経済産業省

中小企業が取り組むべきサイバー対策と経済産業省の支援策

2026年3月

商務情報政策局サイバーセキュリティ課　係長

橋本　里菜

１．サイバー攻撃の実態

２．中小企業が取り組むべきサイバー対策

３．中小企業支援策の新たな体系

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。

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

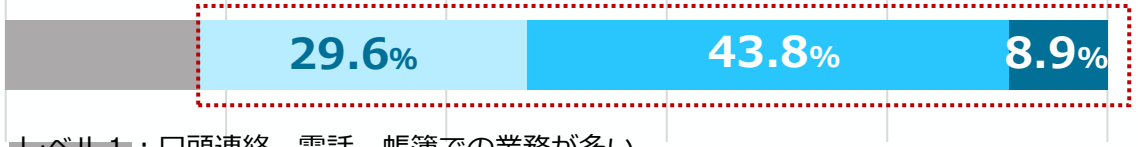
中小企業のデジタルシフトの状況

【東京商工会議所が実施した調査】

- **約８割の中小企業がITを「導入」**しており、より積極的に活用している企業も増加。デジタルシフトへ取り組んだ結果、**77.9%の企業が成果が出ている**と回答。
- **業務効率化**（コスト削減、時間短縮、ミス防止）を効果として実感しているケースが多い。

デジタルシフトの導入

n＝1,218社(中小企業)

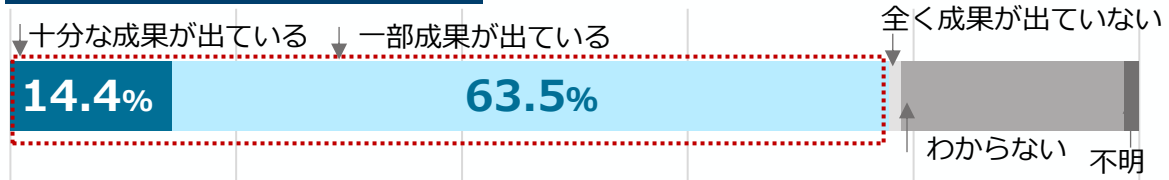


レベル１：口頭連絡、電話、帳簿での業務が多い
レベル２：紙や口頭でのやり取りをITに置き換え
レベル３：ITを活用して社内業務を効率化
レベル４：ITを差別化や競争的強化に積極的に活用

➡**82.3%がITを「導入」**していると回答

デジタルシフトの成果

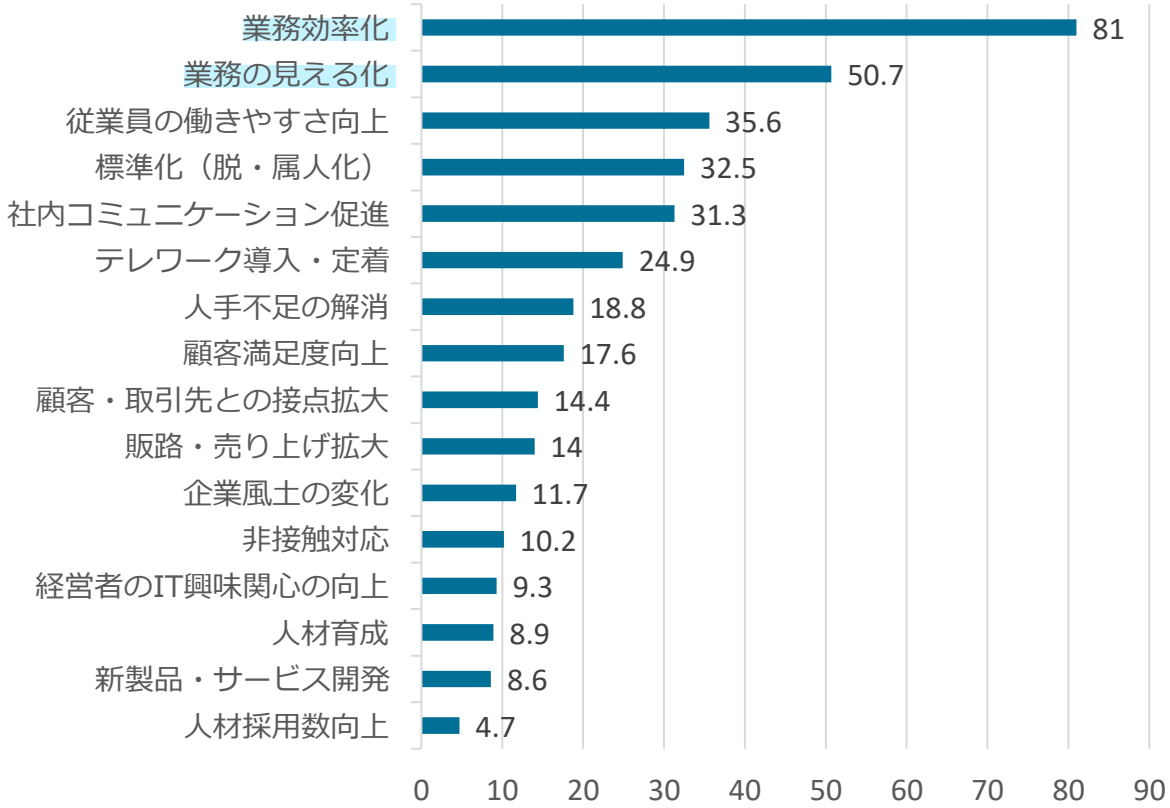
n＝1,218社(中小企業)



➡**77.9%が成果が出ている**と回答

「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）

デジタルシフトの効果

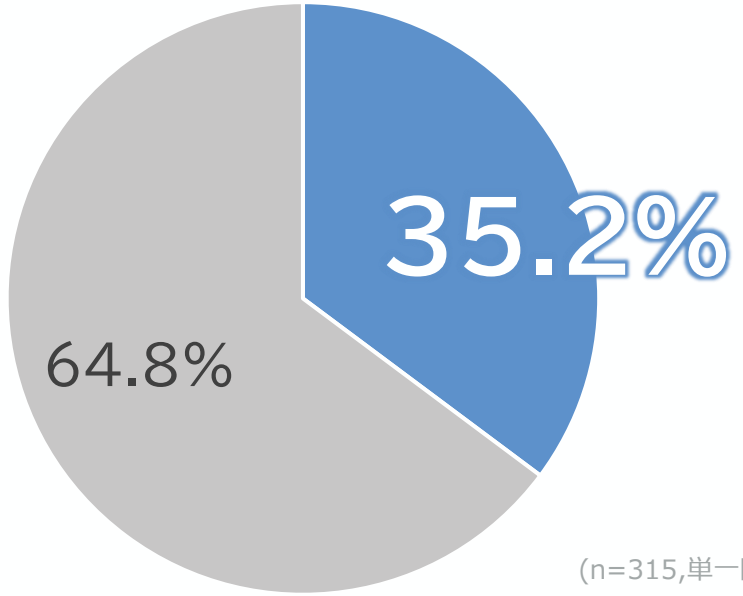


DXの進展が、サイバー攻撃を拡大させた

- DXはビジネスを拡大させたが、**サイバー攻撃の”魅力”も拡大**させた（「13秒に1回の時代」の到来）
- **デジタル＝経営の根幹**　となった今、**サイバー攻撃は経営の根幹を揺るがす大問題**に

DX推進の中で
セキュリティインシデントが発生したと回答した企業は、
35%強にのぼる。

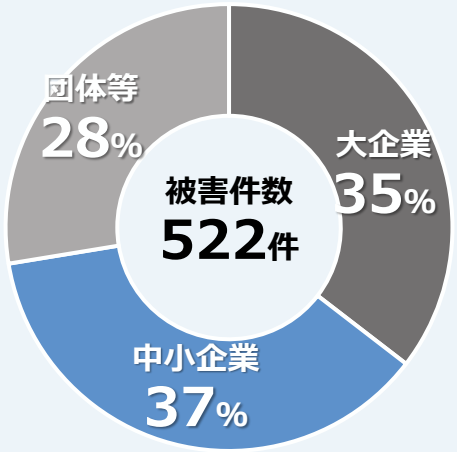
出典:トレンドマイクロ株式会社「DX推進における法人組織のセキュリティ動向調査」



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。**

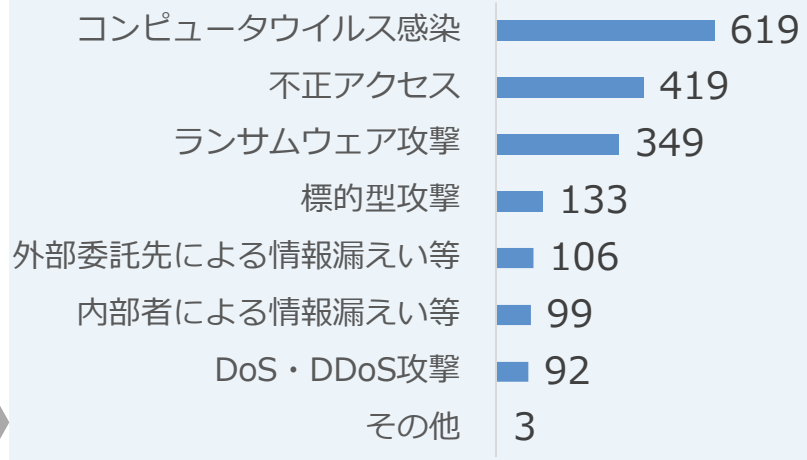
サイバー攻撃の被害組織の規模別割合（2022年７月～2024年6月）



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

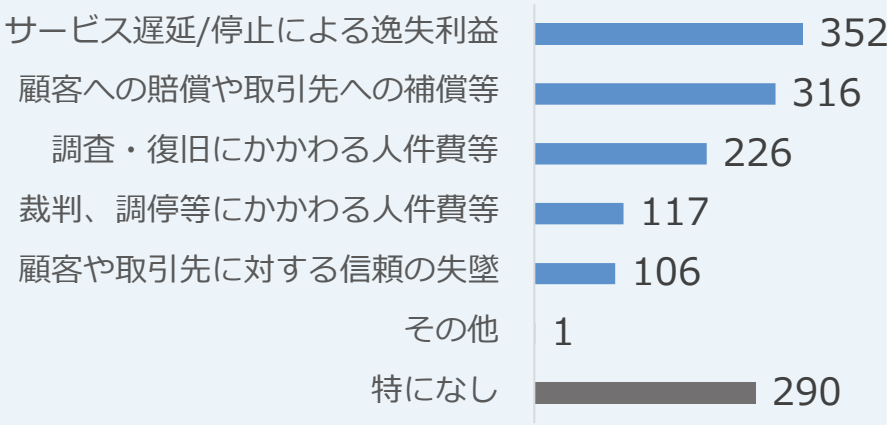
中小企業が実際に受けたサイバーインシデント（複数選択可、回答企業975社）



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：「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）



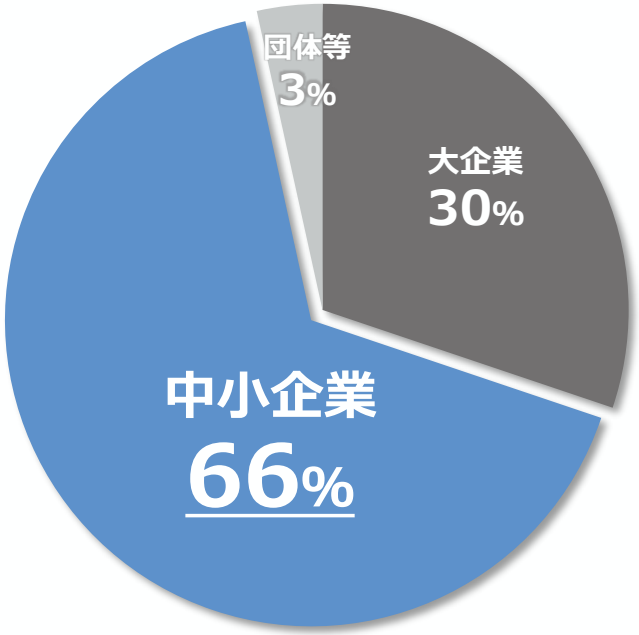
サイバーインシデントの被害を受けたと回答した975社のうち、**685社**がサイバーインシデントにより取引先（サプライチェーン）に影響があったと回答
その割合は**70.3%**

出典：「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

中小企業等にとってもサイバー攻撃は他人ごとではない

- 「サイバー攻撃」は**身近なところで起きている。ランサムウェア被害件数**は2024年から増加しており、**中小企業が狙われる状況**が**過去最多**となった。
- ランサムウェアの被害による調査・復旧費用が高額化しており、実際に、**復旧までに１か月以上を要するケースや数千万円規模の被害が生じるケースが５割を超えている。**

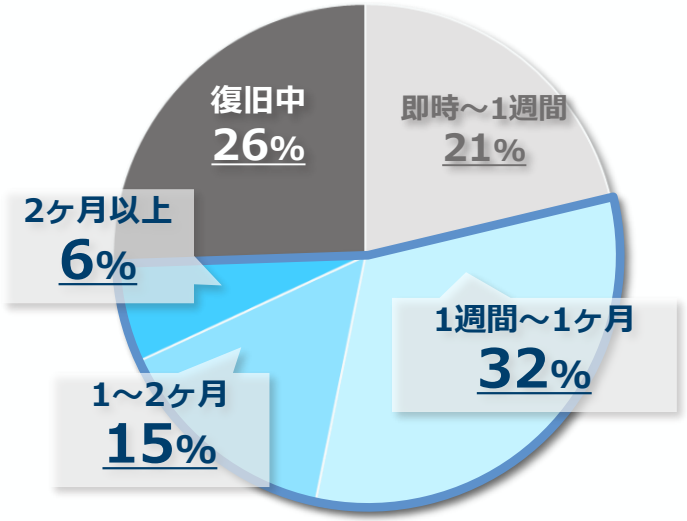
ランサムウェア被害企業等の規模別件数



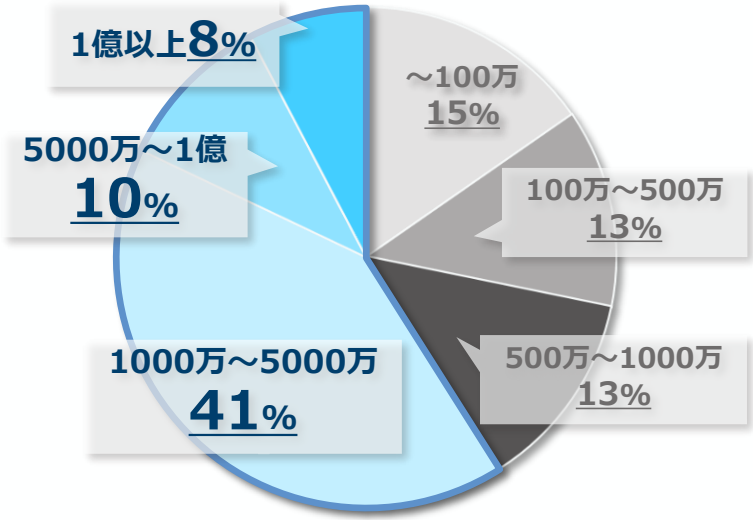
➡ランサムウェア被害の**６割以上**が中小企業
(2024年から３ポイント増加)

ランサムウェア被害（復旧に要した時間、調査費用総額）

【復旧に要した時間】



【調査費用総額】



➡ランサムウェア被害による**調査・復旧費用が高額化**しており、
1000万円以上を要した割合は59%(2024年から9ポイント増加)

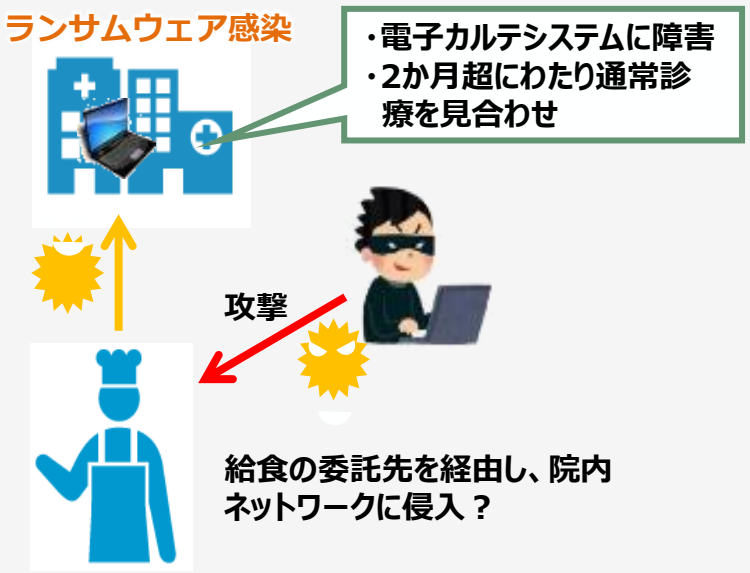
出典：警察庁「2025年上半期におけるサイバー空間をめぐる脅威の情勢等について（2025年9月）」を基に経済産業省作成

顧客・取引先にも影響が及ぶ

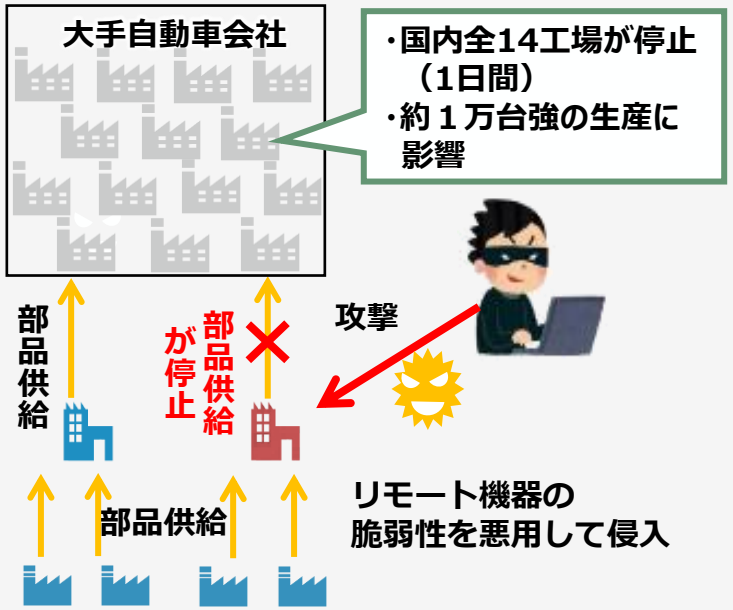
- 攻撃者は、**防御レベルの低い組織**を狙う。サイバー被害は**自社だけの問題では済まない。**

サプライチェーン上の取引先の操業に影響を及ぼした事案

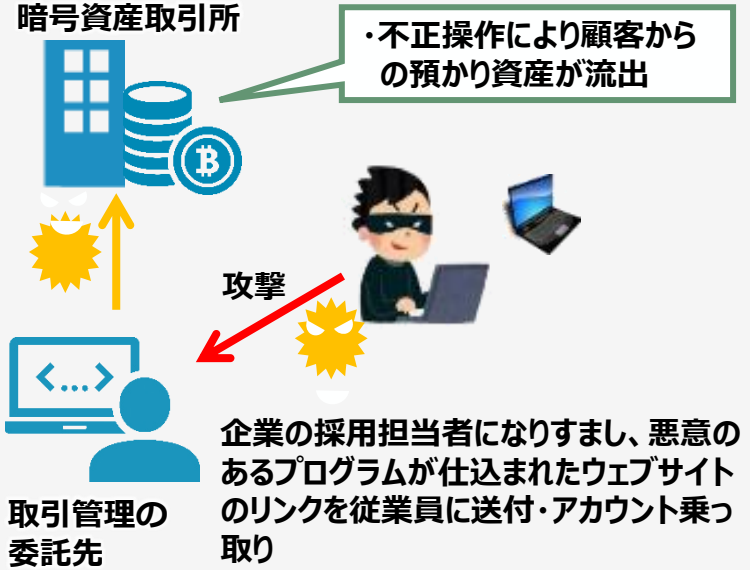
事例①：委託先の給食業者を通じた公立病院への侵入・通常診療見合せ



事例②：自動車部品会社の感染による大手自動車会社の工場稼働停止



事例③：委託先に対する接触を通じた暗号資産取引所への侵入・資産流出



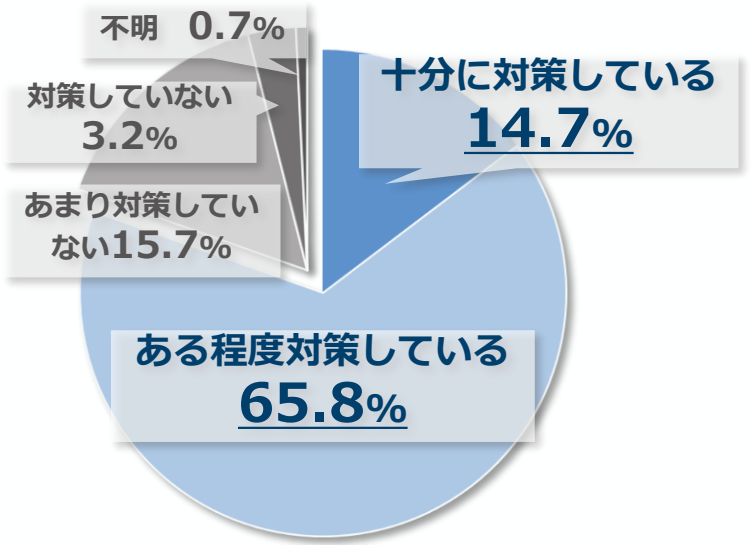
出典：各種報道情報を基に経済産業省作成

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**。

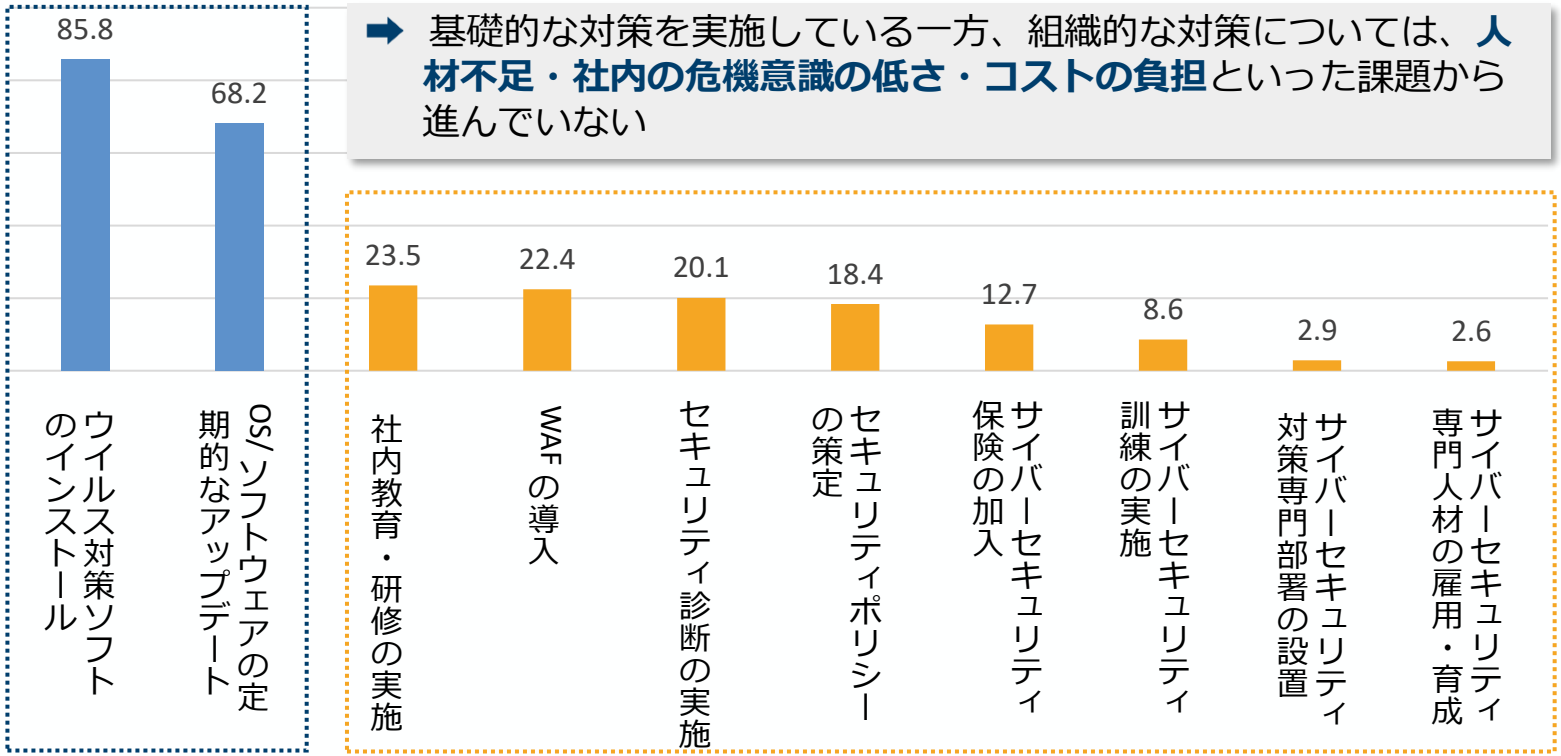
サイバーセキュリティ対策の状況

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

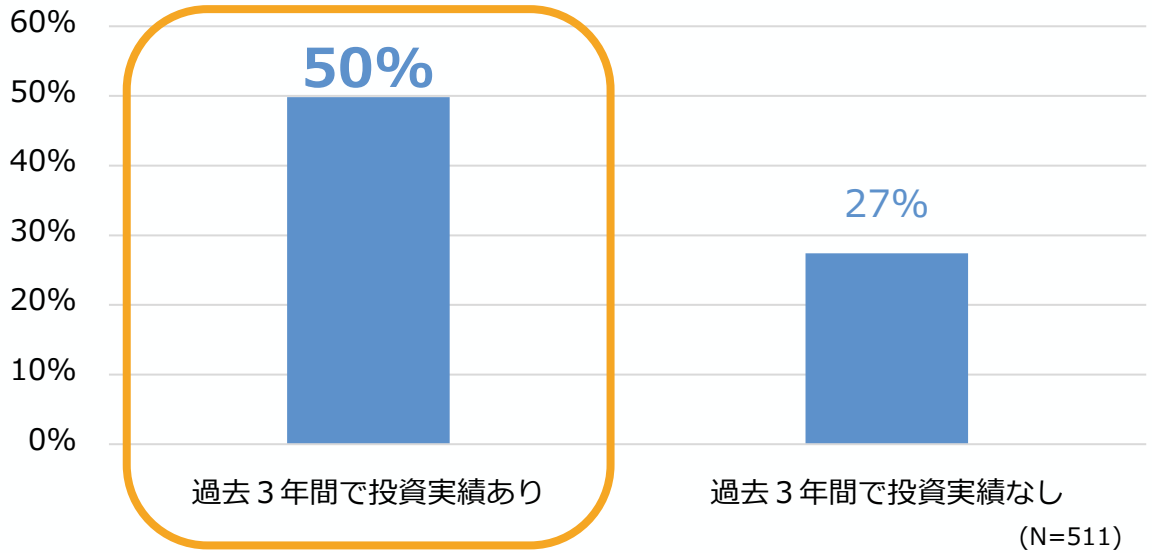
出典：「中小企業のデジタルシフト・DX実態調査集計結果」（2025年1月10日） 中小企業のデジタルシフト・DX推進委員会（東京商工会議所ホームページ掲載資料に基づき、経済産業省において作成）

サイバーセキュリティ対策を行うメリット

- サイバーセキュリティ対策の実施は、**取引先からの信頼の獲得**につながり得る。

セキュリティ対策と取引獲得の関係

要請されたセキュリティ対策を実施したことが取引につながったと考える企業の割合

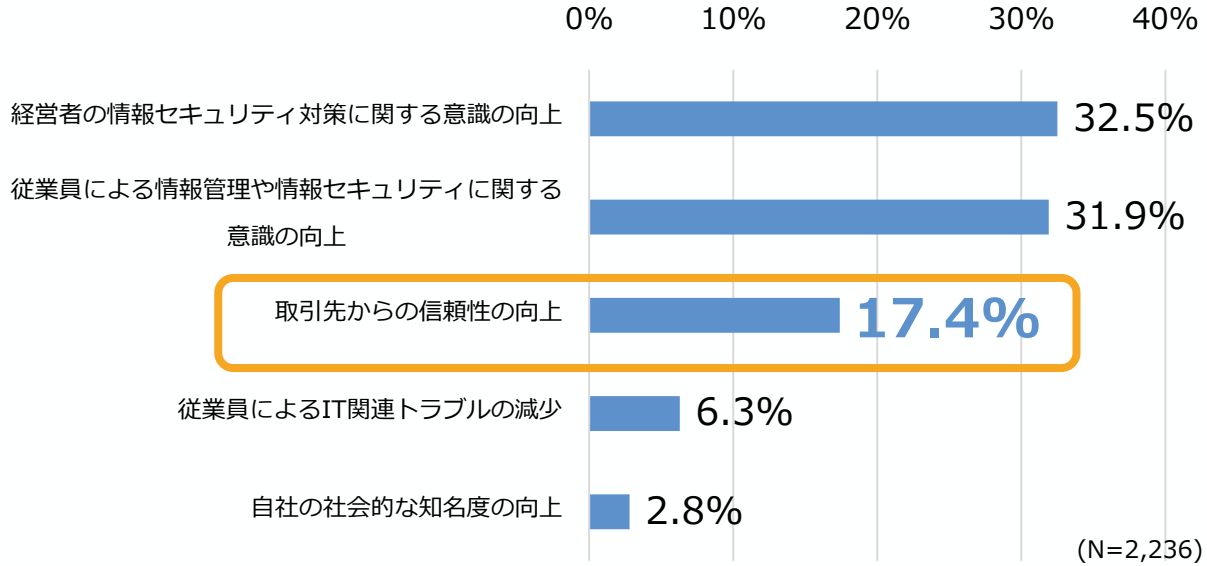


⇒サイバーセキュリティ対策投資を行っている中小企業等の方が、取引につながったと考える割合が高い。

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

SECURITY ACTION 宣言による効果

SECURITY ACTION 宣言による効果のうち特に効果があったと感じるもの



⇒SECURITY ACTION自己宣言が「取引先からの信頼性の向上」につながったと感じる層が２割。

出典：IPA「2023年度 SECURITY ACTION宣言事業者における情報セキュリティ対策の実態調査　調査報告書」を基に経済産業省作成

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」**

１．サイバー攻撃の実態

２．中小企業が取り組むべきサイバー対策

３．中小企業支援策の新たな体系

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

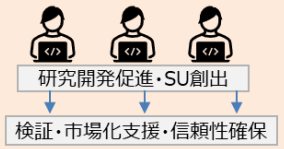
③政府全体でのサイバーセキュリティ対応体制の強化

- 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

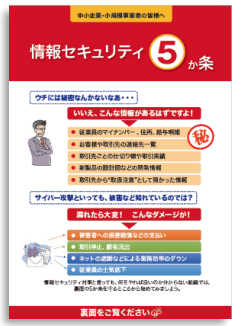
セキュリティ対策の第一歩「SECURITY ACTION」

- **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。

（参考）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

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）

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。

医療機関におけるお助け隊サービス導入事例

無床、職員約20名の診療所

サイバー被害をきっかけにお助け隊サービス（ネットワーク監視）を導入。定期レポートで安心感が向上！

導入きっかけ

過去に小さなセキュリティインシデントを経験し、医療機関での事例報道もあり、危機感を持っていました。院内でセキュリティルールを定め、UTM導入を検討しましたが、1台100万円～150万円の導入費用と月額数千円～1万円の運用費が課題でした。高額で断念しかけたところ、「お助け隊サービス」を知り、すぐに導入を決めました。

導入したサービス

お助け隊サービス（ネットワーク監視型/ UTM）を導入しています。

※UTMとは、複数の異なるセキュリティ機能を1台の機器に統合して、機器の管理や運用の負担を低減すると共に、集中的なネットワークの脅威管理を実現する、セキュリティ機能を集約した機器です。

お助け隊サービスの良いところ

外部からの攻撃をシャットアウトしてくれるという信頼感と、定期的レポートによって異常な攻撃がなかったことを確認できる安心感があります。

産業機械商社におけるお助け隊サービス導入事例

従業員数30名弱の電気設備資材卸売業

サイバー被害をきっかけにお助け隊サービス（端末監視型）を導入。ネットワークの見える化で社員の意識も向上！

導入きっかけ

以前に、リモートワーク中の営業社員がEmotet（エモテット※ ）に感染し、メールアドレスが乗っ取られ、お客様数社にも不正なメールが送信されました。幸いお客様の端末感染の連絡は無く、社内端末の感染もありませんでしたが、もし感染が広がってれば、お客様の信用失墜、営業停止まで至った可能性があります。

※ Emotet（エモテット）：ウイルスの一種。ユーザアカウントやアドレス帳、過去のメール履歴などを窃取し、その情報を元になりすましメールを送信し、感染を拡大させる。

導入したサービス

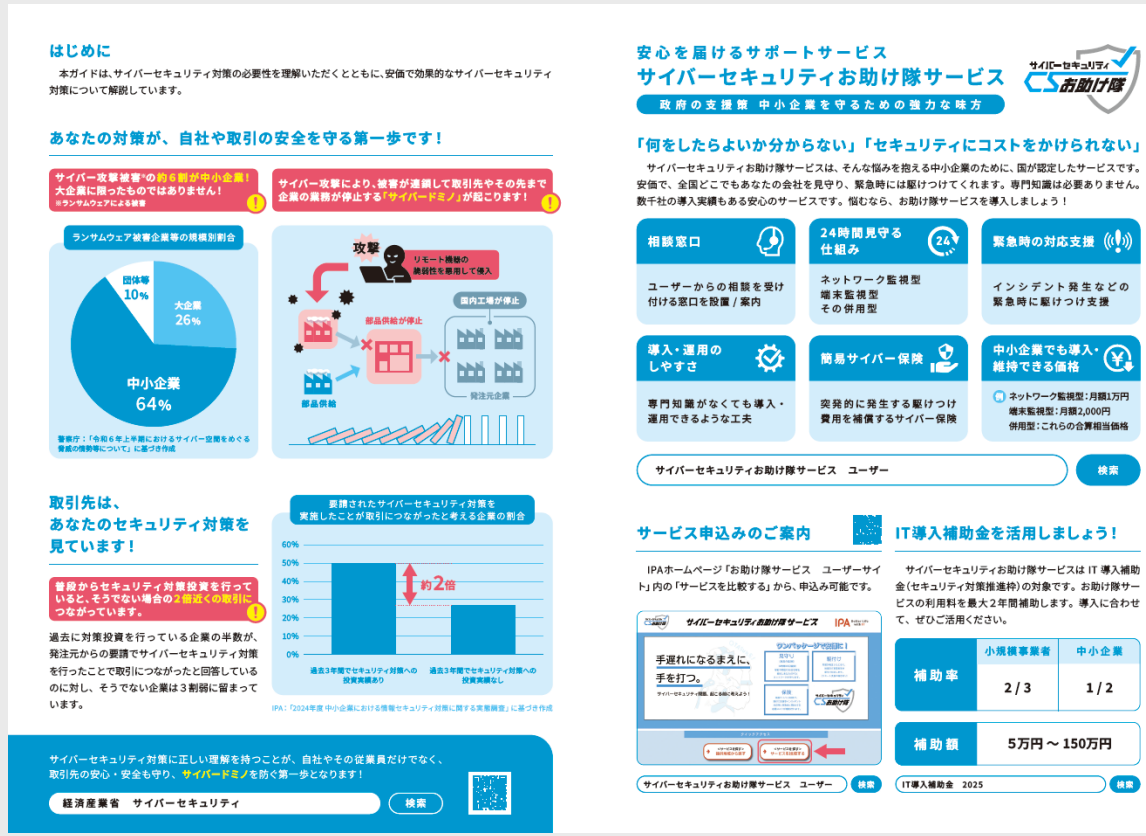
お助け隊サービス（端末監視型／EDR） の導入により、端末から不正サイトへのアクセスをブロック、ウイルスに感染した時は自動でネットワーク隔離対処を行えるようになりました。テレワークでも社員が安心して業務ができるようになりました。

お助け隊サービスの良いところ

端末ごとの不正アクセスレポートをグループウェアにあげて、全員で見れるようにしています。これは、社用車に搭載しているドライブレコーダーと同様に、ネットワークへのアクセス状況の見える化として社員のセキュリティ意識を高めるとともに、インシデント発生時の原因究明に役立つと考えています。

（参考）サイバーセキュリティ啓発用リーフレットによる周知・啓発

- 中小企業に向けて、**サイバーセキュリティ対策の必要性**と、安心・安全の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を普及**するため、リーフレットを作成。
- 経済産業局・総務省総合通信局、都道府県警のほか、商工会議所などの中小企業支援機関や銀行協会等と連携して幅広い中小企業へ配布し、**<u>サイバーセキュリティに対する認知度向上</u>**を実施。



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（現行版）

- 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。
- **令和７年度中に改訂を実施**予定。

- 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

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

（参考）第１部 経営者編　～経営者が認識すべき「３原則」～

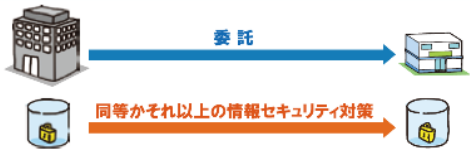
- 経営者は、以下の**３原則**を**認識**し、対策を進める。

原則１	情報セキュリティ対策は経営者の**リーダーシップ**で進める

- 経営者は、IT活用を推進する中で、情報セキュリティ対策の重要性を認識し、自らリーダーシップを発揮して対策の実施を主導

原則２	**委託先**の情報セキュリティ対策まで考慮する

- 必要に応じて委託先が実施している情報セキュリティ対策も確認し、不十分な場合は対処を検討



原則３	関係者とは常に情報セキュリティに関する**コミュニケーション**をとる

- 情報セキュリティに関する取組方針を明確に整理し、常日頃より関係者に伝えておくことで、サイバー攻撃によるウイルス感染や情報漏えいなどが発生した際にも、関係者の不信感の高まりを抑えることが可能

（参考）第1部 経営者編　～経営者が実行すべき「重要7項目の取組」～

- 経営者は、以下の**７項目**を**自ら実践**するか、実際に情報セキュリティ対策を実践する**責任者・担当者に対して指示**し、確実に実行することが必要。

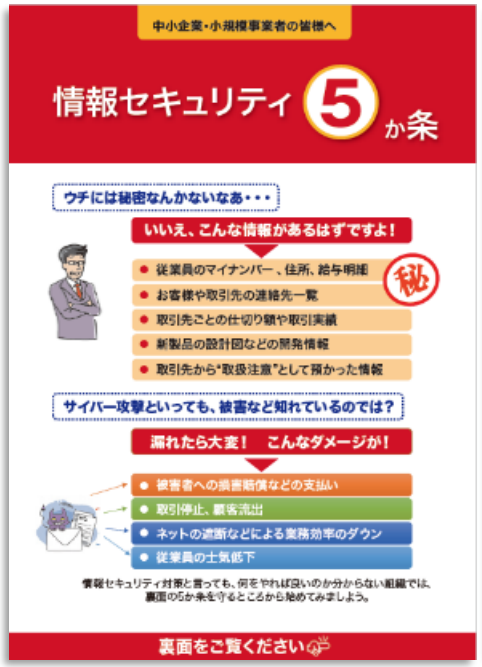
取組 1	情報セキュリティに関する組織全体の対応方針を定める
取組 2	情報セキュリティ対策のための予算や人材などを確保する
取組 3	必要と考えられる対策を検討させて実行を指示する
取組 4	情報セキュリティ対策に関する適宜の見直しを指示する
取組 5	緊急時の対応や復旧のための体制を整備する
取組 6	委託や外部サービス利用の際にはセキュリティに関する責任を明確にする
取組 7	情報セキュリティに関する最新動向を収集する

（参考）第２部 実践編

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

● できるところから始めて段階的にステップアップ

Step1
できるところから始める



情報セキュリティ５か条

SECURITY ACTION ★一つ星を宣言

Step2
組織的な取り組みを開始する

５分でできる！
情報セキュリティ自社診断

SECURITY ACTION ★★二つ星を宣言

Step3
本格的に取り組む

情報セキュリティ関連規程

Step4
より強固にするための方策

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

より強固にするため方策

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

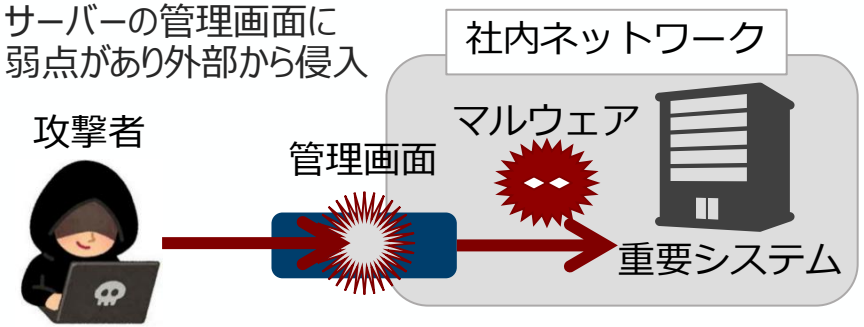
中小企業の経営者・情報システム担当者、中小企業の支援に携わる関係機関の皆様を対象とし、次のような活用を想定

- ✓ **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

令和6年度の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

１．サイバー攻撃の実態

２．中小企業が取り組むべきサイバー対策

３．中小企業支援策の新たな体系

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。

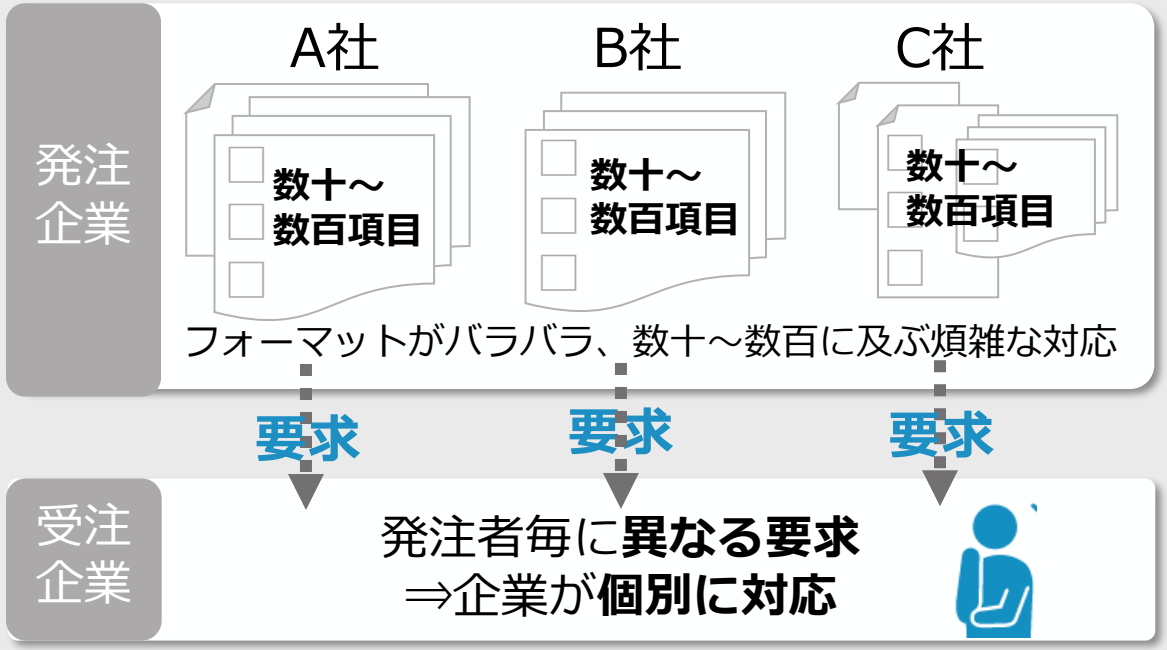
制度の普及施策（例）

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

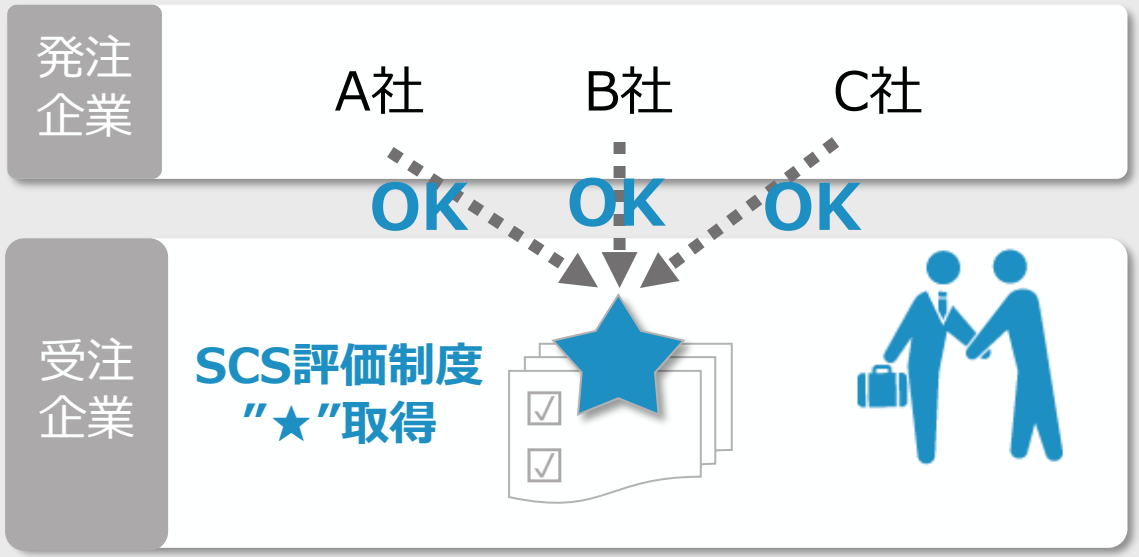
発注者ごとに異なる要求…対応が煩雑で非効率

- ✓ 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**

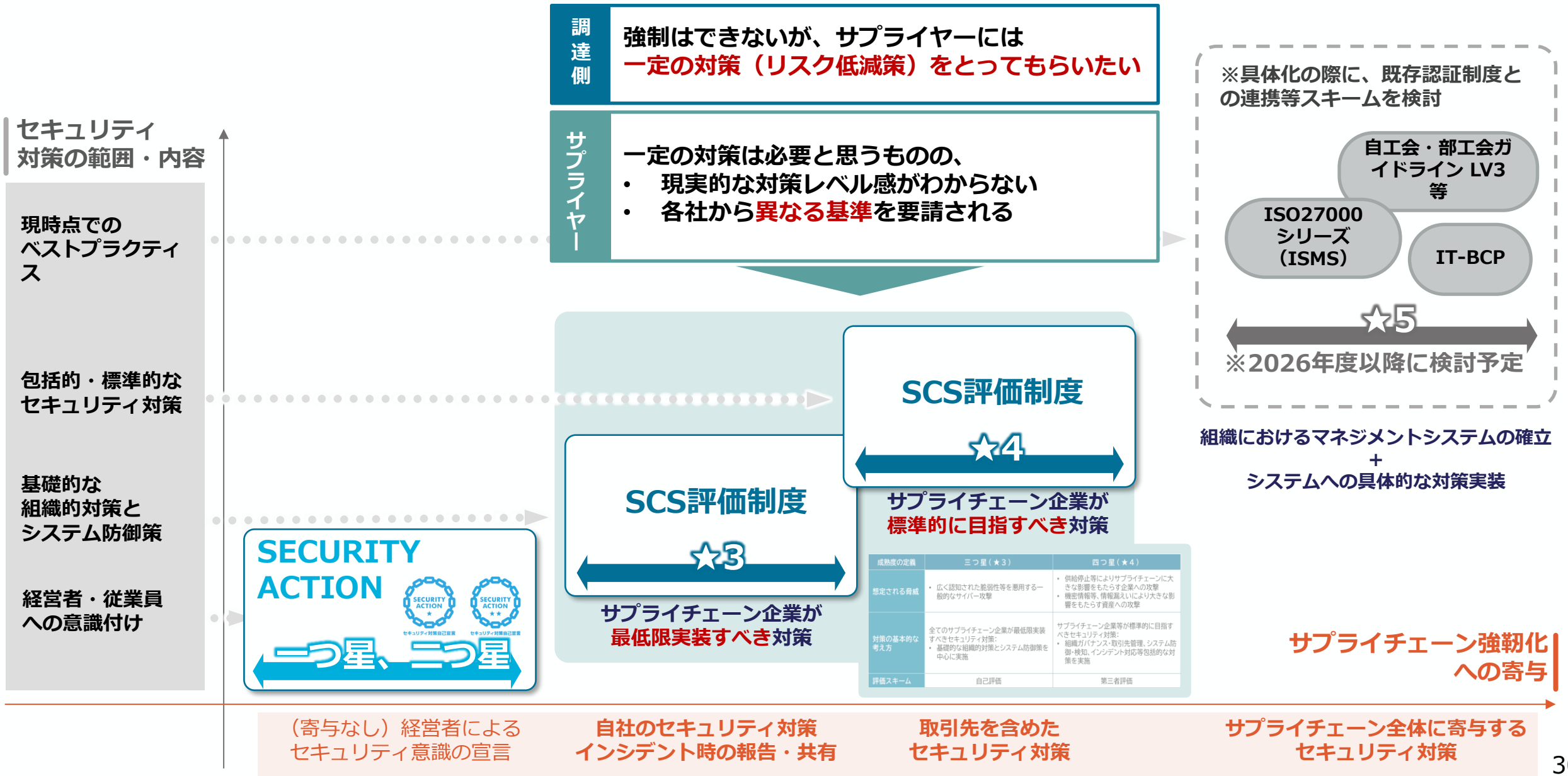


“★”取得で、発注者対応が一括クリア！

- ✓ 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）SECURITY ACTIONとの接続



（参考）制度で用いるセキュリティ要求事項・評価基準

- 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)

（参考）SCS評価制度を補足するガイダンス資料の整備

- ★３・★４要求事項・評価基準に加え、★取得希望組織による自己評価及び評価機関による第三者評価等を支援する観点から、具体的な評価手法やガイダンス情報を提示するためのガイダンス資料を今後策定する予定。

※　下記の図はあくまで本方針作成時点におけるイメージであり、完成後の文書とは異なる場合がある。

★３・★４要求事項・評価基準

要求事項

1-2-1 セキュリティを担当する部署及び従業員を決定し、責任及び権限を割り当てること。

評価基準

1-2-1-1 セキュリティを統括する役員(CISO 等)やセキュリティ担当部署の役割・責任を定めること
1-2-1-2 平時のセキュリティ推進活動に必要な連絡先リストを定めること
1-2-1-3 年1回以上の頻度及び必要に応じて、No.1-2-1-1及びNo.1-2-1-2にて定めた平時の体制について点検を行うこと
1-2-1-4 セキュリティリスクは、経営に重大な影響を及ぼすことを理解し、その対応について情報セキュリティ委員会等の経営判断ができる体制を設置していること

⋮

具体的事項や手法について補足

★３・★４ 自己評価ガイド(仮称)

【1-2-1-1の解説・評価方法】

・・・

【1-2-1-4の解説・評価方法】

■ 情報セキュリティ委員会のような特別な体制を設置している場合、体制の代表者は、必ずしも役員である必要はなく、部門長クラスの就任でもよい。
■ 情報セキュリティ委員会のような特別な体制がない場合、経営会議や取締役会等のより上位の会議体の議題として年1回以上の頻度で取り上げられることが定められているか、又はそれに相当する記録があるかを確認する。

⋮

★４ 第三者評価ガイド(仮称)

【1-2-1-1の評価方法】

■ 面談：「CISO 等やセキュリティ担当部署の役割・責任」(1-2-1-1)について社内規程等に定められているか確認を行う。

【1-2-1-2の評価方法】

■ 閲覧：「平時のセキュリティ推進活動に必要な連絡先リスト」(1-2-1-2)について現物確認を行う。

⋮

★４ 技術検証ガイド(仮称)

実施手順

① 特定されたIPアドレスを、推奨されるTCP/UDPポートとセットでスキャンすること。
② インターネットにアクセス可能なサービスのうち、脆弱性等悪用時に内部への不正アクセスのリスクが高いものについて、以下の事項の確認を実施すること。

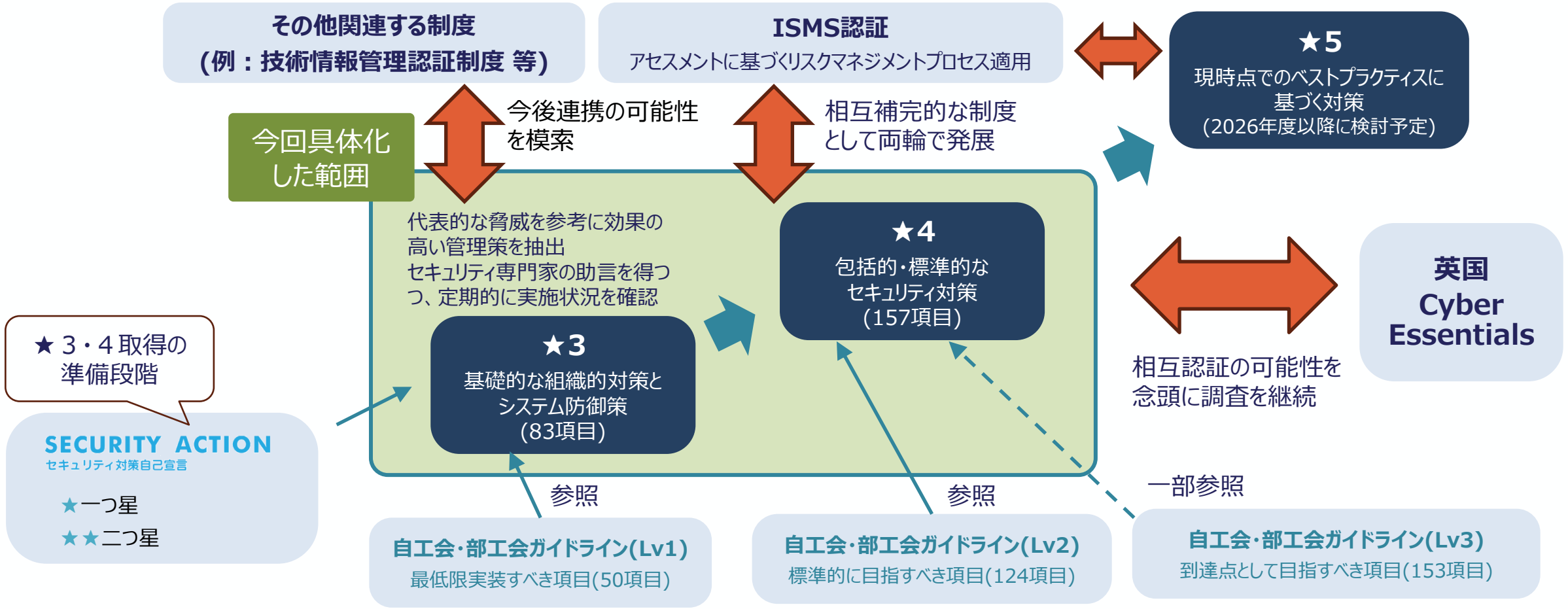
- CVSS 7.0以上の脆弱性の有無
- 多要素認証の実装有無
- 初期パスワードの変更有無

⋮

・・・

（参考）SCS評価制度と国内外の関連制度等との連携・整合

- 本制度(★３・★４)は、先行する仕組みである「SECURITY ACTION」「自工会・部工会ガイドライン」や、国際標準であるISMS適合性評価制度等と相互補完的な制度として発展することを目指す。
- ★３・★４は、自工会・部工会ガイドラインのLv１、Lv２に対応。自工会・部工会とは、本制度との連携を引き続き検討。英国CEとは、将来的な相互認証等の可能性も念頭に、引き続き調査・意見交換を継続。



導入促進の全体像

- ★取得のための各プロセスにおいて推進している支援策について、以下のとおり整理した。

発注元企業	★の取得を求める				
サプライヤー企業		制度について知る	必要な対策を講じる	★を取得する	★を更新等する
実施事項	■ ★の取得をサプライヤー企業に求めることを通じてサプライチェーン全体のサイバーレジリエンスを向上させる。	■ 制度についてインターネット等で情報収集する。 ■ セミナーや講習等に参加する。	■ 必要に応じてベンダーやセキュリティ専門家からの協力を得つつ、★取得に必要なセキュリティ対策を講じる。	■ セキュリティ専門家からの確認(★3)、又は評価機関等からの第三者評価(★4)を受け、★を取得する。	■ ★の有効期限に基づき、適宜更新及びそれに必要な手続き等を行う。
導入促進策	✓ **取引先への要請等に係る考え方の整理** サプライヤー企業への要請に係る独占禁止法等との考え方整理	✓ **本制度の継続的な広報、周知** 制度に対する活用意欲を向上させる広報や周知活動を継続的に実施	✓ **中小企業セキュリティ普及促進** ★3・★4に対応した、新しいお助け隊サービスの開発を検討	✓ **取引先への要請等に係る考え方の整理** 発注元企業は、★取得による価格交渉に積極的に対応する必要がありかつ委託先にこれを周知する必要がある等	
	✓ **業界毎の特性を踏まえた導入促進** 各業界のセキュリティガイドライン等において、本制度の要求基準等の活用や★取得確認の推奨を推進	✓ **「中小企業の情報セキュリティ対策ガイドライン」の整備** 中小企業の情報セキュリティガイドライン及び付録サンプル規程において★の取得を支援		✓ **セキュリティ評価・対策支援人材の育成** 本制度に関わる人材育成のための、コンテンツや研修機会を整備	
	✓ **政府機関や重要インフラ事業者等における活用の推進** 政府調達での参照や重要インフラ事業者等での活用推奨等について検討	✓ **他のガイドラインや国内外の関連制度との整合性確保** 「SECURITY ACTION」「自工会・部工会ガイドライン」等との整合性の確保や、評価結果の本制度での活用などの連携方策を検討	✓ **専門家の活用促進** 「中小企業向けサイバーセキュリティ専門家リスト」を整備し、主に中小企業と専門家とのマッチングの仕組みを構築		

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

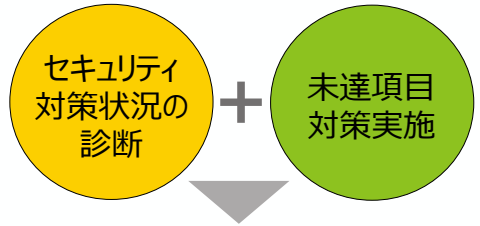
1. **組織的対策を含むセキュリティ対策を無料**で実施（実証期間中最大1年程度）
2. SCS評価制度の“★”**取得**が可能（SCS評価制度開始後の“★”取得要請への備えが可能）
3. サプライチェーン全体での対策強化に取り組む企業として、**取引先との信頼性向上**に繋がる

（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

サイバーセキュリティお助け隊サービス（新類型）実証事業の周知・啓発

- 中小企業向けに「SCS評価制度」や「サイバーセキュリティお助け隊サービス（新類型）の実証事業」を周知するため、**広報用リーフレットを作成し、経済産業省ホームページ内に特設サイトを開設。**
- 全国の中小企業やその支援機関、ITベンダー等へ展開するため、経済産業局と連携のうえ、**各地の業界団体・支援機関等を訪問**し、周知・啓発活動を実施。
- 今後の実証事業の参加募集などの情報は、特設サイトにて**順次掲載**していく予定。

中小企業向けのリーフレットの作成

全国の経済産業局と連携し、総合通信局、都道府県警察をはじめ、中小企業支援団体（商工会議所、情報産業協会、経済連合会等）、ITベンダー、業界団体等へ広く展開

経済産業省　特設サイトの作成

経産省　セキュ活　**検索**

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

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）「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】

- □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！
- **□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】

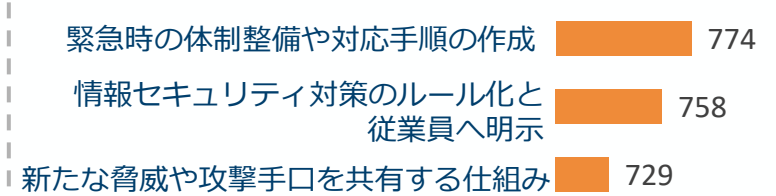
中小企業が読んだ際の重複感を避ける観点から、**関連がある項目を、内容の趣旨は維持したまま整理**

- ✓ 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

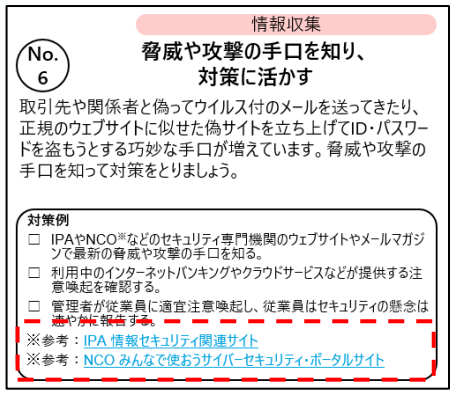
実施率の低い項目の見直し

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

（参考）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

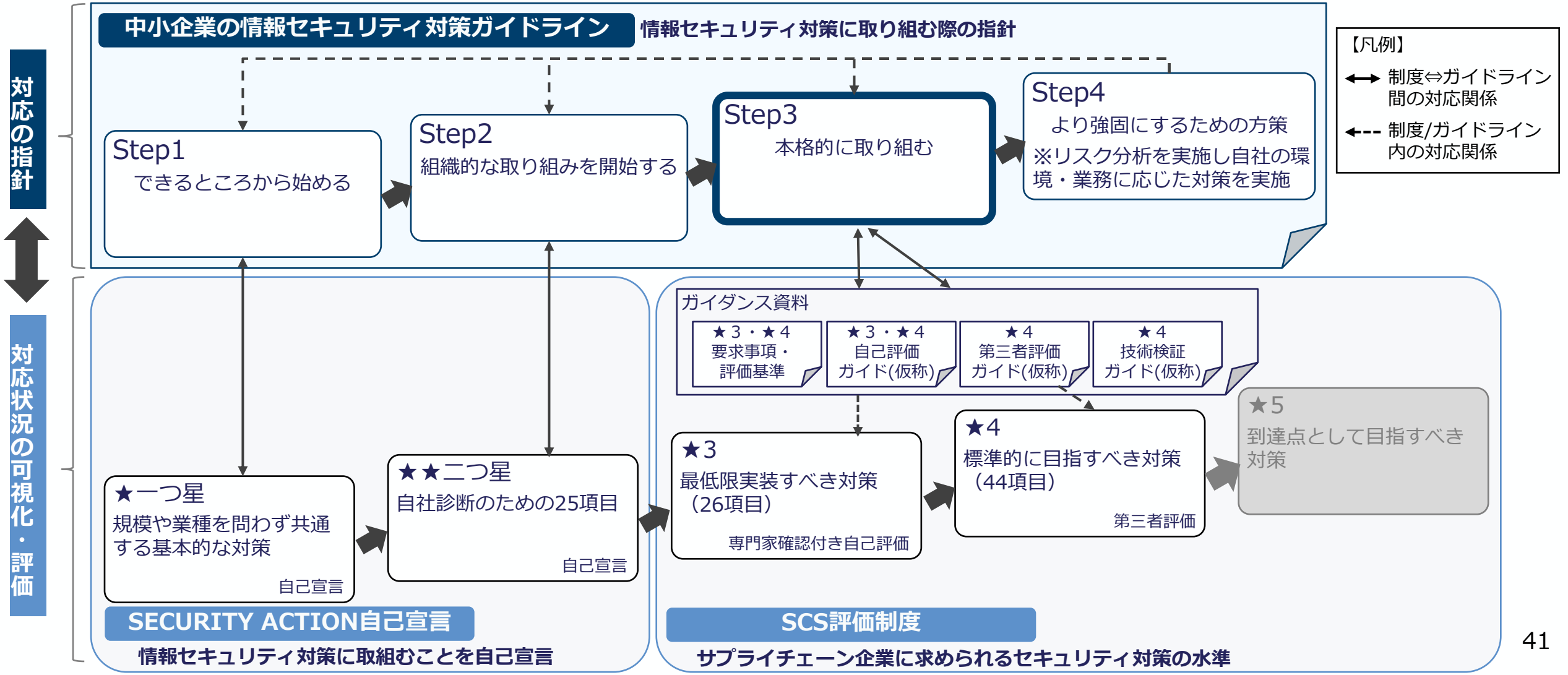
➢ **各STEPの対策について、「自社でやるならどう進めるか」を考える際の参考として活用できる構成**

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**。

（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。



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）

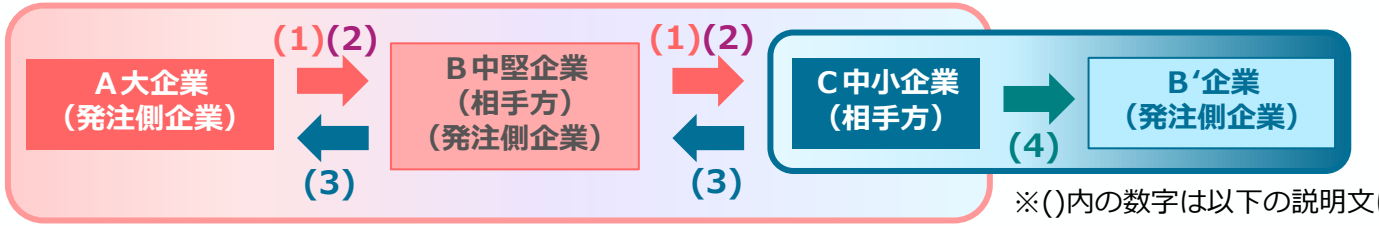
２０２５年１２月２６日
経済産業省・公正取引委員会

○　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。

本日のまとめ

1. サイバー攻撃は**決して他人事ではなく**、自社だけで無く**顧客や取引先**にも影響が及ぶ

2. 中小企業が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まとめた**事例集**を公開予定

3. 経済産業省では、**「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）」を中心とした**中堅・中小企業等支援策の新たな体系を構築中

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

経済産業省　サイバーセキュリティ　検索