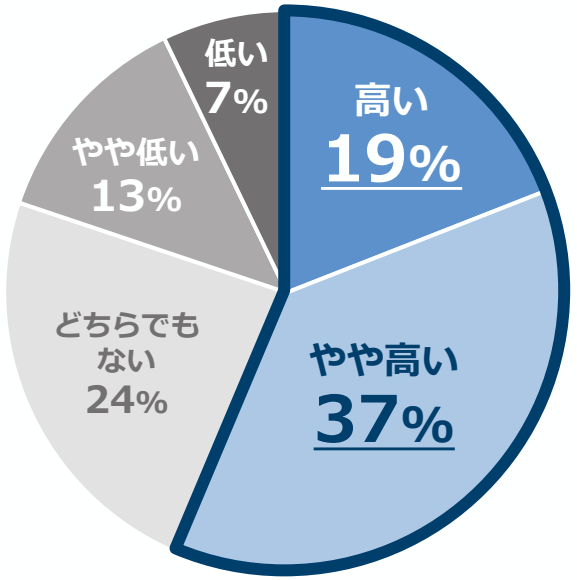
➡ 基礎的な対策を実施している一方、組織的な対策については、**人材不足・社内の危機意識の低さ・コストの負担**といった課題から進んでいない

出典：「中小企業のデジタルシフト・DX実態調査集計結果」（2025年1月10日） 中小企業のデジタルシフト・DX推進委員会（東京商工会議所ホームページ掲載資料に基づき、経済産業省において作成）

中小企業による「組織的な対策」に対する意識の高まり

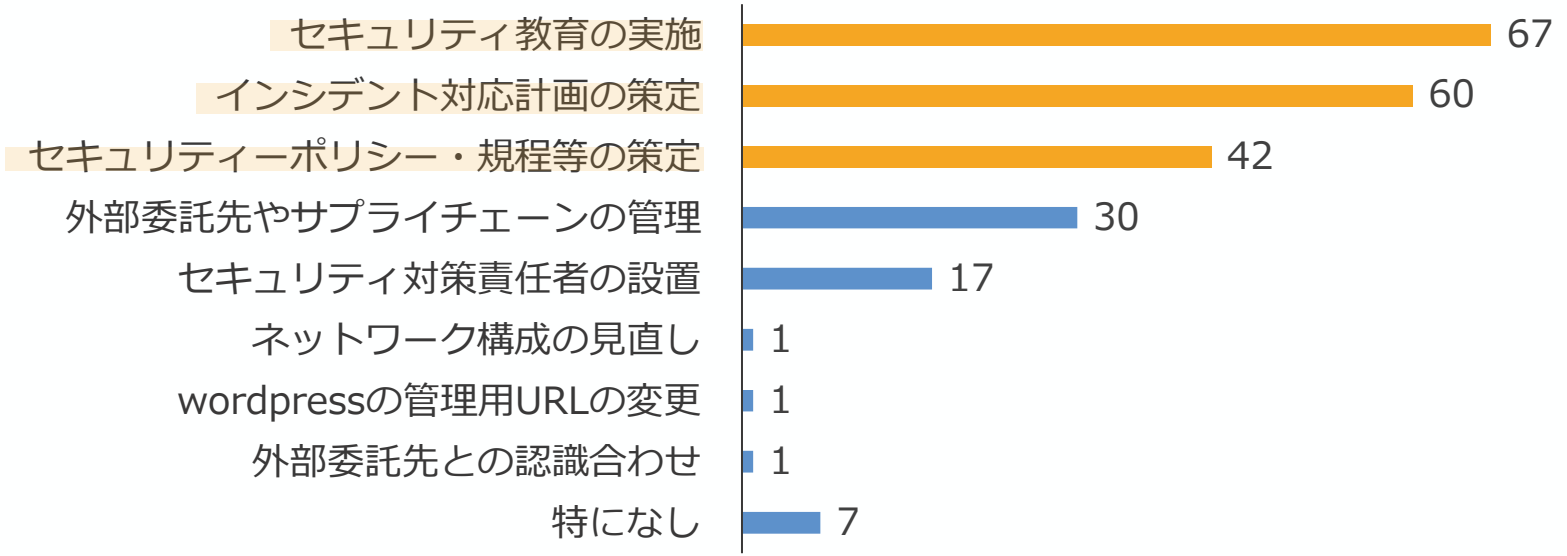
- 中小企業には組織的対策強化の課題があるものの、**経営層のセキュリティ対策に対する意識や、組織的対策の強化に対する意識は高い。**
- 中小企業が**組織的対策も含めたサイバーセキュリティ対策強化に取り組めるよう**、必要な支援策を講じていくことが必要。

経営層のセキュリティ意識
（単一選択、回答企業126社）



➡**56%が経営層のサイバーセキュリティ意識は高い**と回答しており中小企業の意識向上が見られる。

今後強化したい組織的なセキュリティ対策
（複数選択可、回答企業126社）



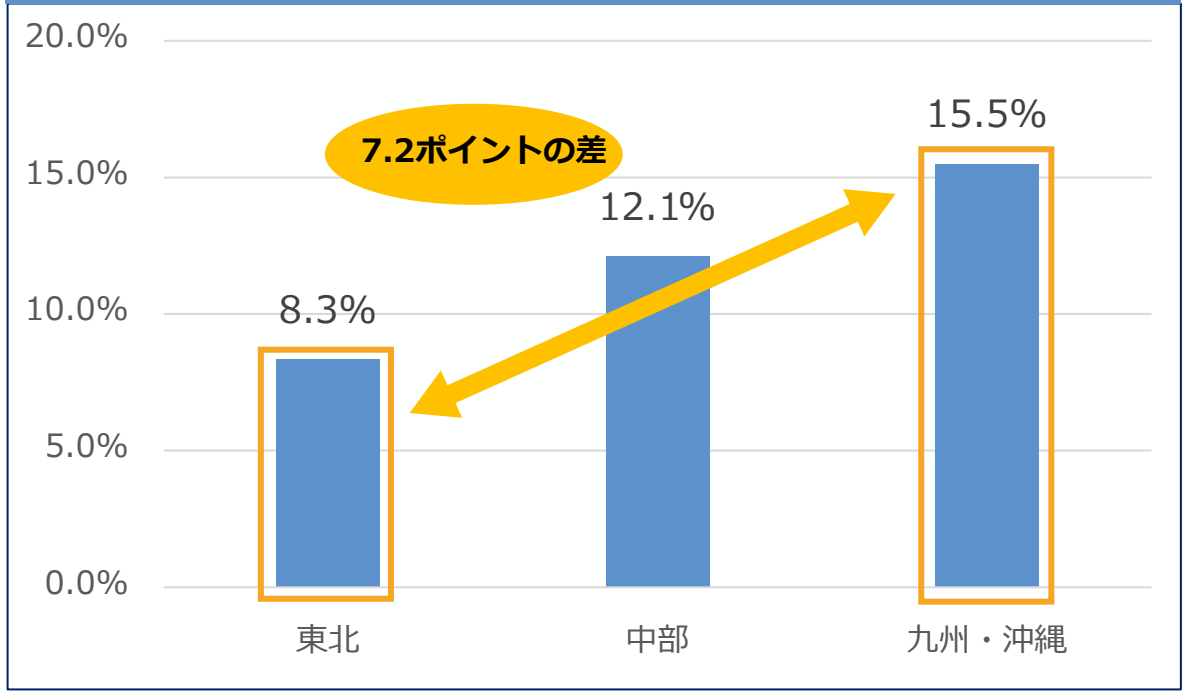
➡実証を通じて、**セキュリティ教育・インシデント対応計画策定・セキュリティポリシー策定などの組織的対策に対する意識の高まり**が見られた。
➡中小企業に対し、ガイドラインの改訂により具体的な対策方法を提示するなど、対策の底上げを図っていく。

出典：IPA「ASM診断および事例集作成業務」に参加した中小企業126社を対象に実施したアンケート結果（令和７年９月）を基に経済産業省作成

地域におけるサイバーセキュリティ対策状況のバラツキ

- 地域により、**中小企業のサイバーセキュリティ対策の状況**や、**セキュリティ人材の人数**に**差がみられる。**
- 特に活動が活発でない地域を中心に、中小企業支援機関と連携した**サイバーセキュリティ対策の普及・啓発を後押し**することで、サイバーセキュリティの地域差を生じさせないための取組が必要。

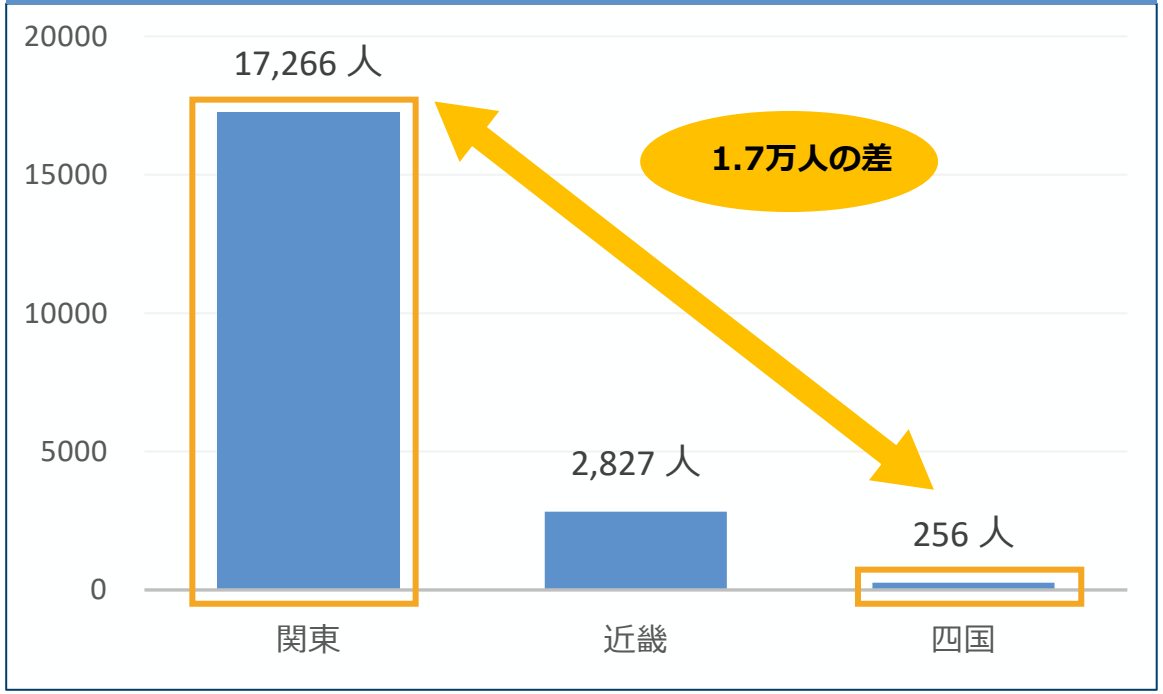
SA自己宣言者数の割合（令和7年12月時点）



➡**SA自己宣言者数の割合は、地域によって様々**であり、**東北地域の自己宣言者数割合は8.3%**に留まる。

出典：IPA提供データ（令和7年12月末時点）及び中小企業庁「令和3年経済センサス-活動調査」を基に経済産業省作成

情報処理安全確保支援士登録者数（令和8年10月時点）



➡**登情報処理安全確保支援士（登録セキスペ）登録者数は、地域毎に大きな差**があり、最も多い地域と少ない地域の間には**約1.7万人の差**が見られる。

出典：情報処理安全確保支援士登録者について（2025年10月1日時点）を基に経済産業省作成

２．令和７年度の主な施策の取組状況

- 経済産業省の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強化に向けた取組状況と今後の方針
- サイバーセキュリティ人材の育成促進に向けた検討会とその後の対応

経済産業省のサイバーセキュリティ政策の全体像及び今後の方向性

- NCO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
- 我が国の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）
- SCS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

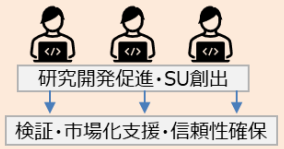
③政府全体でのサイバーセキュリティ対応体制の強化

- 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強化に向けた取組状況と今後の方針

課題	サプライチェーンに及ぼすリスクが増す中、組織的対策を含めたサイバーセキュリティ対策が不十分	地域・企業によって、サイバーセキュリティ対策の取組状況にバラツキがある
対策の方向性	**サプライチェーン全体での対策強化** 中小企業等が最低限実施すべき取組の可視化と実装支援	**地域SECUNITY活動の促進** コンテンツの充実化と支援機関による活動支援
現状の対策	各企業の満たすべきセキュリティ対策を提示した上でその対策状況を可視化する仕組みとして、**SCS評価制度の構築**を検討。制度開始に向け、以下、**本制度に対応した中小企業への取組を推進**。 ・SCS評価制度の対策要請にあたり、独占禁止法や取適法上「問題ない」とする**想定事例**を公表。 ・**中小企業の情報セキュリティ対策ガイドライン**を改訂。 ・SCS評価制度“★”取得支援可能な**登録セキスペ**の育成に資する指導ツールを策定。	・被害事例などから中小企業にセキュリティ対策の必要性を理解いただくための**「事例集」**を作成。 ・中小企業が実施すべきセキュリティ対策に応じた**人材確保・育成の実践的方策ガイド**を作成。 ・**地域SECUNITY連絡会**等で地域事例共有、普及啓発を実施 ・地域セミナー等で**登録セキスペによる相談会**を実施。 ・外部専門人材の探索負担軽減に向け、**支援可能な登録セキスペのリスト**を整備・公表。
今後の方向性	・SCS評価制度に対応した**サイバーセキュリティお助け隊サービス（新類型）の創設**と、価格要件等を検証する実証事業を実施。 ・作成した**想定事例の普及**に向けた周知・広報を実施。	・SCS評価制度“★”取得支援や機微情報を扱う業界支援に対応できる登録セキスペを育成し、**中小企業・支援機関による登録セキスペのリストの活用を促進**。	・インシデント対応力強化に向け**机上演習コンテンツを作成し、地域SECUNITYを通じた活用を図る**。 ・**東北地方の地域SECUNITY活性化のため**、セミナー・机上演習等の複合イベントを実施。

サイバーセキュリティ人材の育成促進に向けた検討会とその後の対応

「サイバーセキュリティ人材の育成促進に向けた検討会最終取りまとめ」より抜粋し、一部更新

- 我が国においてサイバーセキュリティ人材が不足しているとの声は多く、国内で約17万人不足しているとの民間調査結果※もある。
  （出典）ISC2 Cybersecurity Workforce Study 2024
- サイバーセキュリティ人材の不足に対応するためには、トップ人材や高度専門人材から、地域の中小企業等でセキュリティ対策を推進する人材まで、各層の課題に応じた施策を戦略的に進めることが重要。
- このため、これまで一定の効果を生み出している既存の施策の拡充・改善をベースとして、実際に政策ニーズを有する組織の方へのヒアリング等も通じ、令和７年５月に政策対応の方向性を取りまとめ。検討会を踏まえ、各施策の継続的な改善を実施。

対応の方向性

①セキュリティ・キャンプ※の拡充

※世界に通用するトップクラスの人材を育成・発掘する取組

- AI等の特定領域と掛け合わせた高度セキュリティ人材の育成を目的とする新たな「キャンプ」を実施
- 修了生の継続的な知見研鑽・社会還元・活躍状況共有等を目的とした「コミュニティ」を整備

②登録セキスペ※の活用促進

※セキュリティに係る専門的な知識・技能を備えた国家資格（情報処理安全確保支援士）

- 個社の状況に応じた個別相談・支援等が可能な登録セキスペのリストを整備し、中小企業支援機関等を通じて中小企業との人材マッチングを促進
- 更新時に受講すべき講習について、所定の実務経験を有する者を対象とした新たな講習制度を創設　等

③中小企業等における人材確保策の提示

- 中小企業が実施すべきセキュリティ対策に応じた人材確保・育成の実践的方策ガイドをβ版として整理
- 人材を「育成」する際に参照できる教材・資格等も提示

現在の取組

- 「セキュリティ・キャンプコネクト」として新たなキャンプを開催（令和8年3月末予定）
- 修了生向けコミュニティの活動開始（令和8年3月末予定）

- 登録セキスペのリストについて、整備・運用を開始
- SCS評価制度と連携した指導テーマの拡充
- 「実務経験者に対する講習制度」を創設（令和8年4月より申請受付開始予定）

- 中小企業に対するヒアリング等を実施しながら成案化
  （令和8年3月末公表予定）
  ※登録セキスペのリストの活用方法も提示

目指す効果

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

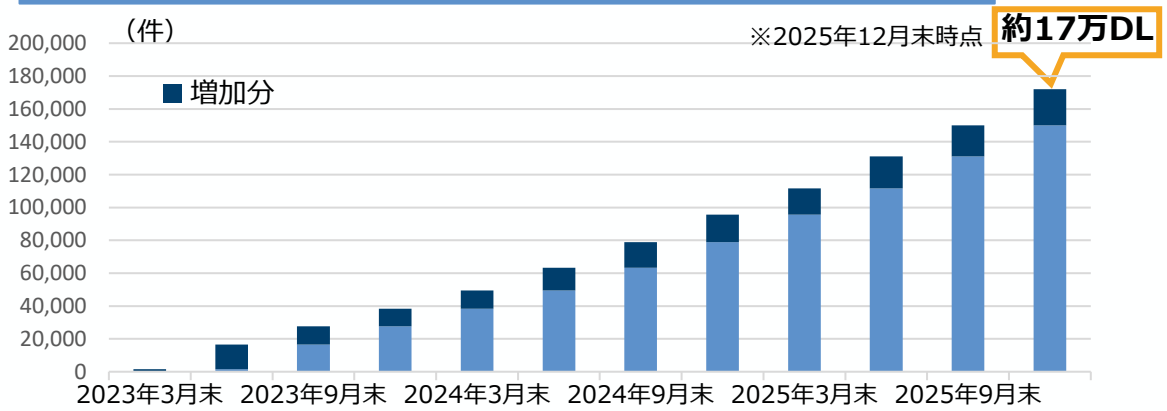
- 登録セキスペの活躍機会（中小企業のセキュリティ確保等の実務経験機会）増加
- 登録セキスペ資格更新時の負担軽減
- 中小企業におけるセキュリティ人材探索コストの低減
- 中小企業内での内部人材育成容易化

2030年までに登録セキスペ５万人
（2025年10月時点で約2.5万人）を達成

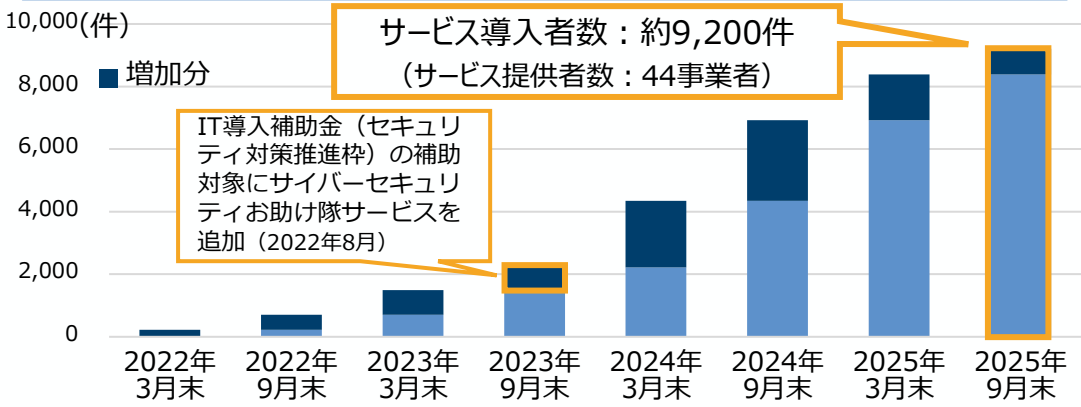
（参考）ガイドライン・各種施策の普及状況

- 「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**約17万件**まで到達。
- 補助金の申請要件化を通じてSECURITY ACTION自己宣言者数が拡大。宣言数は**約45万件**まで到達。
- サイバーセキュリティお助け隊サービス導入件数は**約9,200件**まで到達。
- 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

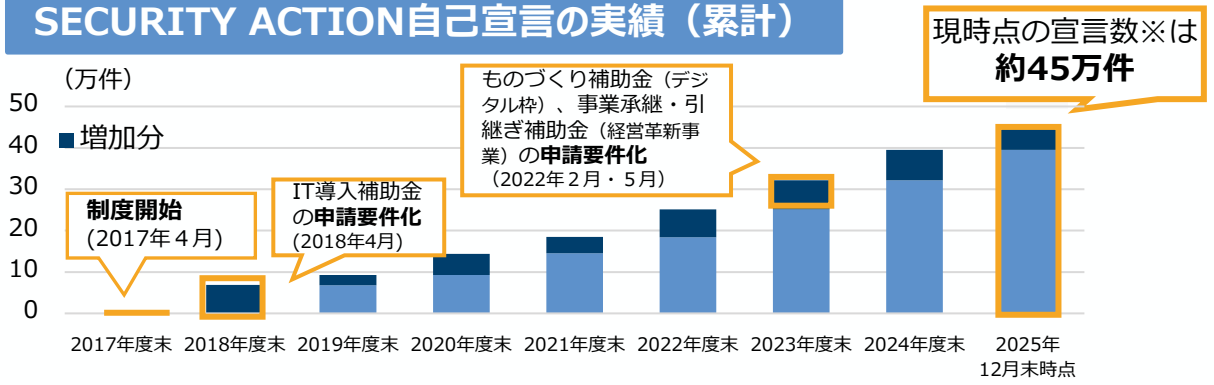


サイバーセキュリティお助け隊サービス導入実績（累計）



※サービス提供者数は2025年12月末時点

SECURITY ACTION自己宣言の実績（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～2025年)
情報処理安全確保支援士	24,937名(2025年10月時点)
セキュリティ・キャンプ参加者数	全国大会：1,311名(2004年～) ネクストキャンプ：62名(2019年～) ジュニアキャンプ：18名(2023年～)
IPA　セキュリティ講演者派遣	108件(2026年2月時点)
IPA　セキュリティセミナー支援	セミナー開催支援：21件 経営者向けインシデント机上演習WS：19件(2026年2月時点)

２．令和７年度の主な施策の取組状況

（１）サプライチェーン全体での対策強化

- 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（SCS評価制度）
- SCS評価制度を中心とした中小企業支援策の新たな体系

① サイバーセキュリティ対策要請と関係法令整理に係る想定事例

② サイバーセキュリティお助け隊サービス（新類型）制度創設と実証事業に向けた検討

③ 中小企業の情報セキュリティ対策ガイドライン改訂

④ 情報処理安全確保支援士を活用した中小企業支援

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（SCS評価制度※1）の概要

※1 SCS（supply chain security）評価制度

- 「対策状況は**外部から判断が難しい**」「**複数の取引先から様々な対策を要求**される」等の課題に対し、サプライチェーンにおける重要性を踏まえた上で満たすべき対策※2を提示しつつ、その状況を可視化する仕組み※3の構築※4を進めている。
- ２社間の取引契約等において、**発注企業が、受注側に適切な段階の”★”を提示**し、示された対策を促すとともに実施状況を確認することを想定。 本制度の活用促進を通じ、サプライチェーン全体でのセキュリティ対策水準の向上を図る。
- ３段階の水準のうち、★３・★４について、**令和８年(2026年)度末頃の制度開始**を予定。

※2　本制度では、サプライチェーンを構成する企業等のIT基盤が対象。
※3 発注時等に、必要なセキュリティ対応状況の可視化を目的としたもので、いわゆる「格付け」制度ではない。
※4 2025年12月26日に制度構築方針案を公表。2026年3月中に成案化予定。

構築する評価制度（案）

成熟度の定義	★３	★４	★５［検討中※5］
想定される脅威	• 広く認知された脆弱性等を悪用する一般的なサイバー攻撃	• 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	• 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全てのサプライチェーン企業が**最低限実装すべき**セキュリティ対策： • 基礎的な組織的対策とシステム防御策を中心に実施	サプライチェーン企業等が**標準的に目指すべき**セキュリティ対策： • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施	サプライチェーン企業等が到達点として目指すべき対策： • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善工程を整備、システムに対しては現時点でのベストプラクティスの対策を実施
評価スキーム	**専門家確認付き自己評価**	**第三者評価**	第三者評価

※5　ISMS適合性評価制度、★3・4との整合性も踏まえ、対策事項を今後検討

政府調達や重要インフラ事業者等での活用推進

取引先からの対策要請による活用促進

利害関係者への情報開示による対話の促進

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

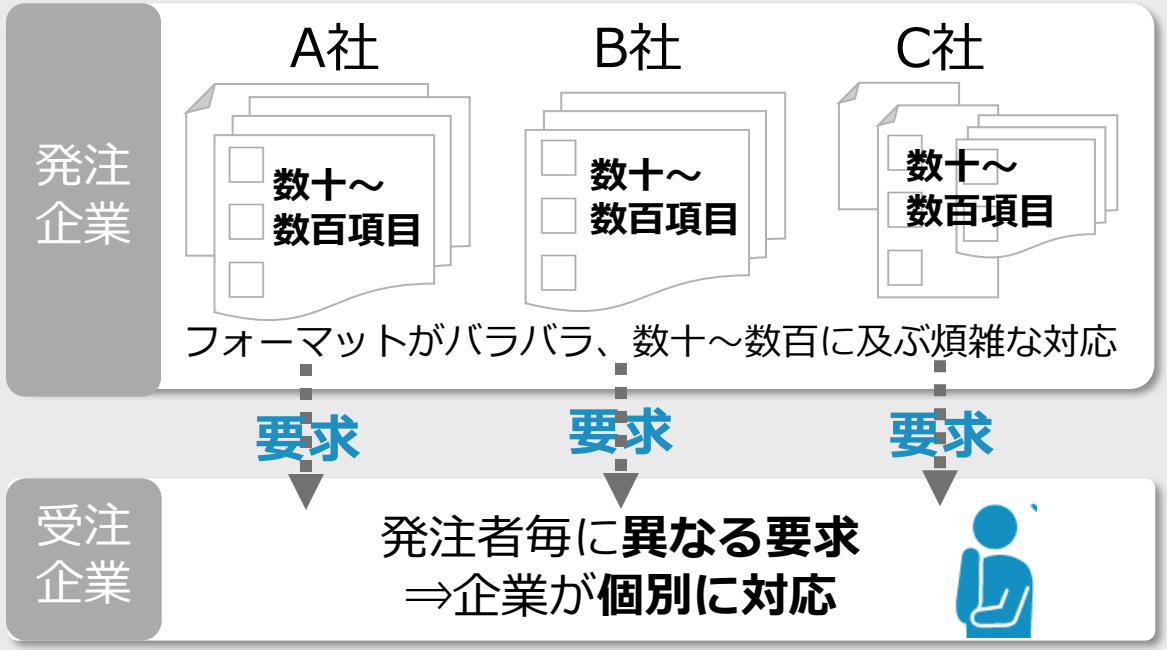
制度の普及施策（例）

想定される課題	中小企業等における”★”取得の負担		中小企業等における セキュリティ専門家の確保	サプライヤー企業への “★”取得要請時の関係法令の適用
普及施策	サイバーセキュリティお助け隊サービス（新類型）の創設	中小企業ガイドライン整備	専門家の活用促進	取引先への要請等に係る考え方の整理
	★3・★4に対応した、サイバーセキュリティお助け隊サービスの新たな類型創設により、安価な”★”取得を実現	中小企業の情報セキュリティ対策ガイドライン及び付録サンプル規程の整備により、”★”の取得を容易化	「中小企業向けサイバーセキュリティ専門家リスト」の整備により、中小企業と専門家とのマッチングを促進	取引先とのパートナーシップ構築促進に向けた想定事例及び解説案の策定により、費用に係る価格交渉を推進

（参考）中小企業がSCS評価制度の“★”を取得するメリット

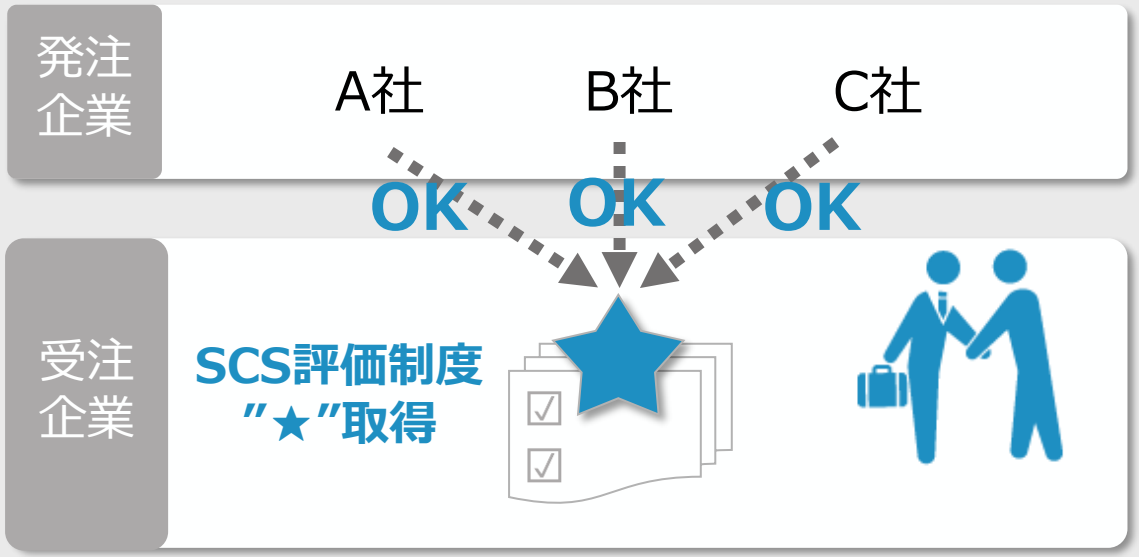
発注者ごとに異なる要求…対応が煩雑で非効率

- ✓ 発注者側からの**様々な要求に一つずつ対応**する必要がある
- ✓ 複数社と取引する場合、**それぞれの企業からの要求に対応**するのが困難
- ✓ 各企業の要求リストは似ていてもフォーマットがバラバラで、内容を理解していないと対応できず、**数百項目に及ぶ煩雑な対応が発生**



“★”取得で、発注者対応が一括クリア！

- ✓ SCS評価制度の“★”取得が、発注企業・受注企業双方にとっての**「共通のものさし」**となる
- ✓ 結果、各社からの要求に説明できるようになり、**対応工数削減や業務の標準化・効率化に繋がる**
- ✓ “★”取得済み企業は、発注者がどのレベルまで対応できているかが一目でわかりスムーズな取引が可能となり、**発注者との信頼構築に繋がる**



（参考）SCS評価制度とSECURITY ACTIONとの接続

調達側

強制はできないが、サプライヤーには
一定の対策（リスク低減策）をとってもらいたい

サプライヤー

一定の対策は必要と思うものの、
- 現実的な対策レベル感がわからない
- 各社から**異なる基準**を要請される

セキュリティ対策の範囲・内容

現時点でのベストプラクティス

包括的・標準的なセキュリティ対策

基礎的な組織的対策とシステム防御策

経営者・従業員への意識付け

SECURITY ACTION

一つ星・二つ星

SCS評価制度 ★3

サプライチェーン企業が**最低限実装すべき対策**

SCS評価制度 ★4

サプライチェーン企業が**標準的に目指すべき対策**

成熟度の定義	三つ星（★3）	四つ星（★4）
想定される脅威	• 広く認知された脆弱性等を悪用する一般的なサイバー攻撃	• 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃
対策の基本的な考え方	全てのサプライチェーン企業が最低限実装すべきセキュリティ対策： • 基礎的な組織的対策とシステム防御策を中心に実施	サプライチェーン企業等が標準的に目指すべきセキュリティ対策： • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施
評価スキーム	自己評価	第三者評価

※具体化の際に、既存認証制度との連携等スキームを検討

自工会・部工会ガイドライン LV3 等

ISO27000シリーズ（ISMS）

★5

※令和7年度以降に検討予定

組織におけるマネジメントシステムの確立
＋
システムへの具体的な対策実装

サプライチェーン強靭化への寄与

（寄与なし）経営者によるセキュリティ意識の宣言

自社のセキュリティ対策インシデント時の報告・共有

取引先を含めたセキュリティ対策

サプライチェーン全体に寄与するセキュリティ対策

（参考）制度で用いるセキュリティ要求事項・評価基準の概要

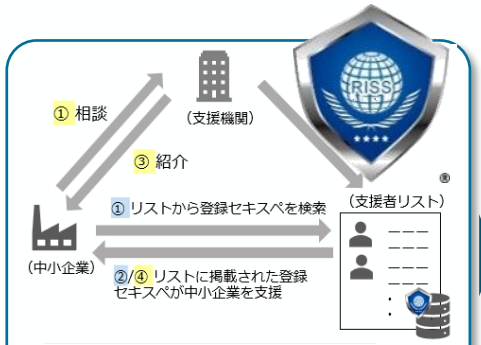
- NIST Cyber Security Framework(CSF)の機能に対応した６つの分類に、取引先管理に重点を置いた分類を加えた７つの分類において、それぞれレベルごと達成すべき対策を提案。詳細は別添を参照。要求事項・評価基準は、サイバーセキュリティの動向等を踏まえ今後定期的な見直しを想定。

[註] 以下は必ずしも全要求事項を網羅しているわけではない点に留意されたい。　[註] []内は要求事項No.を指す

大分類	★3	★4	NIST CSFにおける機能
ガバナンスの整備	**企業として最低限のリスク管理体制の構築** • 自社のセキュリティ担当の明確化 [No.1-2-1] • セキュリティ対応方針の策定 [No.1-3-1]	**継続的改善に資するリスク管理体制の構築** • 定期的な経営層への報告、不備の是正等 [No.1-4-1]	統治(GV)
取引先管理	**取引先に課す最低限のルール明確化** • 他社との機密情報の取扱い明確化 [No.2-1-2] • 接続している外部情報サービスの把握 [No.3-1-3]	**取引先の管理・把握及び取引先との役割・責任の明確化** • 機密情報共有先の把握 [No.2-1-1] • 重要な取引先等の対策状況把握 [No.2-1-3] • インシデント発生時の他社との役割等の明確化 [No.2-1-4]	
リスクの特定	**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把握 [No.3-1-1,3-1-2] • 外部情報サービスの管理 [No.3-1-3]	**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.3-2-1]	識別(ID)
攻撃等の防御	**不正アクセスに対する基礎的な防御** • ID管理手続、アクセス権限の設定[No.4-1-1,4-1-2] • パスワードの安全な設定及び管理 [No.4-1-4,4-1-5] • 内外ネットワーク境界の分離・保護 [No.4-5-1] **端末やサーバーの基礎的な保護** • 適時のアップデート適用、不要ソフトウェアの削除[No.4-4-1,4-4-4] • 端末等へのマルウェア対策 [No.4-4-1,4-4-4]	**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.4-3-1,4-3-2] • ログの収集・定期的な分析の実施 [No.4-4-3] • 社内システムにおける適切なネットワーク分離 [No.4-5-1] • 社外への不正通信の遮断(出口対策) [No.4-5-2]	防御(PR)
攻撃等の検知	**ネットワーク上の基礎的な監視等** • ネットワーク接続・データの監視[No.5-1-1]	**迅速な異常の検知** • 情報機器等の状態、挙動の監視・対応や分析[No.5-1-1,5-1-2]	検知(DE)
インシデントへの対応	**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.6-1-1]	*大分類「インシデントへの対応」において、★４での追加項目はなし	対応(RS)
インシデントからの復旧	**インシデント発生から復旧するための対策の整備** • インシデント発生から復旧するための対策の整備[No.7-1-1]	**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.7-1-1]	復旧(RC)

SCS評価制度を中心とした中小企業支援策の新たな体系

- 中小企業に対し、**SCS評価制度★３・★４水準のセキュリティ対策実施を後押しする**ため、各種施策を展開していく。



★3～4取得支援のための**人的支援**
（登録セキスペとのマッチング）

★3～4取得にむけた**きっかけ作り**
（補助施策と連動）

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（SCS評価制度）

成熟度の定義	★3	★4	★5［検討中※5］
想定される脅威	• 広く認知された脆弱性等を悪用する一般的なサイバー攻撃	• 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	• 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全てのサプライチェーン企業が**最低限実装すべき**セキュリティ対策： • 基礎的な組織的対策とシステム防御策を中心に実施	サプライチェーン企業等が**標準的に目指すべき**セキュリティ対策： • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施	サプライチェーン企業等が到達点として目指すべき対策： • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善工程を整備、システムに対しては現時点でのベストプラクティスの対策を実施
評価スキーム	専門家確認付き自己評価	第三者評価	第三者評価

★3～4を伴走支援
中小企業が導入しやすい価格でサービス提供

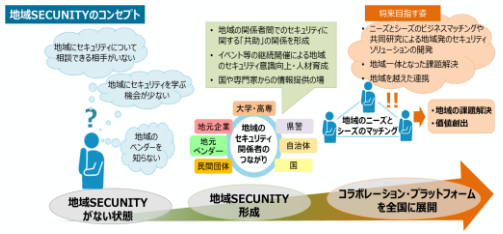
★3～4取得につながる**実践方策＋規程類ひな形**

パートナーシップ構築宣言

サイバー対策要請時の、
関係法令の適用関係明確化

支援機関等と連携した
面的な普及展開活動

【地域SECURITY】



（参考）【パートナーシップ構築文書】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）

２０２２年１０月２８日
経済産業省・公正取引委員会

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】

■ 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。

サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップ構築促進に向けた想定事例及び解説（概要）

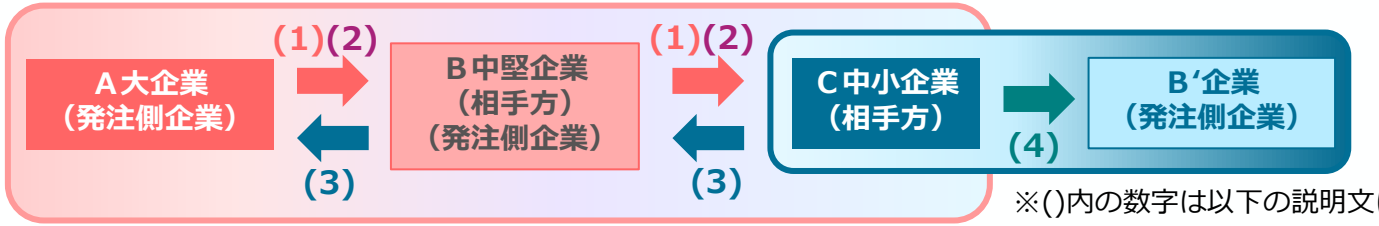
２０２５年１２月２６日
経済産業省・公正取引委員会

○　経済産業省及び公正取引委員会では、「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」を補足するため、**発注者・相手方双方を対象とした、独占禁止法・取適法上「問題とならない」想定事例及びその解説文書を作成。**

○　想定事例は、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（SCS評価制度）に基づく対策要請を円滑に行い、発注者側・相手方がパートナーシップを構築してセキュリティ対策と価格交渉を実施し、円満に合意するものとしている。

【想定事例】

【サプライチェーンのイメージと想定事例の各場面】



※()内の数字は以下の説明文に対応

(1) セキュリティ対策実施の要請

A（大企業）は、相手方であるB（中堅企業）に対し、①組織ガバナンス・取引先管理、システム防御・検知、事案対応等の対策の実施(＊)、②Bの相手方であるC（中小企業）に対し①と同様の対策を講ずることを要請。

(＊)**「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（SCS評価制度）」中の「★４」に相当**

(2) 要請に当たってのパートナーシップの構築

Aは、自社の対応方針を定め、B・Cに対する説明会を定期的に開催（講ずべきセキュリティ対策の内容や国の支援策等を説明）。また、AからB、BからCに対し、費用負担の考え方、セキュリティ対策が価格交渉の対象になる旨、価格交渉に積極的に対応する旨を周知。

(3) 要請への対応と価格交渉の実施

B・Cは、それぞれ発注者側から受けた説明により対策の必要性を理解し、国の支援策を活用することで要請された対策を安価に実現。対策に要したコストに関し、発注者側による説明に基づき価格交渉を実施し、円満に合意。結果を双方が書面に記録して保存。

(4) 要請を行っていない発注者側企業への対応

Cは、要請を受けていないB'（中堅企業）とも価格交渉を行うため、取引かけこみ寺などの支援機関へ相談。得られた助言に基づき、Bとの交渉で用いた費用負担の考え方等を整理した上でB'に対し価格交渉を申し入れ、対策の必要性や同社との取引割合などを勘案した費用負担の考え方等を説明。交渉は円満に合意に達し、結果を双方が書面に記録して保存。

【想定事例解説】

想定事例を補足するため、以下の点について解説を作成。

① SCS評価制度に基づいたセキュリティ対策要請が合理的範囲を超えた負担を課すものではないこと。
② 発注者・相手方双方でパートナーシップを構築することの必要性や重要性。
③ セキュリティの経費が物件費や人件費などの間接経費として計上されること。
④ 価格交渉の考え方や、要請をしていない発注者側企業に対する価格交渉に当たって支援機関を活用すること。
⑤ 取引かけこみ寺や公正取引委員会の事前相談制度・一般相談・事例集の紹介。

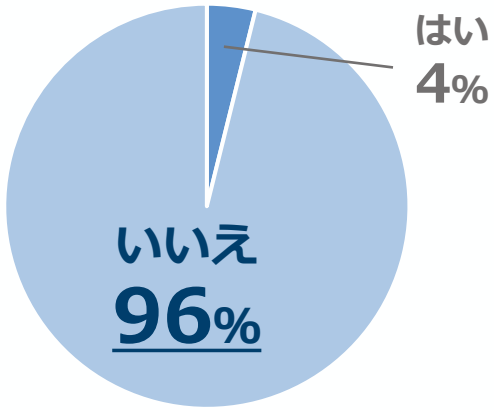
【今後の取組】

本文書について、経済団体や中小企業支援機関等に協力いただきつつ、大企業・中小企業等の双方に対して、普及展開を進めていく。

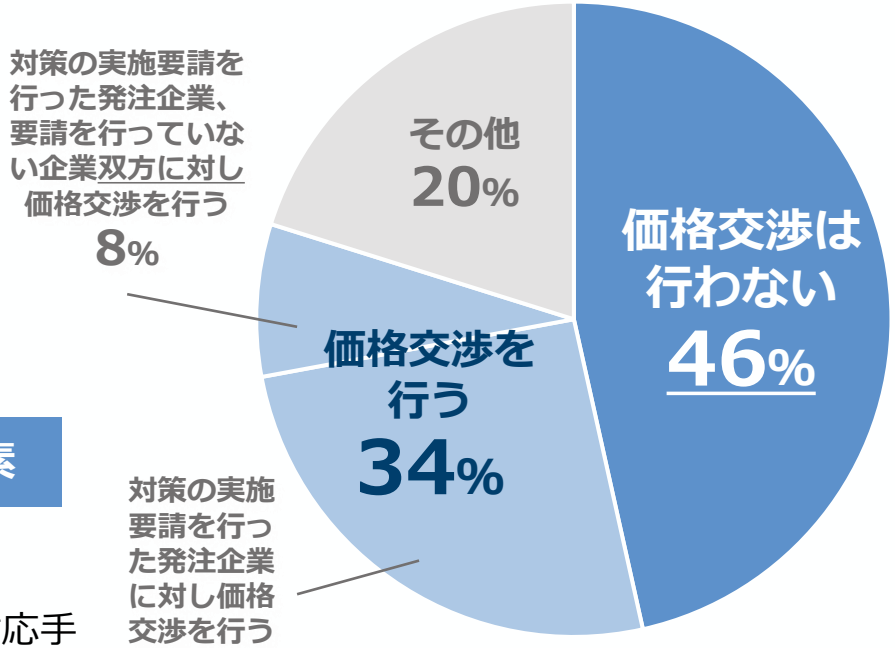
（参考）セキュリティ対策の取組に関する価格転嫁の現状

- 現状、発注側企業の要請の有無を問わず、セキュリティ対策による**間接経費の増加を価格交渉の対象とする動きは少ない**。他方、発注側企業による要請時に、**対策内容への助言や支援を希望する声は多い**。
- 作成した想定事例が多くの中小企業に認知され、**セキュリティ対策とともに価格交渉が円滑に進むよう、中小企業への啓発を促進**する。

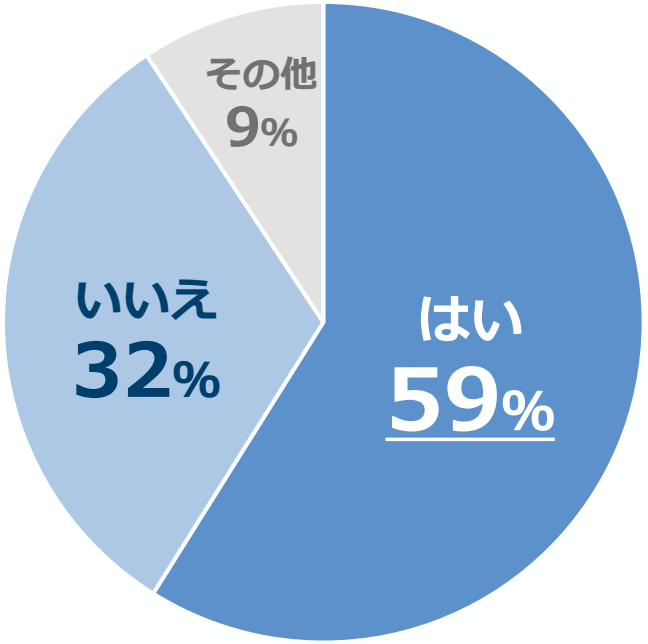
Q. 要請の有無を問わず、セキュリティ対策実施による間接経費発生を価格転嫁できたか



Q. 発注側企業からの要請でセキュリティ対策を実施することで定期的に生じる間接経費の価格転嫁をどう考えるか



Q. 発注側企業からセキュリティ対策の要請があった場合、助言や支援を希望するか



Q. 価格転嫁できた間接経費の主な要素

- ✓ セキュリティ機器の**導入コスト**
- ✓ セキュリティ機器の**運用コスト**
- ✓ セキュリティポリシーやインシデント対応手順の策定に当たっての**専門家への相談コスト**

n=129社(中小企業)

出典：大阪商工会議所により中小企業等を対象として2025年７月に実施された実態調査の結果を基に、経済産業省にて加工

サイバーセキュリティお助け隊サービス（新類型）について

- 中小企業向けの支援策として、**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（SCS評価制度）の★3・★4の取得支援を目的としたサイバーセキュリティお助け隊サービス（新類型）**を創設する。具体的には、★3・★4の要件項目のうち未達成の項目について、サイバーセキュリティお助け隊サービス（新類型）の導入により要件項目を達成させるものとする。
- 今後、**実証事業を通じて、**令和８年(2026年)度末頃のSCS評価制度開始に合わせて、サイバーセキュリティお助け隊サービス（新類型）の**基準案を公表し、先行版としてサービスイン**する予定。

サイバーセキュリティお助け隊サービス（新類型）のイメージ

STEP1：課題の可視化

SCS評価制度
★3・★4の
取得及び更新時
に各要件項目の
対応状況を診断

STEP２：対象サービスの選定と対応実施

診断結果に基づき、以下の支援を実施

✓ITツールによる支援
★３・★４取得に推奨されるITツールを導入

✓ITツール以外の支援
セキュリティポリシーやインシデント手順書の整備、セキュリティ教育など、中小企業が自助努力で達成しづらい項目を支援

【サービス例】

SCS★４＋	★４要件に駆付け支援がプラスされたサービス
SCS★４	★４要件を最低限満たすサービス
SCS★３＋	★３要件に駆付け支援がプラスされたサービス
SCS★３	★３要件を最低限満たすサービス

STEP1・STEP2の支援サービスを一定の価格要件の下で提供

STEP3：★取得

SCS評価制度の★3・★4の**要件項目をすべて充足することで“★”を取得**

サイバーセキュリティお助け隊サービス（新類型）実証事業

- サイバーセキュリティお助け隊サービス（新類型）創設に向け、**全国十数社程度のITベンダーに実証事業に参加いただき、顧客である中小企業にサービスを提供しながら、技術要件・価格要件を検証**する実証事業を実施する（令和８年８月頃から令和９年９月頃までの１年間を予定）。
- 実証の結果を踏まえ、令和９年３月頃までに、**価格要件を含むサービス基準の制度化**につなげる。

実証で検証すること（ITベンダー向け）

中小企業へのサービス提供を通じて以下の項目を検証

1. セキュリティ要求に対応できる**技術要件（サービスの内容・品質等）**を検証
2. サービス導入が継続的に可能な**価格要件**を検証

実証を通して、**ITベンダー・中小企業の双方にとってメリットのあるサービス**を創設する

中小企業の実証参加メリット

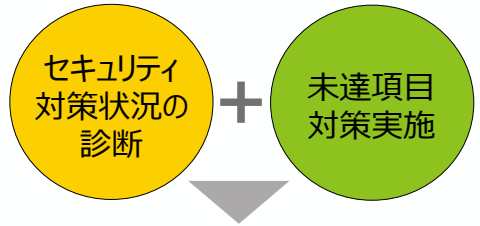
1. **組織的対策を含むセキュリティ対策を無料**で実施（実証期間中最大1年程度）
2. SCS評価制度の“★”**取得**が可能（SCS評価制度開始後の“★”取得要請への備えが可能）
3. サプライチェーン全体での対策強化に取り組む企業として、**取引先との信頼性向上**に繋がる

（参考）サイバーセキュリティお助け隊サービス　既存類型と新類型のサービス内容

既存類型 セキュリティ対策に不安のある中小企業に向けて、**最低限必要なセキュリティ対策**を安価に提供（令和7年9月末時点で9,200件の導入実績有り）

ワンパッケージで安価に提供

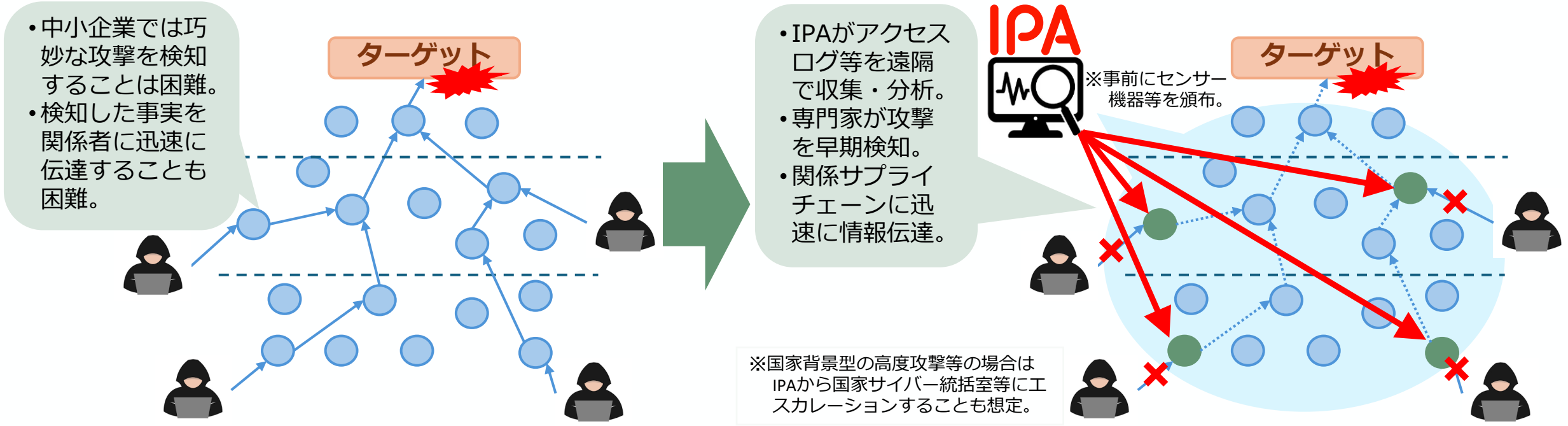
新類型 **SCS評価制度の★３・４取得を目指す中小企業**に向けて、セキュリティ対策状況を**診断**し、未達成項目が全て達成されるまで**伴走支援**するサービス



SCS評価制度の“★“取得

中小企業等向け集団的防御プラットフォームの構築

- 基幹インフラ事業者等を標的としたサイバー攻撃は、そのサプライチェーンの中で**比較的脆弱な中小企業等から侵入**して標的に到達しようとすることが一般的。
- 一方で、**中小企業等**は、**攻撃の兆候を十分に検知することが難しい**状況。
- このため、高度なサイバー情勢分析機能を有する**IPA**が、サプライチェーン上の中小企業等への**アクセスログ等を遠隔で収集・分析**し、**サイバー攻撃の早期検知**や取引先への波及を防ぐための**情報展開を実施**する。　※令和７年度補正予算事業を通じて、分析力向上の程度・情報還元の有用性等を検証予定。



中小企業の情報セキュリティ対策ガイドライン改訂の全体像

- 新たに開始されるSCS評価制度や中小企業の実態を踏まえ、中小企業が自社の状況に応じて段階的にセキュリティ対策を進められるよう、ガイドラインの内容の見直しを進めている。（令和8年3月末公表予定）

改訂のポイント

①サイバー攻撃の実態及び中小企業の実態を踏まえた見直し

- 中小企業が**ランサムウェアの攻撃対象とされている実態**を踏まえ見直し。
- 令和６年度に実施した中小企業実態調査を踏まえ、 SECURITY ACTION 自己宣言（SA宣言）制度 25項目のうち**実施状況が低い項目について実行性を上げるための対策例の見直し**を実施。
- また、実態調査から中小企業においても**ファイアウォールの導入やWebサイトの開設が多く、このようなIT導入状況を踏まえた対策の見直し**を実施。

②SCS評価制度の取り込み

- SCS評価制度の★3・★4は、SA宣言の一つ星、二つ星の上位基準として位置づけられていることを踏まえ、本ガイドラインが、SA宣言に限らず、**SCS評価制度の“★”取得につながるものとなるよう見直し**を実施。

③人材確保・育成の実践的方策ガイド（β版）の成案化

- サイバーセキュリティ人材の育成促進に向けた検討会の最終取りまとめとして公表された**人材の確保・育成に関する取組を、中小企業が実践できるよう、中小企業の情報セキュリティ対策ガイドラインの付録として成案化。**

ガイドラインへの反映の方向性

第2部 実践編

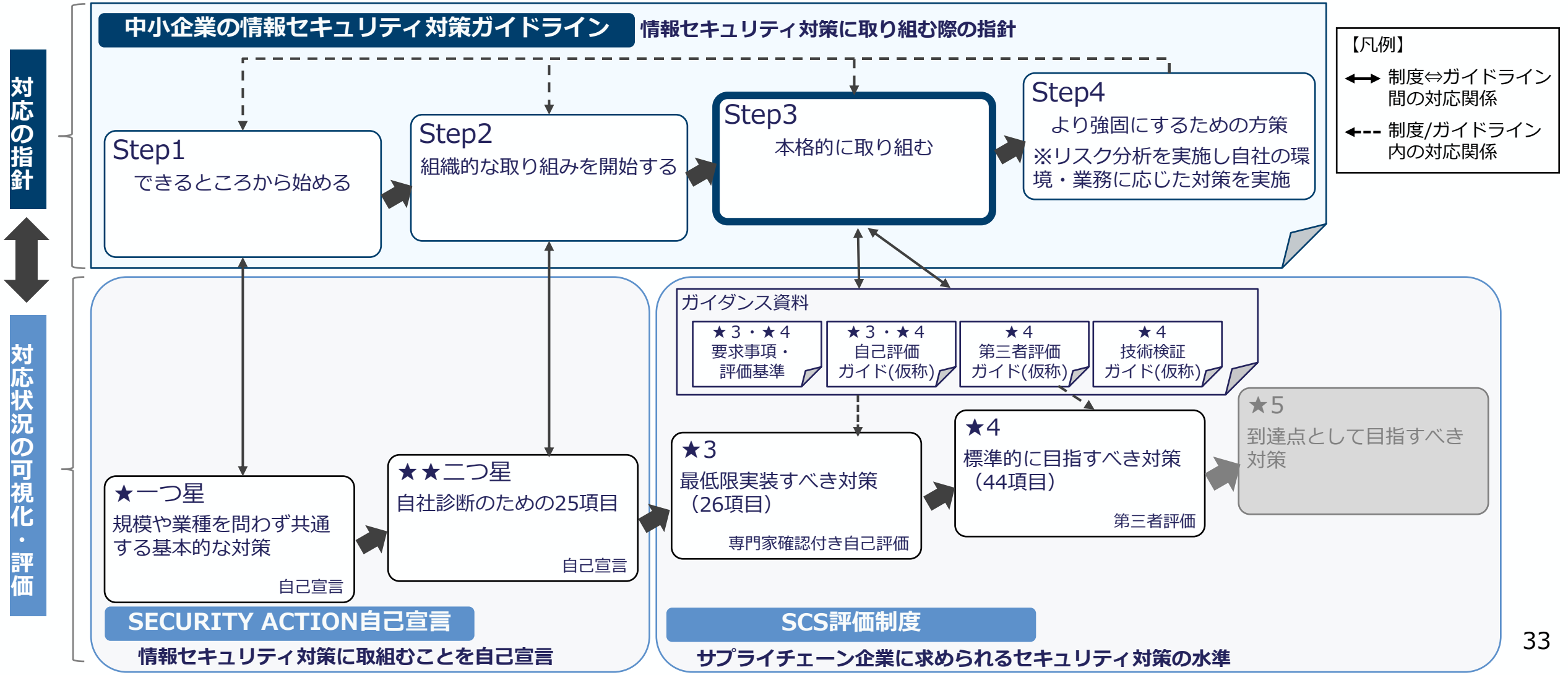
- ✓ 「STEP1」をSA宣言一つ星とし、**サイバー攻撃の実態を踏まえバックアップを加え「6か条」**にする。
- ✓ 「STEP2」をSA宣言二つ星とし、実態調査を踏まえ、**FWやWebサイトの導入に係るセキュリティ対策を追加**するとともに、25項目の具体的対策例を見直し。
- ✓ 「STEP3」をSCS評価制度の★３・★４の対策実施につながるよう、**規程策定などの組織的対策や、技術的な防御策に取り組むための考え方**を提示。
- ✓ 「STEP4」としてSTEP1～3の取組を踏まえた**リスク分析に基づき、これまでの取り組みに加え、個社の実情に応じた追加的対策を行うための考え方**を提示。

付録

- ✓ **規程類のサンプル・ひな型についてSCS評価制度に対応する形で拡充。**
- ✓ 実践的方策ガイドについて、ガイドライン改訂案を踏まえ企業へのヒアリングを実施し、**取組事例の収録や分かりやすい表現を用いることで、中小企業が活用しやすい形で整理し、付録として成案化。**

（参考）ガイドラインとSCS評価制度の関係性

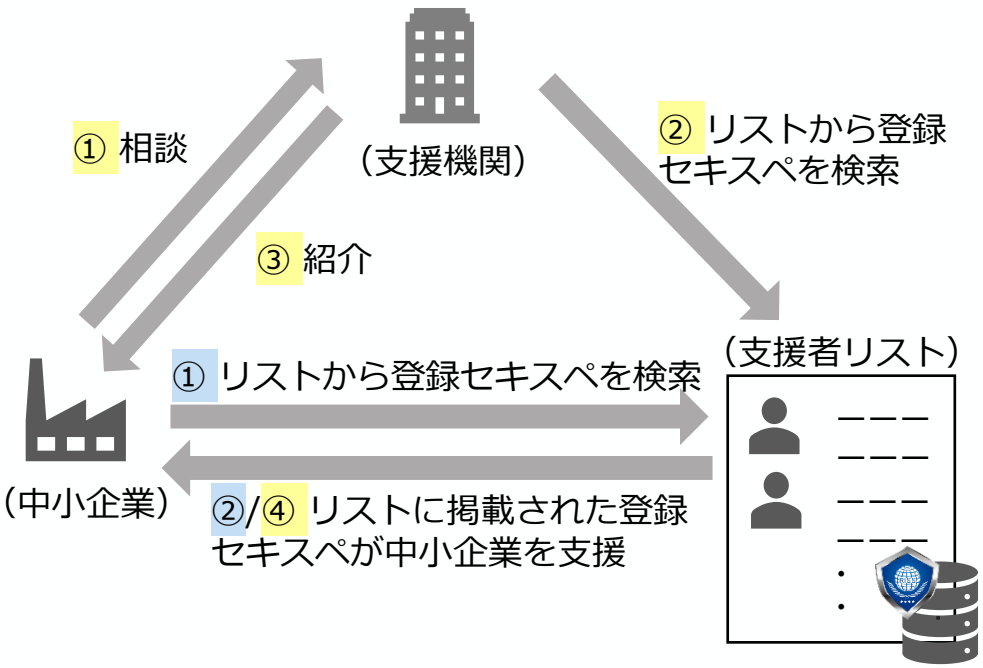
- STEP3では、SCS評価制度の考え方を取り込み、本格的な対策に取り組む段階としている。
- 中小企業がガイドラインに沿って取組を進めることで、SCS評価制度において求められる対策の考え方や水準を参考にしながら、段階的にセキュリティ対策を強化していくことが可能。



情報処理安全確保支援士（登録セキスペ）を活用した中小企業支援

- 社内のセキュリティ人材育成に課題を抱える中小企業にとって、セキュリティ対策における**外部のセキュリティ専門家の活用**が効果的であることを踏まえ、**登録セキスペを効率的に探索するためのツール（支援者リスト）を整備。**
- **SCS評価制度の★３取得のために同リストを活用**できるよう、**”★”取得の適合可否を確認可能な登録セキスペの増加**を促進。

（今後の支援者リスト活用スキーム）



①.②.　　中小企業自身によるリスト活用スキーム
①.②.③.④. 支援機関を通じたリスト活用スキーム

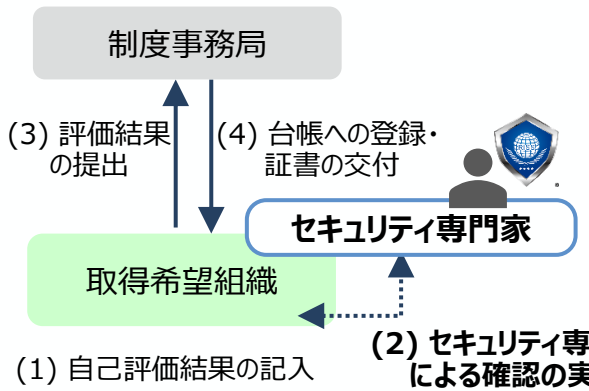
支援者リストの整備（利便性向上・掲載者の増加）

- ✓ **利便性を向上し「中小企業向けサイバーセキュリティ対策支援者リスト」**としてIPAのHP上に公開（改修イメージは次スライドの通り）。
- ✓ 全登録セキスペに向けた**セミナー**（※1）**を開催**し、**リスト掲載者は340人に増加。**一方、支援ハードルの高さ等、掲載者数の更なる増加に向けた課題も明らかになった。

※1：中小企業支援の方法解説、実際に支援を行った登録セキスペによる体験談の共有を実施。

SCS評価制度★３取得の適合可否を確認できる登録セキスペの拡充

（SCS評価制度★３の評価スキーム）



- ✓ 中小企業が**SCS評価制度の★3を取得する際、セキュリティ専門家として登録セキスペが適合可否の確認**及び助言ができるよう、指導テーマ（※2）に「セキュリティアセスメント」を追加し、指導の実践に向けた施策（※3）を実施。

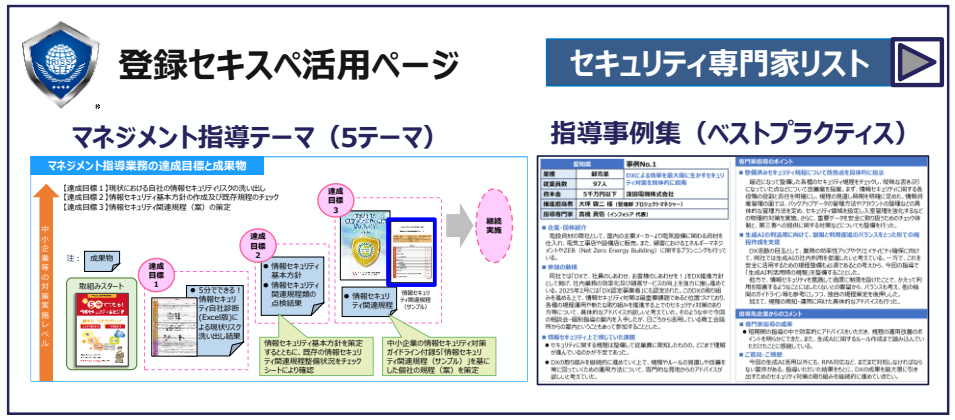
※2：支援者リストに掲載された登録セキスペは、指導テーマ（情報セキュリティ規程の整備等）から中小企業が指定するものに基づき支援を実施。
※3：指導要領の作成や、スキル習得のためのケース演習を実施。

今後の方向性について

商工会議所等の支援機関や中小企業による支援者リストの活用に向け、**活用事例の蓄積**を図るとともに、リスト掲載者数の更なる増加に向けた取組を検討。

（参考）今後のリスト公開イメージ（令和８年3月末時点）

- リストの利便性を向上するため、**支援対象地域及び得意とする業界毎の絞り込み検索**や、**各登録セキスペの個票（HTML形式）表示**を実現。（令和８年3月末頃公開予定）



【簡易検索】
・支援対象地域別（10地域）
・得意業種別（8業種）

IPA 独立行政法人 情報処理推進機構

中小企業向けサイバーセキュリティ対策支援者リスト

支援対象地域：すべて　　得意とする業界：すべて

登録番号	氏名	居住地	支援可能な指導テーマ					企業支援実績	支援対象地域	得意とする業界	支援可能な期間					支援料金（1回/2時間あたり）	初回指導割引	支援可能な形態						所属状況	他の資格
			規定整備	情報管理・リスク分析	クラウド安全利用	インシデント対応	従業員教育				スポット対応	1~3か月	3か月~半年	半年~1年	1年以上			訪問	リモート	講演・研修	緊急対策	製品選定・導入	長期支援		
100001	情報 太郎	東京都文京区	可	可	可			4件/1年	埼玉県,千葉県,東京都,神奈川県	自動車産業/その他製造業/建設業/小売業/サービス業	可				可	20,000円以上~30,000円未満			可	可		可		企業勤務	ITストラテジスト,ネットワークスペシャリスト
100002	伊波 花子	神奈川県横浜市旭区	可				可	2件/10年	関東,甲信越,静岡県	金融業/医療/教育	可	可	可			20,000円未満	有	可	可		可		可	独立	中小企業診断士,ITコーディネータ
123456	駒込 一郎	北海道	可			可	可	5件/5年	全国		可	可	可	可	可	40,000円以上		可		可			可	独立	医療情報技師,システム監査技術者

出典：IPA「中小企業向けサイバーセキュリティ対策支援者リスト」https://www.ipa.go.jp/security/sme/shien/list.html

専門家個票

中小企業向けサイバーセキュリティ対策支援者リスト

■基本情報

カナ	センゴク キョウコ
氏名	千石 京子
公開用メールアドレス	abcd-efg@gmail.com
登録番号	122333
居住地	千葉県船橋市
所属状況	企業勤務
所属先	○○○株式会社
他の資格	ネットワークスペシャリスト
所属・関係する団体	
自己PR	UTM製品を提案した経験が豊富で、セキュリティ技術をわかりやすく説明することが強みです。

（写真）

■支援実績

セキュリティ実務経験	15年
企業支援経験	経験あり
企業支援実績	支援件数10件 / 支援年数10年
企業支援内容	ファイアウォール、VPN、Proxyサーバ、UTMの設計・導入作業の実施
得意とする業界	自動車産業/その他製造業/金融業

■支援可能な範囲

企業規模				
支援対象地域	東北,茨城県,埼玉県,千葉県,東京都,神奈川県			
支援可能な期間	スポット対応		1~3か月	可
	3か月~半年		半年~1年程度	
	1年以上の長期的支援(顧問契約等)	可		
支援料金（1回/2時間あたり）	20,000円以上~30,000円未満		初回指導割引	有
支援可能な形態	訪問によるコンサルティング	可	（補足事項）	
	オンラインコンサルティング			
	講演・研修			
	インシデント発生時の緊急対策支援			
	セキュリティ製品の選定・導入支援	可		
	長期的支援(顧問契約等)	可		
支援可能な指導テーマ	情報セキュリティ規程の整備		情報資産の洗い出しとリスク分析	可
	クラウドサービスの安全利用	可	セキュリティインシデント対応	可
	従業員向け情報セキュリティ教育	可		

■保有スキル

【0】セキュリティ対策戦略の立案	◎	【1】サイバーセキュリティ対策の方針策定と管理体制づくり	
【2】セキュリティリスクの識別	○	【3】サイバーセキュリティ対策の実践と運用の強化	◎
【4】サイバー攻撃の検知、監視、検知後の運用策定		【5】セキュリティインシデント発生時の対応	○
【6】セキュリティインシデントからの復旧やコミュニケーション		【7】システム監査	

２．令和７年度の主な施策の取組状況

（２）地域の中小企業におけるセキュリティ対策促進

- 地域SECUNITY活動促進に向けた取組
  - ① 地域SECUNITYの活動内容の横展開促進
  - ② SC3と連携した普及・啓発活動の実施
  - ③ 中小企業向け情報セキュリティポリシー策定ワークショップ＋個別相談会の開催
- 中小企業のための実例で学ぶサイバーセキュリティリスク事例集（案）
- 「SECURITY ACTION」の対策項目の見直し
- 人材確保・育成の実践的方策ガイドの概要

地域SECUNITYの活動内容の横展開促進

- 地域SECUNITY団体の活動促進が普及・啓発にとって必要不可欠。そこで、**地域SECUNITY間の「横のつながり」を作るとともに、各地域の取組事例を共有し、地域SECUNITYの活動活性化を図るため、**令和８年３月、経済産業省及びIPAにおいて「地域SECUNITY連絡会」を開催予定。
- 地域SECUNITY連絡会で各団体から発表いただいた内容に基づき、**今後、経済産業省において地域SECUNITYプラクティス集として情報発信していく**予定。

地域SECUNITY連絡会

地域SECUNITY連絡会は、地域で普及・啓発活動に取り組む団体から、取組内容や工夫したことなどを発表いただくもの。
取組事例を地域SECUNITY間で共有することで、地域SECUNITY活動の活動促進につなげる。

【地域SECUNITY連絡会での発表予定団体】
- ○ 四国総合通信局
- ○ 新潟県警本部
- ○ 一般財団法人関西情報センター（KIIS）
- ○ 一般社団法人鹿児島県情報セキュリティ協議会（KPSEC）
- ○ 一般社団法人LOCAL
- ○ 宮崎県サイバーセキュリティ協議会
- ○ YOKOSUKA情報セキュリティプロジェクト

（参考）令和７年２月開催の地域SECUNITY連絡会での主な発表内容

農業をテーマとした普及・啓発活動

・農業のような一次産業はITが進んでいない一方で、個人としてはスマートフォンの利用が進んでいることや、若手就農者がECサイトを利用している実態があることから、農業分野においてもサイバーセキュリティ対策が必要と判断し、農業をテーマとした普及・啓発活動を実施。

⇒農業分野において多くの集客が実現

地域SECUNITYのノウハウを活用

・八戸地域の方々からの依頼を受け、一般社団法人地域セキュリティ協議会（ASC）のノウハウを共有、九州地域と東北地域と連携してサイバーセキュリティセミナーを企画・開催。

⇒地域SECUNITY活動のノウハウを他の地域でも活用することによって、セミナー開催の向上が図られる

具体的メッセージをキャッチフレーズとする

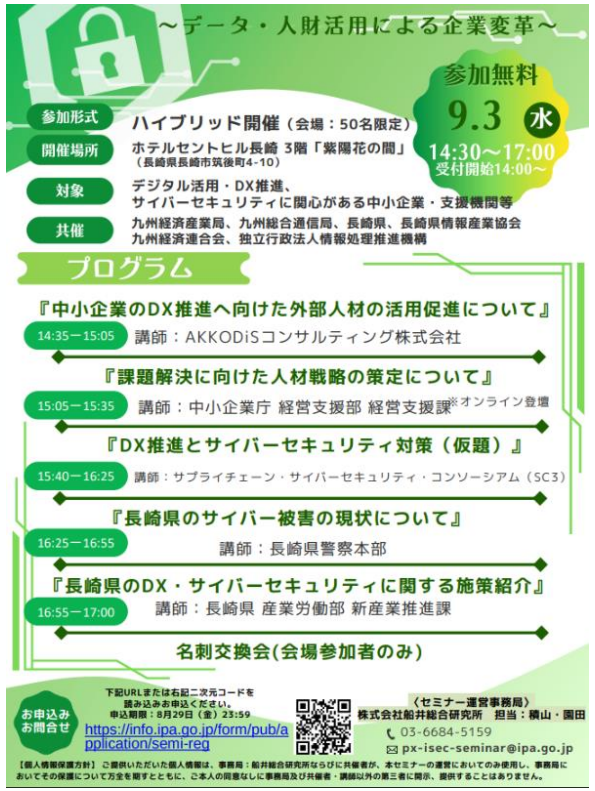
・千葉県地域SECUNITY連絡会では、「かっこつけない、お金をかけないセキュリティ対策」をキャッチフレーズに参加を呼びかけ。キャッチフレーズの効果もあって、105名の中小企業に参加いただいた。

⇒中小企業に向けた具体的メッセージをキャッチフレーズとすることで、より高い集客につながる

出典：経済産業省「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」抜粋

SC3と連携した普及・啓発活動の実施

- サイバー攻撃の悪質化、巧妙化による経済社会活動への影響拡大を踏まえ、全国網羅的な中小企業等における対策の底上げに係る取組のほか、**地域の特性を考慮した重点的取組**を行う必要がある。
- そこで、**SC3と連携し、半導体産業のある九州地域において「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」の普及に向けた講演を実施**。工場のスマート化が製造業発展のカギであり、製造業全体の対処能力底上げを図りつつ、普及を図ることを目的として実施。



「ＤＸ＆サイバーセキュリティ対策推進セミナーｉｎ大分」におけるSC3講演

中小企業向け情報セキュリティポリシー策定ワークショップ＋個別相談会の開催

- 東海サイバーセキュリティ連絡会では、過去の中小企業に対するヒアリング等から**中小企業にセキュリティポリシー策定に対するニーズがある**ことを踏まえ、令和７年11月、「情報セキュリティポリシー策定ワークショップ（WS）+登録セキスペによる個別相談会」を開催。
- 参加者からは、**大変有意義なWSであった**と高い評価が得られ、また登録セキスペによる相談会についても**「有意義であり、専門家に直接自社の課題について相談することができてよかった。」**などの高評価をいただいた。

セキュリティポリシー策定に対する中小企業の意見

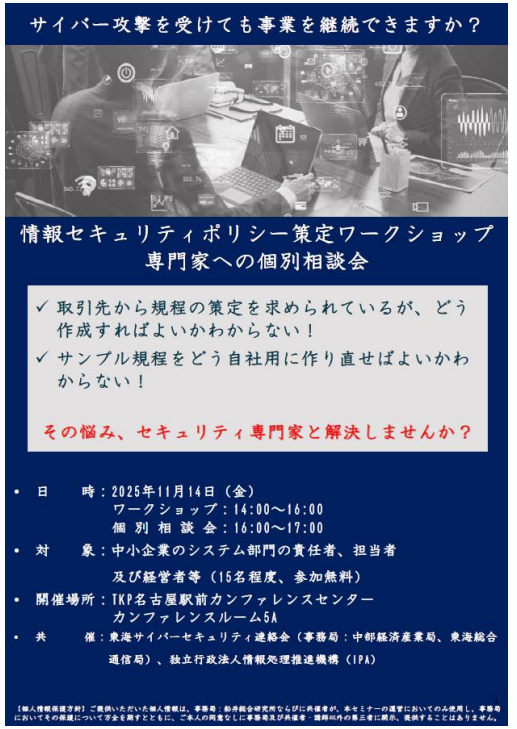
- 東海サイバーセキュリティ連絡会では過去の企業ヒアリングから、
  - ○ 標準的なひな形を自社向けにカスタマイズしたい
  - ○ 取組中の対策の妥当性を確認したい
  - ○ 自社だけでポリシーを策定することが難しい

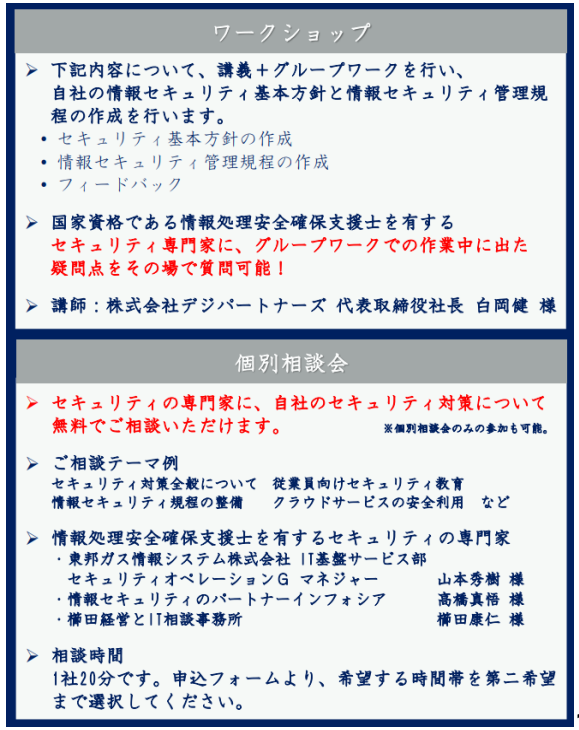
  といった課題を把握し、
  これを踏まえ、令和７年11月ワークショップ+個別相談会を開催。

情報セキュリティポリシー策定WS+個別相談会参加者の声

- ワークショップ+個別相談会参加者からの主な意見
  - ○ 有意義であった、理解ができた
  - ○ **専門家（登録セキスペ）の方に、直接自社の課題について相談することができてよかった**
  - ○ **セキュリティ対策についてシステムベンダしか相談先を知らなかったので、相談先が増えてよかった**
  - ○ 是非次回もやってほしい

情報セキュリティポリシー策定WS+個別相談会の概要





出典：サイバー攻撃等初動対策手順書策定ワークショップ（主催：東海サイバーセキュリティ連絡会）

中小企業のための実例で学ぶサイバーセキュリティリスク事例集（案）

- 中小企業の多くが「セキュリティ対策の必要性を十分に理解していない」実態。
- そこで、中小企業一般にありがちなサイバーセキュリティ・リスクや、攻撃された場合に想定される被害額とそれを防ぐための主な対策を（約30事例）示し、中小企業にセキュリティ対策の必要性を理解いただくための「事例集」をIPAにて令和８年3月末に公表予定。今後、地域SECUNITY等での講演資料や社内での教材としての活用を想定。

事例集の読者層・使い方

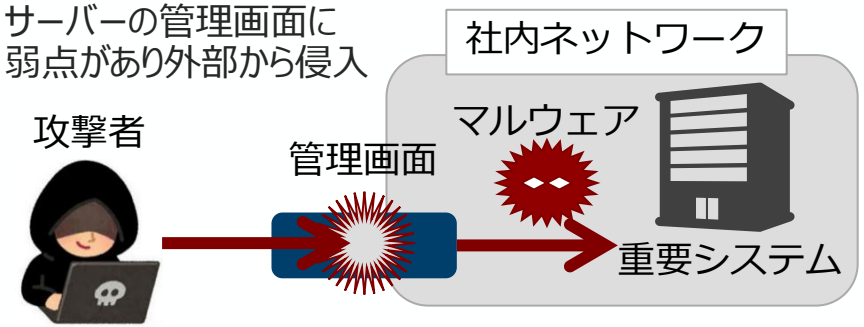
中小企業の経営者・情報システム担当者、中小企業の支援に携わる関係機関の皆様を対象とし、次のような活用を想定

- ✓ **中小企業でも被害がある**ことを示す資料や、専任の情報システム担当がいない企業の**工夫事例紹介**として
- ✓ **自社に合った対策を見つけるきっかけ**や、**社長への相談・予算交渉の材料**として
- ✓ 社内研修や勉強会、地域SECUNITY等での**講演資料や教材**として

事例集事例

①中小企業で**実際に見つかった弱点**を紹介
②中小企業のサイバー被害事例と**被害額**を紹介
③自社にあった**レベルの対策**が見つかる

1 サーバーの管理画面に弱点があり外部から侵入



2 **想定被害額** **3,900万円**

初期対応費用、復旧費用、報告公表費用、弁護士訴訟費用、再発防止費用等

業務停止し**完全復旧まで2か月**要した

3

すぐにできる対策

- ✓ 機器のIDとパスワードが**初期設定のまま**になっていないかチェック

より強固にする対策

- ✓ トラブルが起きた時にどう対応するかの**手順書を整備**する

IPA「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」で中小企業のセキュリティ意識の不足を確認し、令和7年度に複数業界・規模の中小企業126社を対象にASM診断※を実施。アンケートとヒアリングで被害事例や好取組事例を収集し、リスクと対策を整理した「事例集」を作成
※ASM診断は、インターネットから見える自社のIT資産（サーバ、ネットワーク機器、IoT機器など）を把握し、攻撃されやすいポイントを特定する仕組み

「SECURITY ACTION」の対策項目の見直し

- 中小企業の実態や最新の脅威動向を踏まえ「SECURITY ACTION」の対策項目の見直しを実施。
- **バックアップをSA宣言一つ星の対策項目に追加**したほか、**実施状況が低い項目について具体的対策例の見直し**などを実施。中小企業の情報セキュリティ対策ガイドラインの改訂に合わせて公表予定。

情報セキュリティ5か条の見直し

情報セキュリティ5か条（SA宣言一つ星）に二つ星の項目であった**「バックアップを取ろう！」を新たに位置づけ、6か条**として整理

上記追加の背景：

- ✓ **IPA「10大脅威」においてランサムウェア攻撃が上位に位置づけ**られ、その対策として重要
- ✓ 中小企業が初めに手掛ける対策としてわかりやすく、BCP観点でも重要

【情報セキュリティ６か条】

- ロOSやソフトウェアは常に最新の状態にしよう！
- ロウイルス対策ソフトを導入しよう！
- ロパスワードを強化しよう！
- ロ共有設定を見直そう！
- ロ脅威や攻撃の手口を知ろう！
- **ロバックアップを取ろう！**
- **※SA宣言一つ星の項目として位置づけ**

診断25項目の見直し

【追加】

「中小企業実態調査」において、**ファイアウォールおよびWebサイトの導入率が比較的高い**ことが確認された

導入セキュリティ製品Top3

利用ITサービスTop３

- ✓ **「ファイアウォール」については、定着を図る観点から項目として整理**
- ✓ 導入実態があるにもかかわらず、これまで対策項目として整理されていなかった**「Webサイト」について、新たに対策項目として位置づけ**

【統合】

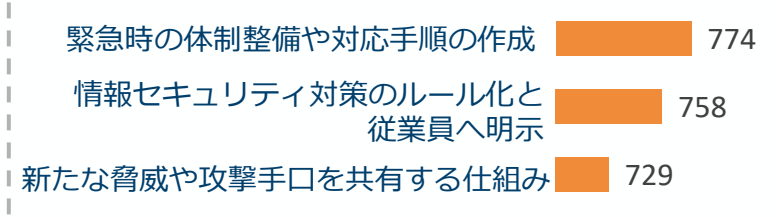
中小企業が読んだ際の重複感を避ける観点から、**関連がある項目を、内容の趣旨は維持したまま整理**

- ✓ 物理的なアクセス管理に関する項目を統合
- ✓ 従業員の情報セキュリティ意識に関する項目を統合

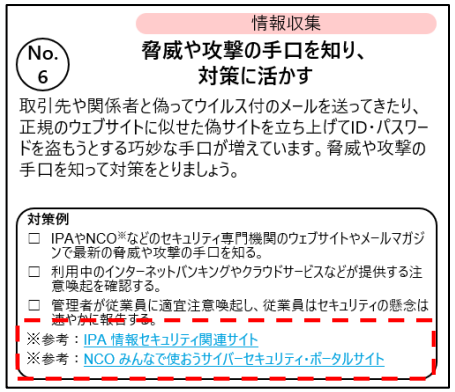
実施率の低い項目の見直し

実施率が低い項目について、**具体的な参照先を追加して対策を実施する際の導線を強化**

SA宣言25項目実施ワースト３



（例）項目：6「脅威や攻撃の手口を知り、対策に活かす」


情報収集

No. 6

脅威や攻撃の手口を知り、対策に活かす

取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げてID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。

対策例

- □ IPAやNCO※などのセキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る。
- □ 利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認する。
- □ 管理者が従業員に適宜注意喚起し、従業員はセキュリティの懸念は速やかに報告する。

※参考：IPA 情報セキュリティ関連サイト

※参考：NCO みんなで使おうサイバーセキュリティ・ポータルサイト

⇒情報収集先としてIPAやNCOなどが運営しているWebサイトを参考として明記予定

出典：IPA 「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」（n=中小企業4,191社、複数選択可）を基に経済産業省作成

人材確保・育成の実践的方策ガイドの概要

- 中小企業がセキュリティ人材の確保・育成をできるよう、**4つのSTEPごとにセキュリティ担当者の役割・業務を段階的に整理し、人材の確保・育成の方策を紹介する手引き**を作成。
- また、自社で実践する際の参考となるよう、**中小企業へのヒアリングに基づいた事例を紹介**している。

付録の目的・ターゲット

✓企業がサイバーセキュリティ対策を進めるには、対策をリードできる人材を組織として確保・育成することが重要。
✓**セキュリティ対策に本格的に取り組む、または取組を強化したい中小企業の経営者・担当者を対象。**

付録のポイント

付録の構成

チェックポイント
チェックすべき基本観点

活動内容
基本観点に基づき実施すべき対策内容

人材確保・育成（内部）
社内人材を活用した確保・育成策の提示

人材確保・育成（外部）
外部人材による補完・支援策の提示

◆4つのSTEPごと段階的に、社内セキュリティ担当者の役割・業務を提示
✓ セキュリティ対策として中小企業が取り組むべきタスクを、コンパクトかつ段階的に整理

◆対策を実行するための人材の確保・育成の方策を紹介
✓ セキュリティ対策に必要なタスクを実行するため、社内人材の確保・育成に向けた考え方を整理
✓ 社内での育成が難しい場合を想定し、外部人材や支援サービスの活用についても併せて紹介

事例集のポイント

事例の構成

企業のプロファイル
業種・規模等の紹介

事例の概要
- 対策を進めた背景
- 具体的にどうやって人材を確保し、何を活用して進めたのか
- 成果として何ができるようになったのか

イメージ・ポイント
プロセスや内容を簡潔に紹介

◆どう進めれば良いか分からないという課題に対し、実際の企業ヒアリングを基に整理
✓ 各STEPの対策に取り組むにあたりどのような人材を、どのように確保・配置したか
✓ 社内人材で対応した対策、外部の支援やサービスを活用した対策
✓ 担当者の任命から、学習・相談・役割分担までの現実的な進め方

➢ **各STEPの対策について、「自社でやるならどう進めるか」を考える際の参考として活用できる構成**

今後の方向性について

✓**「中小企業の情報セキュリティ対策ガイドライン」改訂に併せて付録として成案化**、令和8年3月末公表予定。
✓SCS評価制度など各種施策と整合を図りつつ、**中小企業の人材確保・育成の取組を支援するガイドとして位置づけ**。

３．前回ＷＧで御指摘いただいた事項の対応状況

- 前回のＷＧ２でいただいた御意見への対応状況

前回のWG2でいただいた御意見への対応状況（１／２）

項目	前回の主な御意見	令和７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）	・SCS評価制度★3～★5の取組は高く評価できる。サイバーセキュリティお助け隊サービスは商工会議所でも普及に向けて活動しているが、**既存の施策と評価制度との連動を深められたい**。	・中小企業支援策として、**SCS評価制度の対策支援を目的としたサイバーセキュリティお助け隊サービス（新類型）の創設**の検討及び**同制度の考え方を取り込む形で中小企業の情報セキュリティ対策ガイドラインを改訂**。	・令和８年度からサイバーセキュリティお助け隊サービス（新類型）創設に向けた**実証事業を実施**し、中小企業やサービス提供事業者にとって継続的に導入できるサービスとなるよう制度設計を行う。**SCS評価制度の施行に合わせて同サービスの提供を開始**する予定。
	・関心が高いのはランサムウェアへの対応。**インシデント発生時に備えた訓練**（どのように意思決定をして、どのように対応していくのかというプロセス作成）**を、ITDX 部門だけではなく、コンプライアンス部門含めて訓練されている企業が増えている**。	○地域SECUNITYの活動促進 ・地域SECUNITY活動の横展開の場として**地域SECUNITY連絡会を開催**。 ・地域で開催されるサイバーセキュリティセミナー等の中で、**登録セキスペによる中小企業に対する個別相談会を開催**。 ・**SC3と連携して工場セキュリティに係る講演を実施**。 ○セキュリティ対策の必要性を喚起するためのコンテンツ作成 ・**中小企業が実施するべき必要な対策をまとめた事例集を作成**。地域での啓発・広報を通じて対策実施を促す。	○地域SECUNITYの活動促進 ・東北地方での地域SECUNITY活動を活性化させ、活動団体の形成促進を図るため、**東北地方の産学官が連携する形での、サイバーセキュリティセミナー・机上演習・展示会などの複合イベントを開催**。 ○セキュリティ対策の必要性を喚起するためのコンテンツ作成 ・**中小企業にとって身近なサイバー事案を収集し、**中小企業の経営者や従業員も含め、**自分事に感じる机上演習コンテンツを作成**し、各地域の団体・支援機関等による活用（机上演習企画の実施）を促す。
	・サイバーセキュリティ対策に関心のある方はセミナー等に参加するが、**関心のない方にどうアプローチするかが大きな課題**である。		
	・**取引関係における優越的地位の濫用の問題については**公正取引委員会と経済産業省の共同文書が令和４年に公表されているが、**浸透はこれからという印象である。**	・令和７年12月、経済産業省と公正取引委員会において、発注者及び取引の相手方双方を対象とした、**独占禁止法・取適法上「問題とならない」想定事例及びその解説文書を作成**。	・作成した想定事例が発注者・取引の相手方双方にとって活用されるよう、**中小企業への普及・啓発活動を実施**する予定。

前回のWG2でいただいた御意見への対応状況（２／２）

項目	前回の主な御意見	令和７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）	・投資家や取締役、監査役など、ガバナンス全体の問題として議論しなければならない。スチュワードシップやコーポレートガバナンス・コード等、以前から取り組まれてきたことをさらに深化させ、**投資家も含めてサイバーセキュリティリスクに対するより深い理解を求めるべき**。	・中小企業の実態調査を通じ、**セキュリティ対策に取り組む中小企業が取引上の信頼獲得につながっている実態を提示**。 ・SCS評価制度の設計を進め、**企業が自社のセキュリティ対策の取組状況を可視化**し、取引先がその状況を評価できる仕組みの整備を進捗させた。	・業界団体等と連携して**SCS評価制度の”★”取得企業の拡大に取り組む**とともに、サプライチェーンに関わる**ステークホルダーとの意思疎通**において本制度がセキュリティ対策に関する**共通のものさしとして活用されるよう環境を整備**する（関係主体への制度周知等）。 ・コーポレートガバナンス・コード改訂に係る議論で、**サイバーセキュリティリスクへの対応が中長期的な企業価値向上のために必要**である旨の追記を目指す。
人材育成	・**セキュリティ人材を見える化**し、**活用**できるような制度設計を期待したい。 ・登録セキスペについて、国内で地位を上げたいのであれば、サイバーセキュリティお助け隊サービスと絡めたり、必ず登録セキスペの助言を受ける等、**制度間の連携**を進めてはどうか。 ・登録セキスペの有効活用については、**登録セキスペでしかできない業務を作り出さねば**普及は進まないのではないか。	・セキュリティ人材が不足している中小企業が登録セキスペを効率的に見つけられるよう、**支援者リスト**を整備し、公表。 ・中小企業が**SCS評価制度の★３を取得する際、本リストを活用**して登録セキスペに”★”取得の適合可否を確認してもらうことができるよう、支援者リスト掲載者（登録セキスペ）向けの指導要領の作成やケース演習を実施。 ・「デジタルガバナンス・コード」（DX銘柄やDX認定の基準）等の**DX施策**や、「令和6年度補正予算グローバルサウス未来志向型共創等事業費補助金」等の**補助金施策の要件に、登録セキスペの活用又は配置を明記**。	○以下の取組を通じて、登録セキスペの活躍機会の拡充を図る。 ・**機微情報を取り扱う業界の企業**を支援可能な登録セキスペの増加に向け、指導要領作成等の取組を実施し、**支援者リスト掲載者の増加及び活用を促進**。 ・支援者リストの普及活動を通じて、**SCS評価制度と連携した登録セキスペの活用を推進**。 ・**公的機関・重要インフラ事業者**における配置促進や、各施策との連携を進める。

４．今後の取組の方向性と本日議論いただきたい論点

- 今後の取組の方向性
- 本日議論いただきたい論点

今後の取組の方向性

①中小企業に対するSCS評価制度の活用促進のために実施する施策

サプライチェーン全体でのサイバーセキュリティ対策を強化するため、中小企業等が最低限実施すべき取組を可視化したSCS評価制度について、令和８年度末頃の制度開始を目指すとともに、ステークホルダーとの意思疎通において本制度がセキュリティ対策に関する「共通のものさし」として活用されるよう、関係主体への周知、各種ガイドライン等での活用、新たな支援策の整備等の取組を進める。

具体的には、中小企業等の「自助」を促す取組として、SCS評価制度に対応する規程類のサンプル・ひな型を盛り込んだ「中小企業の情報セキュリティ対策ガイドライン（改訂版）」の普及・広報を進める。

次に、中小企業の「共助」を促す取組として、取引関係のある企業間で、パートナーシップを構築しながらサイバーセキュリティ対策が促されるよう、業界団体と連携したSCS評価制度の活用促進や、独占禁止法・取適法上「問題とならない」想定事例とその解説文書の周知を進め、産業界への浸透を図る。また、SCS評価制度を活用したサイバーセキュリティ対策に係る情報開示の促進に向けて具体的な検討を進める。

一方、「自助」「共助」の取組によっても十分な対応が難しい中小企業等に対しては、「公助」の取組として、SCS評価制度に対応したサイバーセキュリティお助け隊サービス（新類型）の創設及び実証事業を通じた支援強化を実施する。

また、IPAにおいて集団的防御プラットフォーム構築のための実証事業を実施し、サイバーセキュリティお助け隊サービスと連携する形で、中小企業群から脅威情報を収集し、新たな脅威に対応するための仕組みを構築する。

さらに、 SCS評価制度に沿った取組の実施・自己評価にあたって、中小企業が外部の専門家である登録セキスペを容易に活用できるよう、中小企業等と登録セキスペのマッチングの促進を図る。

サイバーセキュリティお助け隊サービス（新類型）実証事業参加へのメリット

今後の取組の方向性

②地域SECUNITY活性化に向けて実施すべき施策

中小企業等にとって身近なサイバー事案を収集し、中小企業等の経営者や従業員も含め、自分事に感じるような机上演習コンテンツを作成し、各地域の団体・支援機関等において机上演習の活性化を促す。

また、東北地方における地域SECUNITY活動を活性化させ、活動団体の形成促進を図るため、地域の支援機関、企業等と連携して、サイバーセキュリティセミナー・机上演習・展示会などの複合イベントを開催する。大規模イベントにより集客効果を高めることで、将来的に、同地域の支援機関・団体がセキュリティ・コミュニティ活動を自走できる素地を整備する。

地域SECUNITY活動

（机上演習）

（危機管理演習）

（企業展示会）

（大規模セミナー）

③中小企業のセキュリティ対策底上げのため更に実施すべき施策

サイバーセキュリティお助け隊サービス（既存類型）について、時勢に沿ったサービス（ゼロトラスト・クラウド化への対応）が提供されるようサービス要件の見直しを行う。

また、製造業等の制御系（OT）システムを持つ中小企業に対し、実施すべきセキュリティ対策を提示するための検討を行う。

加えて、機微情報を取り扱う産業分野でも支援可能な登録セキスペの拡充に向けて指導要領を作成するとともに、支援機関等による支援者リストの活用とリスト掲載者の増加を推進していく。

お助け隊サービス（１類・２類）見直しの方向性

■ **時勢に沿ったサービスのニーズについて**

クラウド型セキュリティへの移行ニーズ

✓ ZTNAやSASEなど、リモートワークや分散環境に対応したクラウドベースのセキュリティモデルとして、SWG（例： i-FILTER）やDNSファイアウォールなどのクラウド監視型サービス。

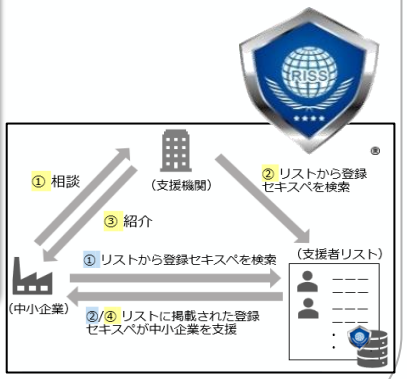
ゼロデイ攻撃・内部漏えい対策

✓ セキュアブラウザ（例：AXISスマートブラウザ）による論理分離や、ログ管理・SIEMによる操作監視等、内部要因による情報漏えい対策に適用したサービス。

EDRの多様化とASM・脆弱性診断のニーズ

✓ 端末だけでなく、サーバ・モバイル端末向けEDR。

✓ ASM（Attack Surface Management）や脆弱性診断サービス



本日御議論いただきたい論点

＜①中小企業に対するSCS評価制度の活用促進のために実施する施策＞

論点１：令和８年度末までに開始予定である**SCS評価制度に基づくサイバーセキュリティ対策の実施**を中小企業等に促進していくに当たり、**どのような課題が考えられるか**。また、**追加的にどのような施策を実施**し、**既存施策・関係組織との連携をどのように図っていくべきか**。

＜②地域SECUNITY活性化に向けて実施すべき施策＞

論点２：全国の**中小企業等へ対策の必要性等を普及・浸透**させていくに当たり、現状**どのような課題が考えられるか**。また、**地域SECUNITYの形成や活動を促進**していくために**どのような施策を講じるべきか**。

＜③中小企業のセキュリティ対策底上げのため更に実施すべき施策＞

論点３：中小企業のセキュリティ対策促進に向けて、**時勢を踏まえて追加的に対応すべき政策領域・課題はあるか**。

論点４：**中小企業等におけるセキュリティ人材の確保**（内部での**育成**、**登録セキスペなど**外部人材の**活用**）にあたり、**どのような課題が考えられ**、**どのような施策を追加的に講じるべきか**。

参考資料

１．中小企業の皆様に向けた既存のサイバーセキュリティ施策
- 中小企業のサイバーセキュリティ対策支援策
- 中小企業のサイバーセキュリティ対策を後押しする主な補助金制度・税制制度
- サイバーセキュリティインシデント発生時の相談窓口

２．支援機関の皆様に向けた施策
- 地域SECUNITYの活動を支援する施策

（参考）１．中小企業の皆様に向けた既存のサイバーセキュリティ施策

中小企業支援施策の全体像

- 中小企業等が抱える主な課題：①「サイバーセキュリティ対策の**必要性を感じない**」、②「**何をすれば良いか分からない**」「**十分にコストをかけられない**」。
- 経済産業省では、地域の支援機関等とも連携し、 ①については**サイバー攻撃が他人事でない旨を周知**し、②については**中小企業等それぞれの課題・ステップに沿った施策を推進**している（以下は主要施策）。

SECURITY ACTION

中小企業自らが、セキュリティ対策に取り組むことを**自己宣言**する制度。**約45万者**の中小企業が宣言。

★一つ星

情報セキュリティ５か条に取り組む

★★二つ星

情報セキュリティ自社診断を実施し、基本方針を策定

⇒セキュリティ対策のきっかけづくり

サイバーセキュリティお助け隊サービス

相談窓口、システムの異常の監視、緊急時の対応支援、簡易サイバー保険など各種サービス内容を要件としてまとめた基準を満たす**ワンパッケージサービス**。（現在、**44事業者**が提供し、 2025年9月末時点で約**9,200件**の利用実績。）

サイバーセキュリティお助け隊

デジタル化・AI導入補助金（旧：IT導入補助金）「セキュリティ対策推進枠」により補助

⇒必要最低限の対策を実行（監視、駆付け、保険）

中小企業の情報セキュリティ対策ガイドライン

経営者編と実践編から構成されており、個人事業主や小規模事業者を含む中小企業等による活用を想定し、具体的な**セキュリティ対策を示したガイドライン**。

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、インシデント対応、クラウド活用に関する手引き等を収録。

経営者向けの解説

経営者が認識すべき３原則と実施すべき重要７項目を解説

実践者向けの解説

企業のレベルに合わせて**段階的にステップアップ**できるような構成で解説

⇒自社の状況に即したより実効的な取組の検討・実行

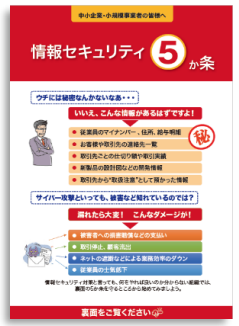
セキュリティ対策の第一歩「SECURITY ACTION」

- **全ての企業に必ず実施していただきたいセキュリティ対策**をまとめたもの。**約４５万者が宣言。**
- 「SECURITY ACTION」を自己宣言することが、**各種補助金の要件**にもなっている。

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/

※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。

SECURITY ACTION自己宣言を申請要件としている補助金・助成金

- デジタル化やサイバーセキュリティ対策などを支援するIT導入の補助金申請の要件にするなど、各種補助金・助成金制度において**SECURITY ACTION自己宣言（SA宣言）制度を活用**。
- 引き続き、各地方自治体や団体組織等とも連携の上、取組の拡大を促進していく。

○国によるＳＡ要件化補助金事業(加点要件を含む)

・デジタル化・AI導入補助金（通常枠・インボイス枠（インボイス対応類型）・セキュリティ対策推進枠）：中小企業庁

・介護テクノロジー導入支援事業（地域医療介護総合確保基金（介護従事者確保分））：厚生労働省（実施主体は各都道府県）

○地方公共団体等による主なＳＡ要件化補助金事業(加点要件を含む)

・令和７年度 サイバーセキュリティ対策促進助成金：東京都中小企業振興公社

・令和７年度 堺市中小企業デジタル化促進補助金：大阪府堺市

・令和７年度 デジタル技術導入補助金：愛知県

・令和７年度 中小企業DX推進補助金：北海道札幌市

・令和７年度 産業DX推進事業費補助金：宮崎県

・令和７年度 かごしま中小企業DX推進事業費補助金：鹿児島県

・令和７年度 セキュリティ支援補助金、ICT補助金「はじめの一歩」：横須賀商工会議所

（参考）１．中小企業の皆様に向けた既存のサイバーセキュリティ施策

必要な対策が揃った「サイバーセキュリティお助け隊サービス」

- 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。**
- **全国で44事業者がサービスを提供**しており、 2025年9月末時点で**約9,200件の利用実績**がある。
- デジタル化・AI導入補助金（旧：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。

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

- ✓ **EDR･UTM等による異常監視**
- ✓ **緊急時の対応支援･駆付けサービス**
- ✓ **簡易サイバー保険**
- ✓ **相談窓口**
- ✓ **簡単な導入･運用**

➡中小企業でも導入・維持できる価格でワンパッケージで提供

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/

サイバーセキュリティ お助け隊

お助け隊マーク

- お助け隊 サービスA
- お助け隊 サービスB
- お助け隊 サービスC

サイバーセキュリティお助け隊サービス審査登録制度：
サービス基準の要件を満たすサービスに対し、**お助け隊ロゴマークの使用を許諾**

サービス提供 → **中小企業** → 自社の信頼性をアピール → **取引先**（大企業等）

お助け隊サービス利用の推奨等の中小企業の取組支援

デジタル化･AI導入補助金（旧：IT導入補助金）に「セキュリティ推進枠」創設
（補助率：中小企業1/2、小規模事業者2/3
補助上限：150万円）

（参考）１．中小企業の皆様に向けた既存のサイバーセキュリティ施策

デジタル化・AI導入補助金による「サイバーセキュリティお助け隊サービス」の導入支援

- 「通常枠」及び「インボイス対応類型」において、オプションとして「サイバーセキュリティお助け隊サービス」をメインツールと組み合わせて申請することが可能。この際、「サイバーセキュリティお助け隊サービス」を申請する事業者については、**申請採択における審査時に加点対象。**
- 2022年８月から、新たに「セキュリティ対策推進枠」を創設。**「サイバーセキュリティお助け隊サービス」のみでの補助金申請が可能。**

デジタル化・AI導入補助金概要

（旧名称：IT導入補助金）

メインツールと組み合わせて、**オプションとして「サイバーセキュリティお助け隊サービス」**を申請可能

「サイバーセキュリティお助け隊サービス」のみで申請可能。

	通常枠	インボイス枠 インボイス対応類型	セキュリティ対策推進枠
要件	業務効率化やDXの推進等に資するITツールを導入	インボイス制度に対応した会計・受発注・決済の機能を有するITツール及びそのためのハードウェアを導入	サイバーセキュリティお助け隊サービスを導入
補助上限	ITツールの業務領域が 1～３まで：5万円～150万円 4以上：150万円～450万円	ITツール： １機能：～50万円 ２機能以上：50万～350万円 PC・タブレット等：～10万円 レジ・券売機等：～20万円	5万円～**150**万円
補助率	中小企業：１/２	～50万円以下：3/4 (小規模事業者：4/5) 50万円～350万円：2/3 ハードウェア購入費：1/2	中小企業：1/2 **小規模事業者：2/3**
対象経費	ソフトウェア購入費、 クラウド利用料（最大2年分）、導入関連費	ソフトウェア購入費、 クラウド利用料（最大2年分）、導入関連費、 ハードウェア購入費	**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）**

オプションとして**「サイバーセキュリティお助け隊サービス」を申請した場合、利用料の1年分（「サイバーセキュリティお助け隊サービス」導入は加点要素）**

赤字は令和６年度補正予算からの**拡充点**

デジタル化・AI導入補助金のインボイス枠(電子取引類型)、複数社連携デジタル化・AI導入枠においては、サイバーセキュリティお助け隊サービスは補助等の対象外である。

取組手法の提示：中小企業の情報セキュリティ対策ガイドライン

- 中小企業における**具体的なセキュリティ対策を示すガイドライン**。
- 本ガイドラインは、**経営者編と実践編から構成**されており、個人事業主や小規模事業者を含む中小企業等による活用を想定。

- 中小企業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

出典：中小企業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

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**を平成28年に創設（根拠法：情報処理の促進に関する法律）。
- 国家試験に合格後（※）、IPAに登録することにより資格を取得。 **登録資格は3年ごとに更新**（定期的な講習受講が義務付け）が必要。 **登録者数は24,937人**（令和7年10月１日時点）。
  ※試験合格者に加えて、国が指定するポストやプログラムに従事した者も登録セキスペとなる資格を有する
- 登録セキスペには、①経営課題への対応（リスク評価、セキュリティ対策、監査）、②システム等の設計・開発（設計段階からのセキュリティ対策）、③運用・保守、④緊急対応等の幅広い業務での活躍が期待されている。

登録セキスペのメリット

＜取得者のメリット＞

①情報セキュリティに関する高度な知識・技能を保有する証

②継続的・効果的な自己研鑽が可能

③就業機会・業務範囲の拡大（※１）

※1 PCI DSS監査人の資格要件、情報セキュリティ監査人資格の取得の優遇、中小企業支援とのマッチング機会等

＜組織･企業へのメリット＞

①提供する機能やサービスへの信頼の向上

②社会的評価・信頼の向上（※２）

③ビジネスチャンスの拡大（※３）

※2 知識・技能の証明に加えて、資格保有者は信用失墜行為の禁止や秘密保持の義務有する

※3 各種補助金、「デジタルガバナンスコード」（DX銘柄やDX認定基準）、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（SCS評価制度）での活用等を推進

（参考）１．中小企業の皆様に向けた既存のサイバーセキュリティ施策

各種補助金施策等における情報処理安全確保支援士の要件化

- **各種補助金事業の要件**として、**情報処理安全確保支援士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やDX施策との紐付け**、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。

✓ **「令和6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）**

（４）サイバーセキュリティへの対応
調達先がサイバーセキュリティの確保に関する対策に適合している事項を示すために、**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。

✓ **「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】。

✓ **「デジタルガバナンス・コード3.0～DX経営による企業価値向上に向けて～」における記載（抜粋）**

（２）望ましい方向性
- サイバーセキュリティリスクに対応できる体制の構築に向けた取組として、**情報処理安全確保支援士（登録セキスペ）の取得や外部人材の活用**、社員への教育等を企業として進めている。

大胆な投資促進税制（特定生産性向上設備等投資促進税制）

目的	高付加価値な国内設備投資の推進
対象業種	全ての業種を対象
対象資産	●生産等に必要な設備等（機械装置、器具備品、工具、建物、構築物、建物附属設備、ソフトウェア） ● 投資下限額：35億円以上（中小企業者等については5億円以上） ● ROI水準：15%以上
措置内容	●即時償却または税額控除７％（建物、建物附属設備及び構築物は税額控除４％） ➢ 控除上限：法人税額の20% ● 事業環境の急激な変化による影響への対応（繰越税額控除） ➢ 予見し難い国際経済事情の急激な変化に対応するための計画について、法律に基づく認定を受けた事業者については、繰越税額控除（3年間）が可能
措置期間	令和11年3月31日までの間に設備投資計画につき法律の確認を受けた者が、その確認を受けた日から5年を経過する日までの間に取得等をし、事業の用に供した設備等を対象

他の設備投資税制の適用：
本措置の適用を受ける場合、投資計画期間中は、中小企業経営強化税制、地域未来投資促進税制、カーボンニュートラルに向けた投資促進税制の設備投資税制は適用しない

租税特別措置の不適用措置（ムチ税制）：
● 大企業については、対前年度の所得を上回る事業年度において、次のいずれかに該当する場合、本制度（繰越税額控除を除く）を適用しない
⑴ 継続雇用者の給与等支給額の対前年度増加率1%未満（従業員数2,000人超の場合等は２％未満）
⑵ 国内設備投資額が当期償却費総額の 30%以下（従業員数2,000人超の場合等は40%以下）

サイバーセキュリティインシデント発生時の相談窓口

- サイバー攻撃又はその疑いにより、情報漏えい、ウイルス感染、システム停止などの**インシデントが発生した場合**、迅速な対応が必要。
- 金銭被害、信用低下、事業停止等や関係者（顧客、取引先、従業員等）への**被害拡大を最小限に抑えるため**、警察への相談に加え、初動対応を支援する以下の**専門機関の活用**が有効。

独立行政法人情報処理推進機構（IPA）

- 不正アクセス等のインシデントに関する相談や届出、情報提供の受付：
  https://www.ipa.go.jp/security/todokede/incidentportal.html

（相談例）
- ランサムウェアに感染したため、対処方法について相談したい
- 普段の情報セキュリティの対策やIPAのセキュリティ施策について知りたい
- サイバー攻撃被害について、サイバー保険の適用を受けるために公的機関への届出を行いたい

一般社団法人JPCERTコーディネーションセンター

- インシデント初動対応（必要な調査、対応方針の検討、被害箇所の特定等）のサポートなどの依頼相談：

  https://www.jpcert.or.jp/form/

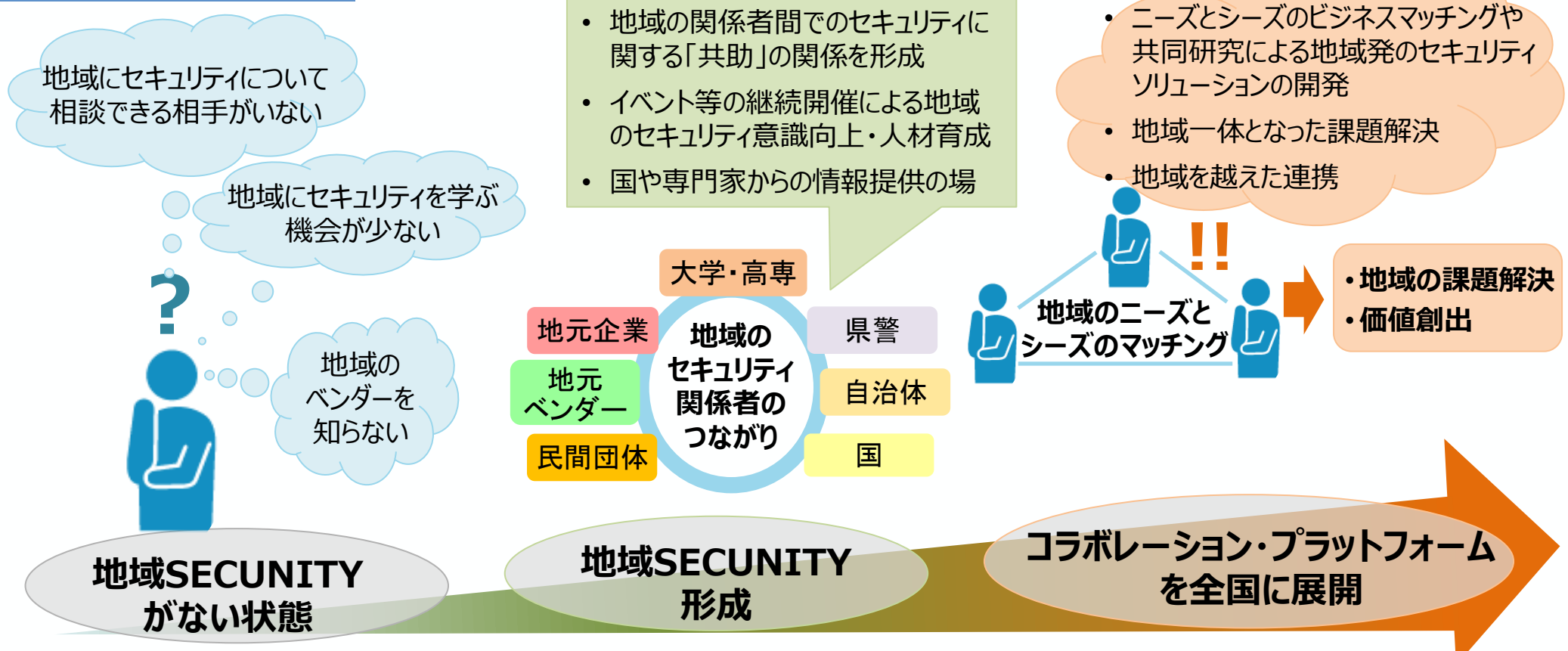
- インシデント対応に関する様々な相談、情報提供の受付：

  https://www.jpcert.or.jp/ir/consult.html

地域SECUNITY（地域に根付いたセキュリティ・コミュニティ）

- 地域の民間企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティ活動を、「地域SECUNITY」と命名。
- まずは各地域で地域SECUNITYの形成を促進し、将来的には、地域のニーズとシーズのマッチングによる課題解決・付加価値創出の場（コラボレーション・プラットフォーム）へと発展することを目指す。

地域SECUNITYのコンセプト



（参考）２．支援機関の皆様に向けた施策

地域SECUNITYの活動を支援する施策の御紹介

- 経済産業省及びIPAでは、地域SECUNITYの活動を後押しするため、以下の支援策を実施しています。
- 支援策の利用は無料です。令和8年度も実施予定ですので、御活用をお願いします。

セミナー開催支援

- 地域SECUNITYの形成・活動に取り組む団体を支援するため、IPAでは、**地域団体等との連携による中小企業のサイバーセキュリティ対策普及促進のためのセミナー開催支援事業**を実施。
- 令和8年度も本事業を実施しますので、ぜひ御活用をお願いします。

＜支援形態＞

1　**セミナー開催支援**
セミナーやワークショップ開催に関する会場の手配、チラシ作成、セミナー運営などをIPAの委託事業者が運営し、地域SECUNITY活動を支援。令和７年度は、全国の地域団体から、セミナー開催支援21件、演習19件の申込みをいただいた。

2　**講演者派遣**
地域団体等が主催するセミナー等にIPAが講演者を派遣。令和７年度は、全国の地域団体から108件の申込みをいただいた。令和７年度は新たな取組として、セミナーで講師を務めた登録セキスペが、セミナー開催後に個別相談を実施。

出典：IPA「地域団体等との連携による中小企業のサイバーセキュリティ対策普及促進のためのセミナー開催支援」
https://www.ipa.go.jp/security/sme/renkei.html

インシデント対応机上演習(TTX)

- 組織においてセキュリティインシデントが発生した場合には、**被害とその影響範囲を最小限に抑えて事業継続を確保**する必要がある。その為には、あらかじめ対応体制と手順を整備したうえで、実際にセキュリティインシデントが発生した場合を想定して演習しておくことが重要。
- こうした背景を踏まえ、IPAは、**セキュリティインシデント対応机上演習の実施を後押しし、**より多くの組織に机上演習を実施いただけるようにするため、令和７年４月、**演習教材と演習実施のためのマニュアルを公開。**

出典：IPA「セキュリティインシデント対応机上演習教材」
https://www.ipa.go.jp/security/sec-tools/ttx.html

セキュリティプレゼンター制度

- IPAのセキュリティ対策資料を活用し、**中小企業等に対して普及啓発を行う人材を「セキュリティプレゼンター」**として登録する制度。
- **全国の中小企業等における情報セキュリティの向上を目的**に、セキュリティプレゼンターによる普及啓発活動を推進。

出典：IPA「セキュリティプレゼンター制度について」
https://www.ipa.go.jp/security/sme/presenter/index.html

（参考）２．支援機関の皆様に向けた施策

セミナー支援業務への新たな取組（個別相談）

- 令和7年度のセミナー開催支援事業では、新たな取組として、セミナー支援に際して、**登録セキスペが講師となることを前提条件として、参加いただいた中小企業を対象に、講師である登録セキスペによる個別相談を開催**。

セミナー開催概要	
主催	地域団体等 （各地域の官公庁や中小企業支援団体、地域金融機関、地域SECUNITY等）
共催	独立行政法人情報処理推進機構（IPA）
テーマ	中小企業のサイバーセキュリティ対策普及促進に資するセミナーやワークショップ・演習等 （DX、IT等の導入にあたっての情報セキュリティ、事業継続計画などを含む） ※セミナー、ワークショップ・演習等に続けて**個別相談**を実施する場合あり
開催方式と想定回数	集合（20回）、ハイブリッド（20回）、オンライン（5回）開催のいずれか（プログラム全体で4時間以内を想定）
開催日程	2026年2月末まで （事業実行可能な日程とし、詳細は協議の上決定）
講演者	セキュリティプレゼンター、IPA職員など （支援対象は4名以内を想定）
受講対象者	• 中小企業の経営者、IT担当者、情報セキュリティ担当者、教育担当者 • 中小企業に対する情報セキュリティ対策支援・啓発を行う地域団体等の役職員等
受講料	無料

【個別相談概要】

対応者：登録セキスペ
相談テーマ：　情報セキュリティ規程の整備
情報資産の洗い出しとリスク分析
クラウドサービスの安全利用
セキュリティインシデント対応
従業員向け情報セキュリティ教育
※詳細については、要相談

※セミナーや演習等の集合会場の一画を利用して対面で実施
※1件あたりの時間：20分（3件計60分まで）

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