

サプライチェーン全体でのサイバーセキュリティ 対策強化に向けた経済産業省の取組

経済産業省商務情報政策局サイバーセキュリティ課

1. サプライチェーンを取り巻く状況について

2. 経済産業省の支援策

2-1 これまでの施策

2-2 これからの施策

最近国内外で発生した主な事案

①機微技術情報等の窃取

- 2019年以降、中国の関与が疑われるグループ「MirrorFace」による、日本の安全保障や先端技術に係る情報窃取を目的とした攻撃キャンペーンが実行されている。(2025年1月 警察庁及びNISC(現:NCO)が注意喚起)

②事業活動の停止

- 2024年6月、(株)KADOKAWAがランサムウェアを含む大規模サイバー攻撃を受け、Webサービス等が停止。大量の個人情報や企業情報が漏えいした上、SNS等を通じて拡散される二次被害も発生。
- 2025年10月、アスクル(株)がランサムウェア感染により受注・出荷業務を停止。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(株)等においてもネットストアでの受注・出荷業務が停止。
- 2025年9月、アサヒグループホールディングス(株)に対するランサムウェア攻撃により、国内の酒類や飲料、食品の受注や出荷業務が停止され、主要工場の生産も一時的に停止するとともに、決算発表を延期。情報漏えいの可能性も確認。

③重要インフラの機能停止等

- 2024年2月、米国政府機関等が、中国を背景とするグループ「Volt Typhoon」による米国の重要インフラを標的とした活動(有事の際にサイバー攻撃を行うためにネットワークへのアクセス権限を確保するような動き)について注意喚起。
- 2024年12月～2025年1月の年末年始にかけて、航空事業者、金融機関、通信事業者等が相次いでDDoS攻撃を受け、サービスの一時停止等の被害が発生。(2025年2月 NISC(現:NCO)が注意喚起)

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・金銭等資産の窃取

- 2025年4月、(株)インターネットイニシアティブのメールセキュリティサービスへの不正アクセス事案が発生。メールアカウントや他社クラウドサービスの認証情報など、586の契約先において情報漏えいが確認。(2025年4月22日時点)

(参考) IPA「情報セキュリティ10大脅威」

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

中小企業の被害が全体の6割以上を占める

相対的にセキュリティ対策の弱い中小企業を起点に、大企業含むサプライチェーンを共有する企業を攻撃

初選出

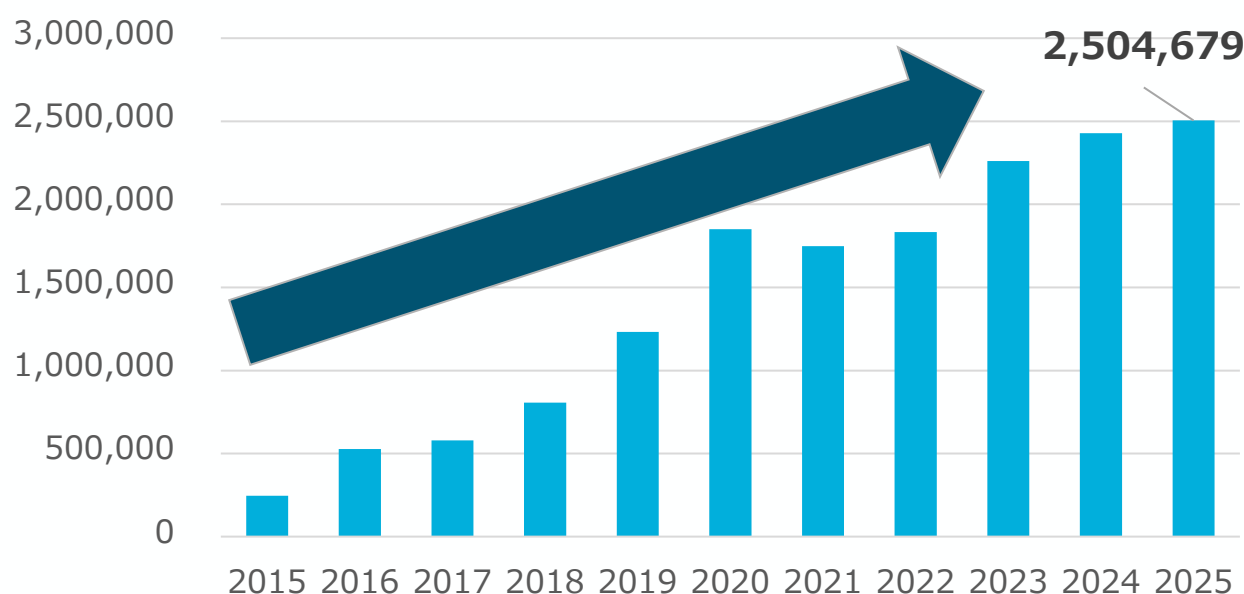
約138回

何の数字でしょうか？

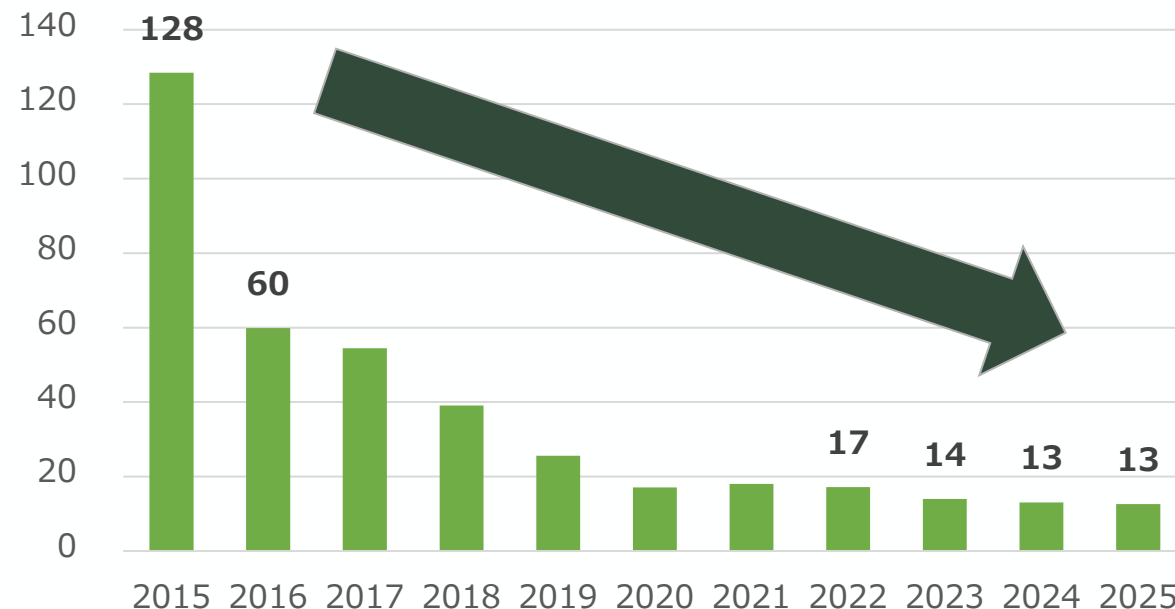
サイバー攻撃関連通信は「13秒に1回」観測される時代に ⇒30分間では138回に相当（6年前だと141回）

ダークネット観測において確認された「サイバー攻撃関連通信」（1 IPアドレス当たり）

年間総観測パケット数



サイバー攻撃関連通信の観測間隔（秒）



出典：国立研究開発法人情報通信研究機構「NICTER観測レポート2025」を基に経済産業省作成

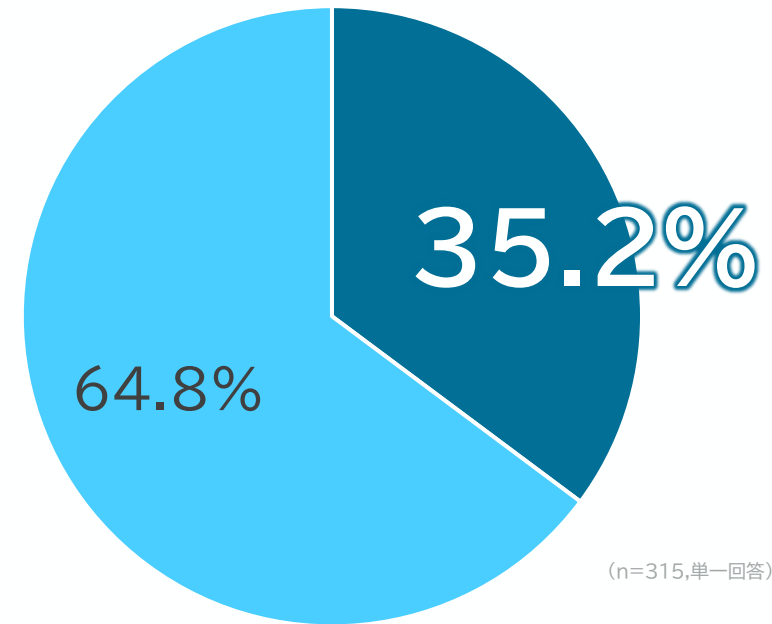
※「サイバー攻撃関連通信」の定義：“ダークネットに届くパケットの総称。マルウェアに感染した機器がインターネット上で次の感染先を探すためのスキャンパケットや、DoS攻撃を受けているサーバからの跳ね返りパケット（バックスキッタ）などが含まれる。”（上記出典より引用）

DXの進展が、サイバー攻撃を拡大させた

- DXは導入企業の恩恵も大きいですが、**攻撃者側の”魅力”も大きく**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」

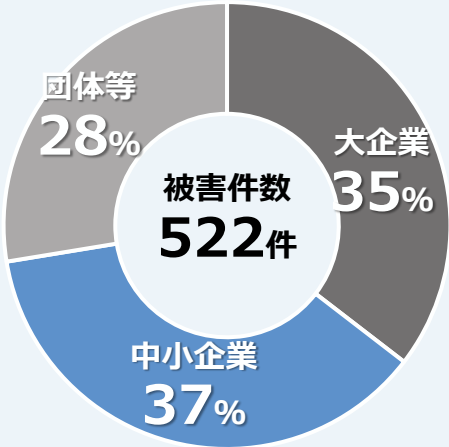


- セキュリティインシデントは発生した
- セキュリティインシデントは発生していない

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、多くの場合、その結果として取引先・サプライチェーンにも影響を及ぼしている。

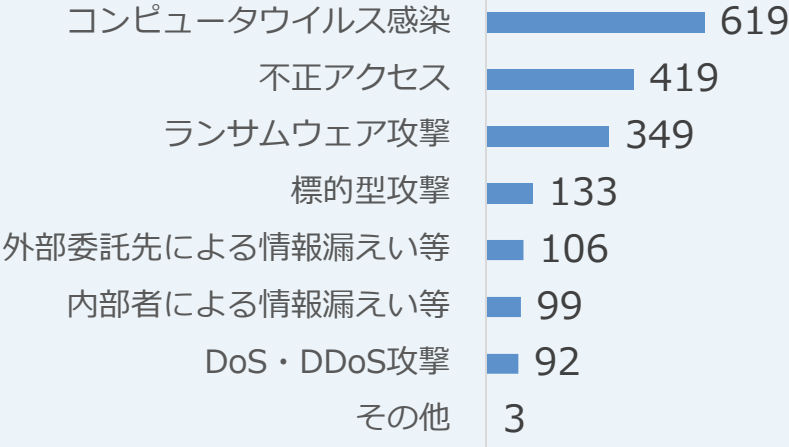
サイバー攻撃の被害組織の規模別割合（2022年7月～2024年6月）



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は発生している状況

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

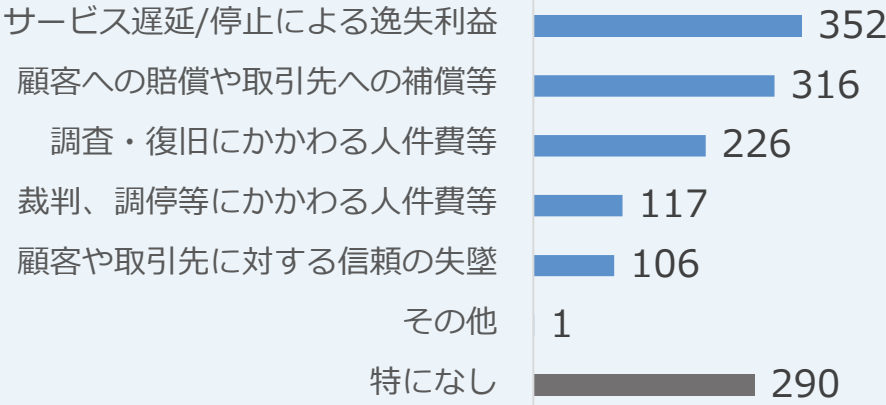
中小企業が実際に受けたサイバーインシデント（複数選択可、回答企業975社）



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

顧客・取引先にも影響が及ぶ

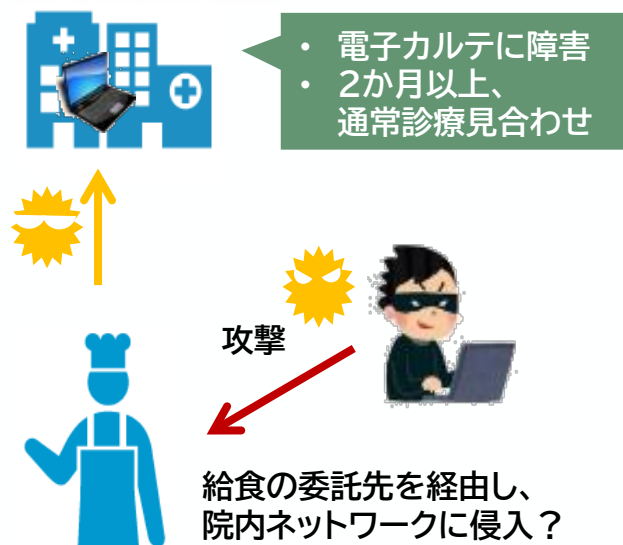
- 攻撃者は、防御レベルの低い組織を踏み台に狙う 被害は自社だけの問題では終わらない

【実際の事例】 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

1

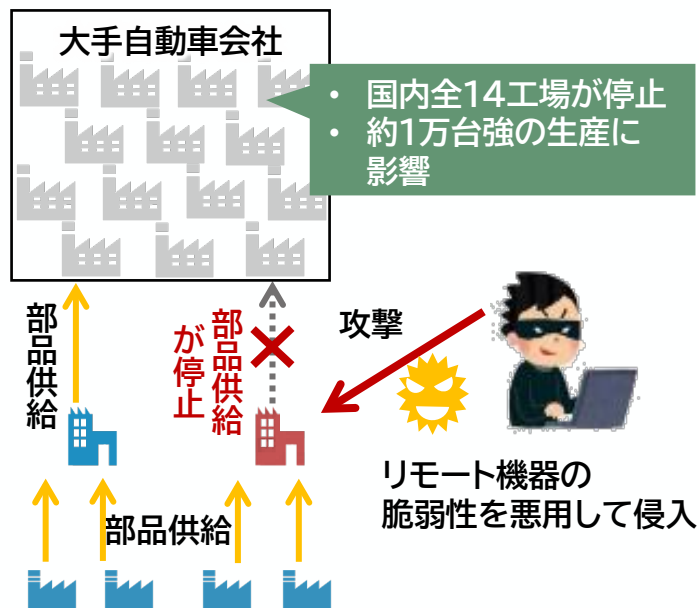
給食委託業者を通じた 公立病院への侵入・診療見合せ

ランサムウェア感染



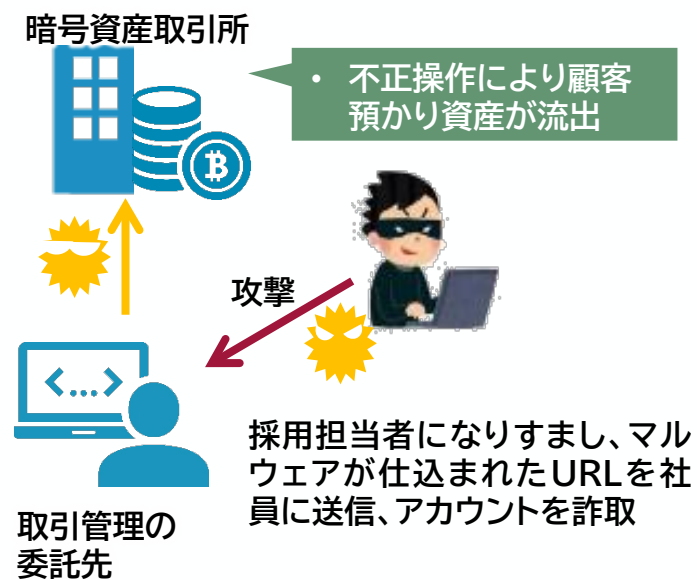
2

自動車部品会社の感染による 大手自動車会社の操業停止



3

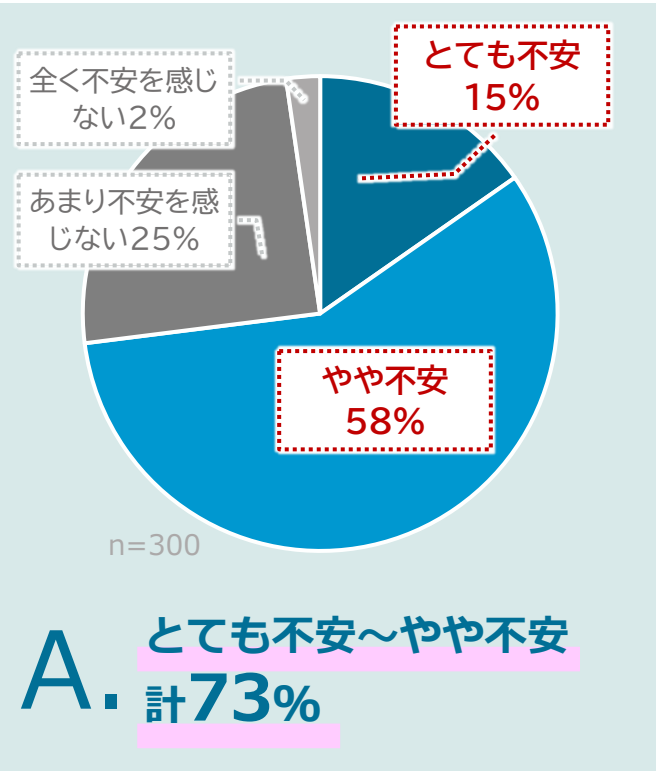
委託先への接触を通じた暗号資産取引所への侵入・資産流出



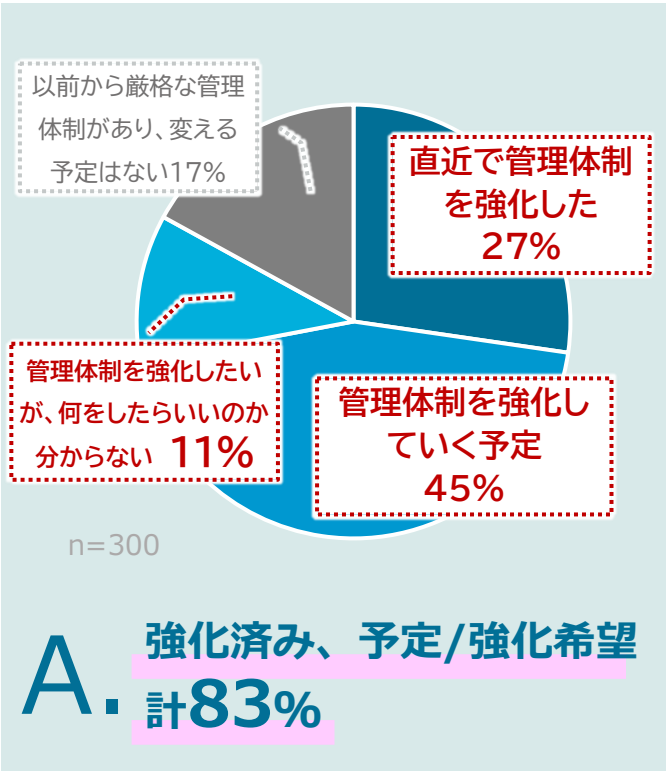
傘下/取引先企業への対策要請ニーズの高まり

- 大手企業の約 7 割が取引先企業のセキュリティに不安 ← 実際取引先起因の事案発生

Q. 取引先企業に対してセキュリティ上の不安を感じるか



Q. 取引先のリスク管理体制を強化・見直す動きがあるか



Q.取引先企業を起因とした情報漏えい、業務停止や遅延などの影響が発生した事例の有無（複数回答）

取引先企業のシステムでマルウェア感染(ランサムウェア含む)、システム停止に伴う自社の業務停止や遅延等の影響	29.7%
取引先企業のシステムでマルウェア感染(ランサムウェア含む)	26.3%
取引先企業のシステム経由で自社のシステムにサイバー攻撃やマルウェア感染	25.3%
取引先企業のシステムで計画外停止や障害(システム故障や緊急メンテナンスなど)が発生、システム停止に伴う自社の業務停止や遅延等の影響	23.3%

取引先起因の情報漏洩/業務影響はよくあること

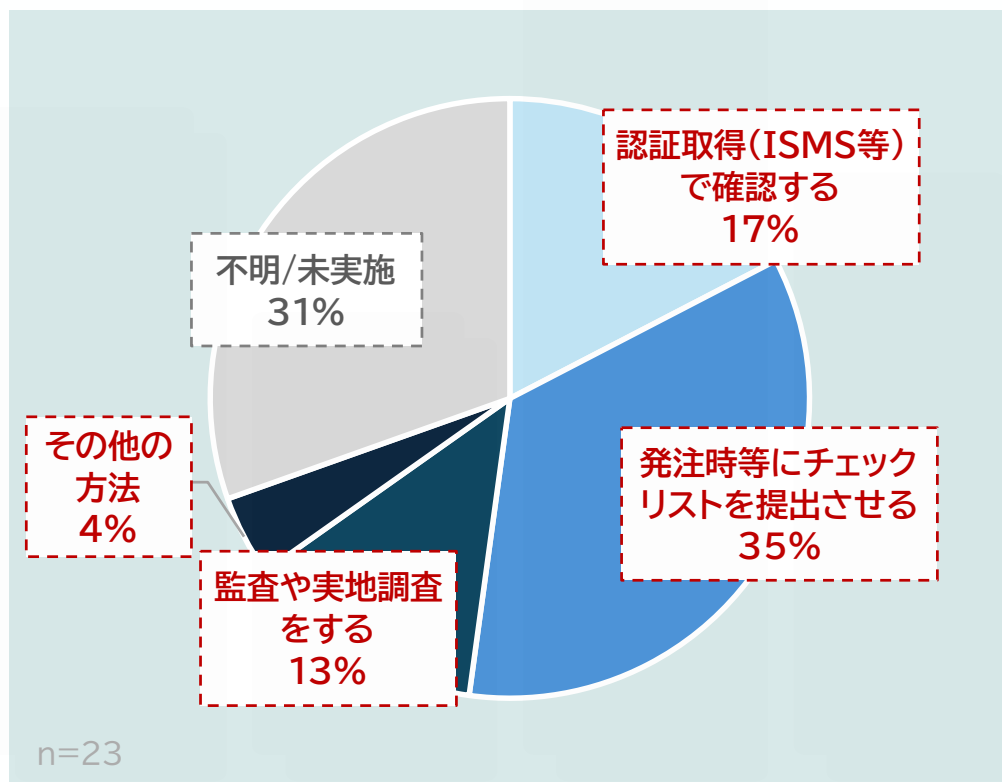
出典：「株式会社アシュアード調べ」（従業員数1,000名以上の大手企業の情シス部門300名を対象として2025年5月に実施された実態調査）を基に、経済産業省にて加工

発注元は、チェックリスト、認証取得、実地調査等に対応

- 大手企業の約7割が、独自に取引先企業のセキュリティ対策評価を実施するも、課題が残る

Q. 主たる委託先のセキュリティ対策評価の実施方法は？

あるコンソーシアム参加の大手企業23社(業態多数)へ聞きました



出典：経済産業省商務情報政策局サイバーセキュリティ課(令和7年)

A. 約7割が取引先の対策評価を実施



複数の独自チェックリストが会社別に流通

- 委託先：異なる複数のチェックリスト対応
- 発注元：チェックリストの妥当性に不安

課題

高度な認証取得や複数企業からの監査/実地調査対応は、中小企業には重い負担に

(参考)取引先にセキュリティ対策を要請等している例

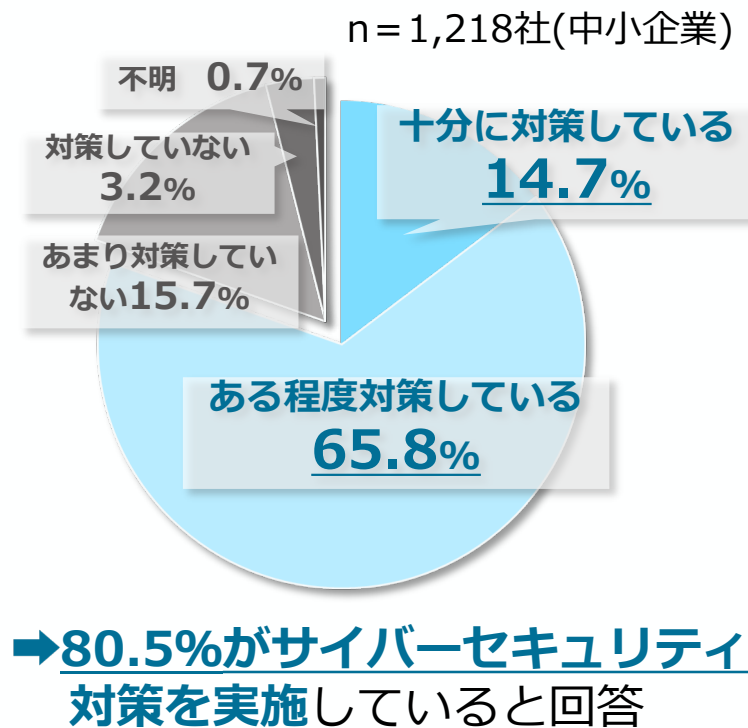
企業名	取組の概要
キオクシアホールディングス株式会社	○ 取引先企業約3,000社に対し、ウェブサイト等のセキュリティ設定や脆弱性の有無などを評価 ○ セキュリティ対応力の低い企業に対して改善を促す
TOPPANホールディングス株式会社	○ データ管理の委託先約500社に対し、外部診断ツールや訪問ヒアリングなどを組み合わせてセキュリティ対策状況を監査 ○ 改善が見込めない企業には重要情報の委託を停止 ○ 2025年度中には確認対象を製造部門の部門調達先にも広げ、重要な取引先にはサイバー被害発生時の対応策を新たに契約条件に盛り込むことも検討
DMG森精機株式会社	○ IT部門の担当者が調達部門とともに町工場等の取引先を訪問 ○ 両部門が共同で取引先向けの研修会を実施

中小企業のサイバーセキュリティ対策状況と内訳

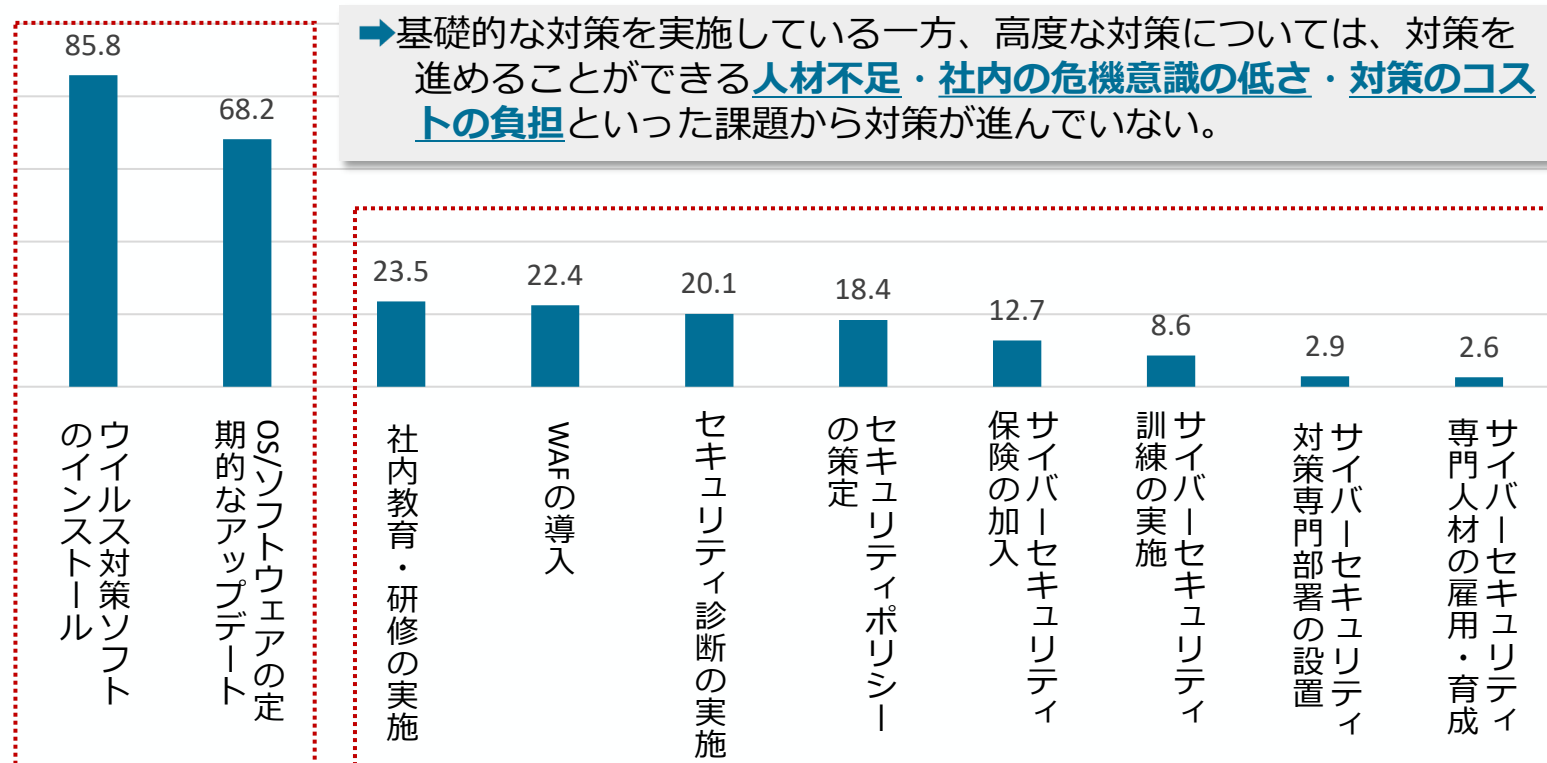
【東京商工会議所が実施した調査】

- 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。
- 対策の内訳については前回調査と同様、「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」といった **基本的な対策が中心**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 **高度な対策は依然として低水準**に留まる。

サイバーセキュリティ対策の状況



サイバーセキュリティ対策の内訳



1. サプライチェーンを取り巻く状況について

2. 経済産業省の支援策

2-1 これまでの施策

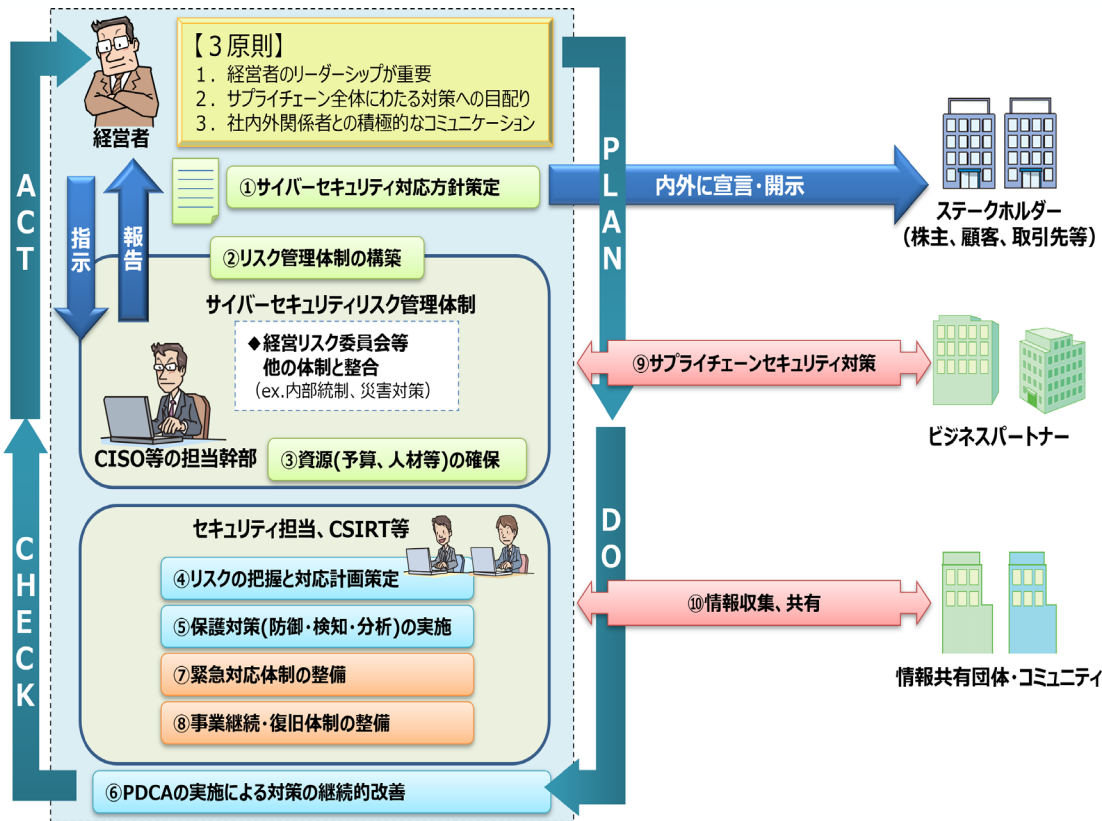
2-2 これからの施策

サイバーセキュリティ経営ガイドラインの全体像

平成27年12月28日策定
令和5年3月24日第3版公表

- 経営者がリーダーシップをとってセキュリティ対策を推進することが重要。このため、**経営者を対象としたガイドライン**を策定。可視化ツールや実践事例集なども整備。

1. 経営者が認識すべき3原則	
(1) 経営者が、 <u>リーダーシップ</u> を取って対策を進めることが必要	
(2) 自社のみならず、 <u>サプライチェーン全体にわたる対策</u> への目配り	
(3) 平時及び緊急時のいずれにおいても、 <u>社内外関係者との積極的なコミュニケーション</u> が必要	
2. 経営者がCISO等に指示すべき10の重要事項	
リスク管理体制の構築	指示1 組織全体での対応方針の策定 指示2 管理体制の構築 指示3 予算・人材等のリソース確保
リスクの特定と対策の実装	指示4 リスクの把握と対応計画の策定 指示5 リスクに対応するための仕組みの構築 指示6 PDCAサイクルの実施による継続的改善
インシデントに備えた体制構築	指示7 緊急対応体制の整備 指示8 事業継続・復旧体制の整備
サプライチェーンセキュリティ	指示9 サプライチェーン全体の状況把握及び対策
関係者とのコミュニケーション	指示10 情報収集、共有及び開示の促進



サイバーセキュリティ経営の考え方

＜サイバーセキュリティ経営ガイドラインの概要から引用＞

- 経営者は、組織の意思決定機関が決定したサイバーセキュリティ体制が当該組織の規模業務内容に鑑みて適切でなかったため、組織が保有する情報の漏えいなどにより会社や第三者に損害が生じた場合、**善管注意義務違反や任務懈怠に基づく損害賠償責任を問われ得るなどの会社法・民法等の規定する法的責任やステークホルダーへの説明責任を負う**。さらに、被害が深刻な場合の事業停止や新たな脅威に対処するための予算措置等の経営判断も要求され、担当者への丸投げは許されるものではない。
- **サイバーセキュリティ対策は「投資」（将来の事業活動・成長に必須な費用）と位置付けることが重要である**。直接的な収益を算出することは困難ではあるが、**企業の価値を維持・増大していく上で、企業活動におけるコストや損失を減らすために必要不可欠な投資**であるとともに、サイバーセキュリティリスクを組織の経営リスクの一環として織り込み、その観点からサイバーセキュリティリスクを把握・評価した上で対策の実施を通じてサイバーセキュリティに関する自社が許容可能とする水準まで低減することは、**企業として果たすべき社会的責任であり、その実践は経営者としての責務である**。

(参考) コーポレートガバナンス・コード改訂への反映状況

- 金融庁において、上場企業の持続的成長と企業価値向上を目的とした**コーポレートガバナンス・コード（CGコード）の改定**を令和7年度に実施（有識者会議を3回開催し、意見公募を経て2026年7月公表。）。
- 各原則の実質的な対応を支援するため、背景・目的・グッドプラクティス等を示す「**解釈指針**」を新設。
- これまでCGコードではサイバーセキュリティに関する明確な記載はなかったが、今回の改定では、**内部統制・リスク管理体制に関する解釈指針**の中で「**サイバーセキュリティリスクへの対応**」が**収益機会につながり得る取組**の一つとして、**明記された**。今後、**上場企業による当該事項への開示充実化が期待される**。

【原則4－4．取締役会の役割・責務Ⅲ：経営陣・取締役に対する実効的な監督②】

取締役会は、内部統制や全社的リスク管理体制を適切に整備すべきである。

【解釈指針】

内部統制や先を見越した全社的リスク管理は、適切なコンプライアンスの確保により持続的に信頼を維持し、リスクを最小化するために重要であるのみならず、経営陣が果断にリスクテイクを行うための裏付けとなり得るものであるから、取締役会は、グループ全体を含めたこれらの体制を適切に構築するとともに、内部監査部門を活用しつつ、その運用状況を監督すべきである。**サイバーセキュリティリスク**、国際的な経済安全保障を巡る環境変化等の地政学的要因によるサプライチェーン途絶リスク及び技術等の情報流出リスクへの対応等も、**収益機会にもつながり得るものとして、リスク管理体制を整備する際の考慮事項に含まれ得るとともに、そうしたリスクへの対応等が適切に行われるべき**である。

中小企業等向けの施策全体像

- 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

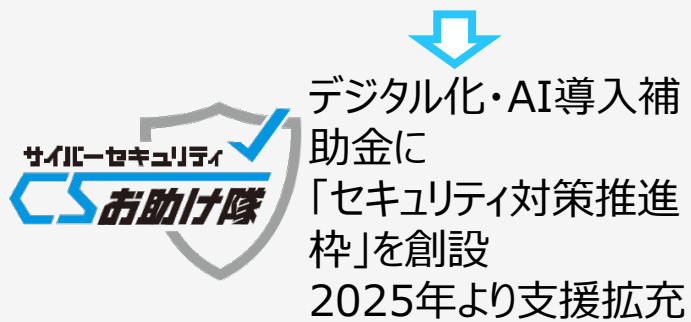
企業自らが、セキュリティ対策に取り組むことを**自己宣言**する制度。**約47万社**の企業が宣言。



⇒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**。（2026年3月時点で**47事業者**が提供し、約**10,900件**の利用実績。）

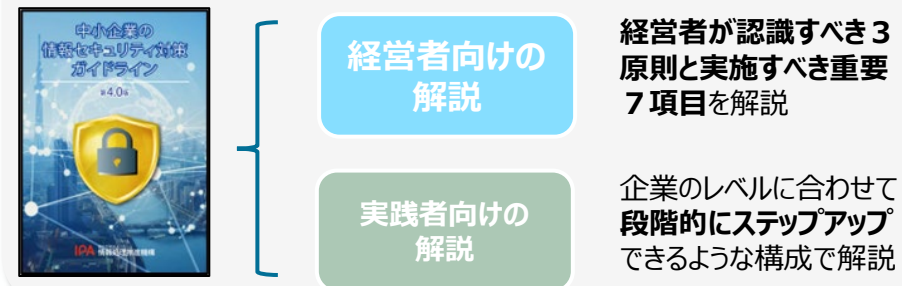


⇒必要最低限の対策を実行
（監視、駆付け、保険）

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。



⇒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47万者が宣言。
- 「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6か条に取り組む



【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！
- バックアップをとろう！
- 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。

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47事業者**がサービスを提供しており、**約10,900件**の利用実績（2026年3月時点）がある。
- デジタル化・AI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。
- 今後、サプライチェーン・セキュリティ対策評価制度に沿った新サービスを創設予定。

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/>



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

お助け隊サービス審査登録制度：

一定の基準を満たすサービスにお助け隊マークの商標利用権を付与

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）

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
 - － 「経営者編」では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
 - － 「実践編」では情報セキュリティ対策の具体的な進め方を4つのステップで分かりやすく説明
 - － 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



1. サプライチェーンを取り巻く状況について

2. 経済産業省の支援策

2-1 これまでの施策

2-2 これからの施策

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)の実現

- 「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※1を提示しつつ、その状況を可視化する仕組み※2を構築（2026年3月27日に「制度構築方針」を公表）。
- 3段階の水準のうち、★3・★4について、2026年度末頃の制度開始を目指し、スキームオーナーであるIPAとともに、制度運営基盤の整備や利用促進等を進めていく。2026年度以降に★5の設計も進める。
- 制度開始5年後（2031年）までに2万件、10年後（2036年）までに5万件の★取得を目指す。

※1 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。

※2 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。

構築する評価制度

成熟度の定義	★ 3	★ 4	★ 5 [検討中※3]
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さらに目指すべき高度な対策： 国際規格等におけるリスクベースの考え方にに基づき、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

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

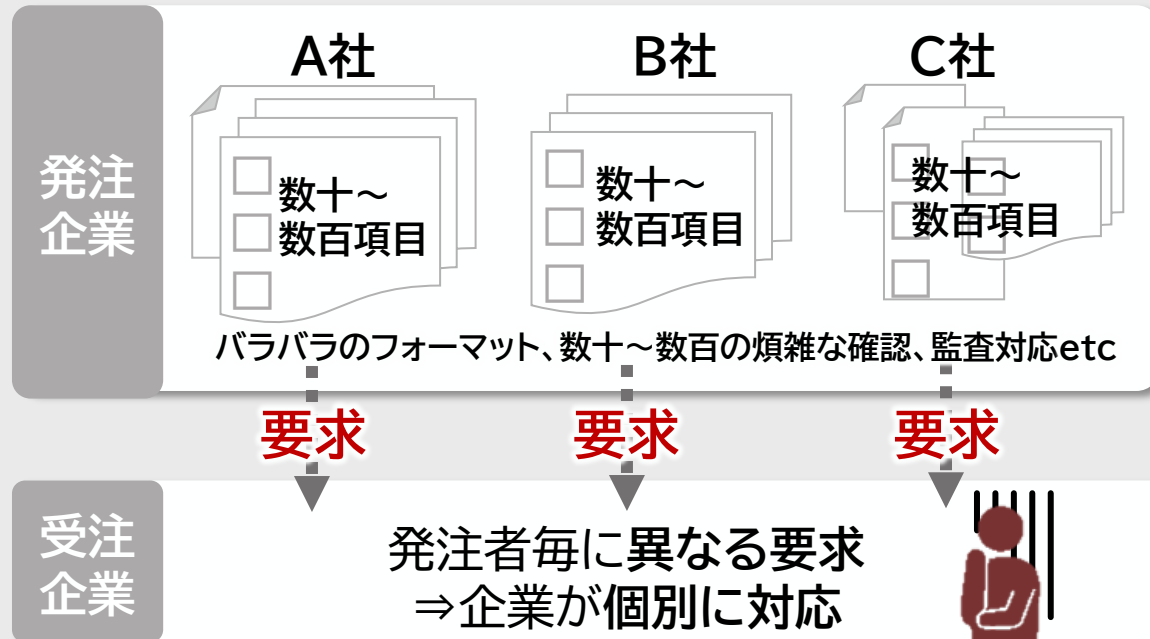
サプライチェーン間の結び付きが強固・複雑な主要製造業（自動車、半導体等）、流通、金融業等において、優先的に本制度の利用を促進。

※3 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

(参考)中小企業にとって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
- ✓ 複数社と取引時、**各社各様の要求に対応**するのが困難
- ✓ 各社の**要求は似て非なるもの&様式もバラバラ**で、内容理解も困難な上、**数百項目に及ぶ煩雑な対応が発生**

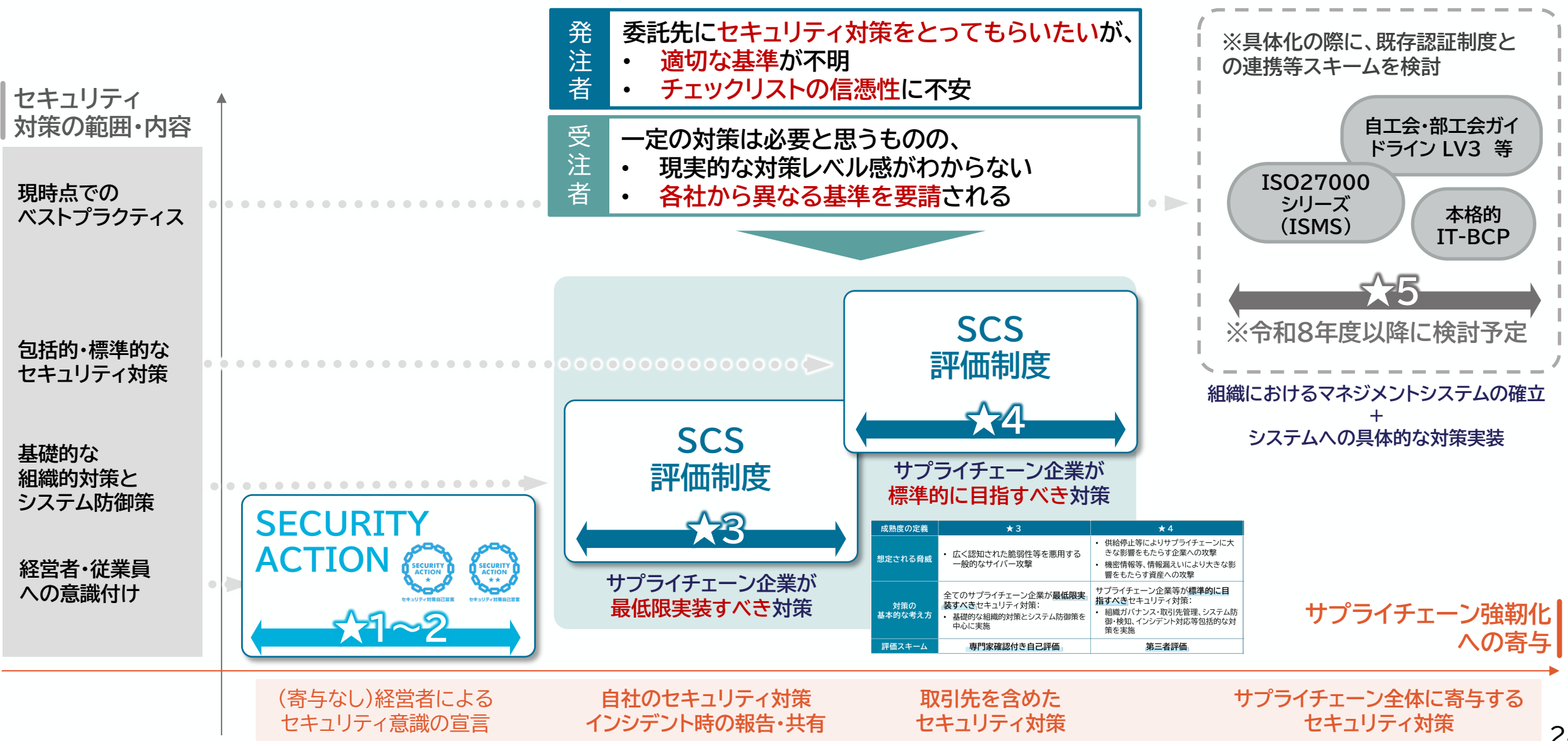


★取得で、受発注対応が一括クリア！

- ★取得が、受発注者双方にとって「共通のものさし」に
- ✓ 各社の要求に即答でき、**対応工数削減や業務の標準化・効率化**に繋がる
- ✓ 発注者との**信頼構築**や、発注先候補としての信頼向上による**新たなビジネスチャンス**に繋がる



(参考)SECURITY ACTIONとの接続

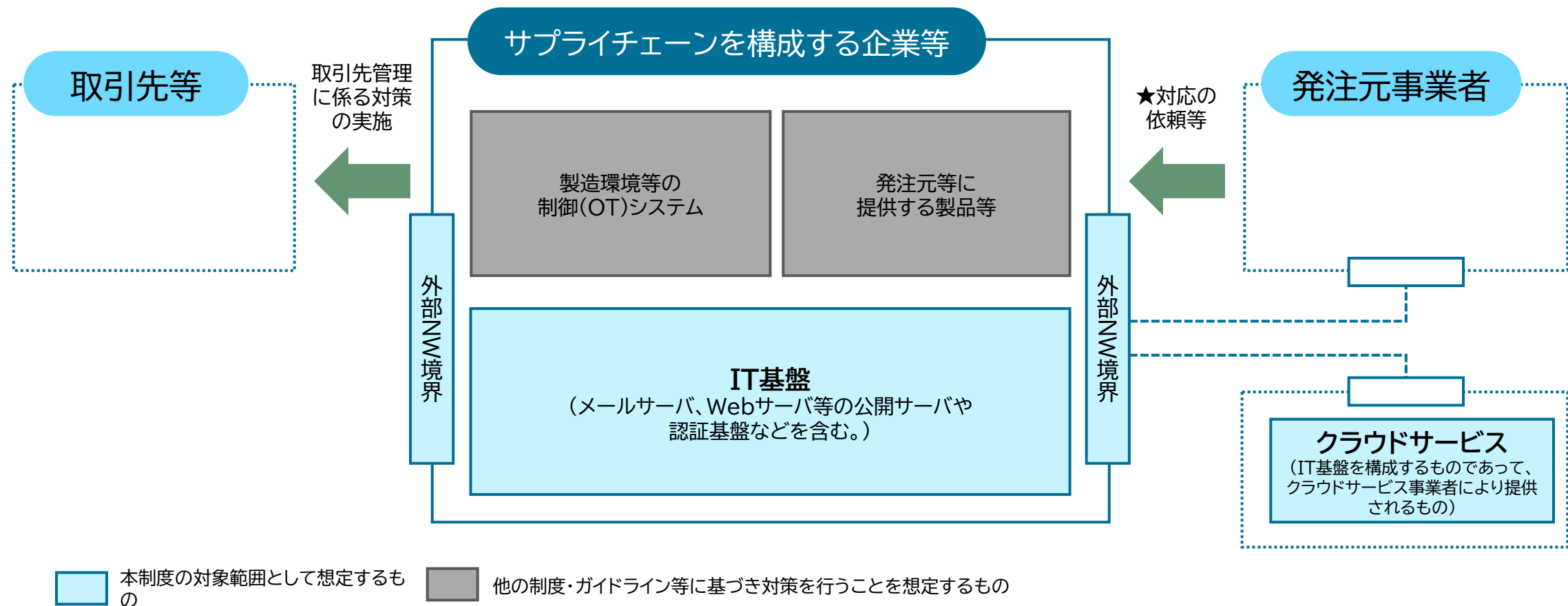


制度で用いるセキュリティ要求事項・評価基準(案)の概要

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一覧化 [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一覧化 [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]	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]	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]		復旧(RC)

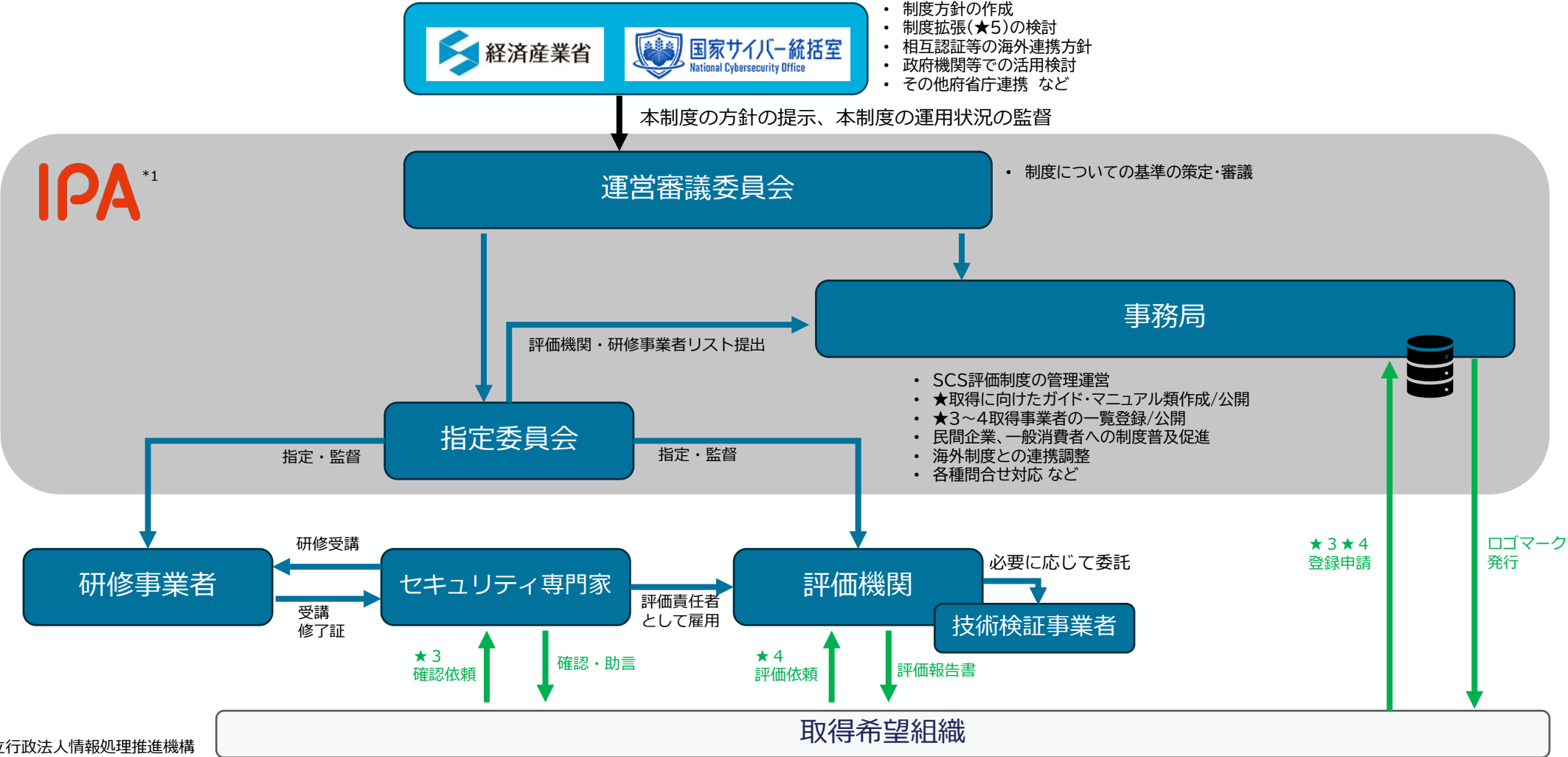
SCS評価制度の対象範囲

- 本制度は、サプライチェーンを構成する企業等のIT基盤(クラウド環境で運用するものも含む。)を対象とする。
- 一般的にIT基盤には該当しないと考えられる製造環境等の制御(OT)システム、発注元等に提供する製品等については求められる対応が基本的に異なることから直接の対象とはせず、他の制度・ガイドライン等に基づき対策を行うことを想定する。



制度の運用体制案

- 基本的な規則を維持管理するスキームオーナーには、社会全体への制度浸透や諸外国の制度との連携を今後調整していくことから、政府のガバナンスが効くことが重要となる。また、任意制度を新しく立上げ普及させるには高いハードルがある。こうした点を踏まえ、経済産業省の示す本方針に従い制度を構築し、同省の監督のもと制度を運営するスキームオーナーは、同省が所管官庁である独立行政法人情報処理推進機構（IPA）とする。



*1 IPA：独立行政法人情報処理推進機構

3.5 制度における評価スキーム

3.5.2 セキュリティ専門家、評価機関及び技術検証事業者の要件 - セキュリティ専門家の要件

- 「力量の保持/維持」及び「研修の受講」の観点から、セキュリティ専門家の要件を設定することとする。当該セキュリティ専門家による管理のもとで別に要員に確認等の作業を行わせる場合、当該作業の従事者(作業従事者)には制度が定める研修の受講を求める。
- 情報処理安全確保支援士、公認情報セキュリティ監査人、CISSP、CISM、CISA、ISO27001主任審査員をセキュリティ専門家の資格として設定する。

セキュリティ専門家及び作業従事者の要件

- セキュリティ専門家には力量の保持/維持と研修の受講に係る要件を課す。
- 当該セキュリティ専門家による管理の下、別の要員に作業を担わせる場合、当該作業従事者には制度が定める研修の受講を求める。

	役割	力量の保持/維持	研修の受講
セキュリティ専門家 *自らの監督の下で確認の実務を作業従事者に担わせることが可能	確認過程全般を統括し、確認を行った上で、自らの責任において確認結果に対する署名を行う。	- IT・セキュリティに関する高度な知見(ITSSレベル4以上又はそれに相当する力量)を保持していること - 上記に加え、力量を維持するために保持している知識を更新していること	制度が定める研修を受講していること。
(セキュリティ専門家が実際の作業を作業者に担わせる場合) 作業従事者	セキュリティ専門家の監督下で、確認を行う。	(不要)	同上

！ セキュリティ専門家の力量の保持/維持要件を満たす資格

項目	力量の保持	力量の維持
情報処理安全確保支援士	ITSSレベル4に位置づけられる	年次でオンライン講習を受けるとともに、3年間のうち1回実践講習を受ける。
公認情報セキュリティ監査人 ※公認情報セキュリティ主任監査人を含む。	ITSSレベル4に相当する力量を有すると考えられる	監査業務等を通じて更新に必要な資格維持ポイントを取得する。
CISSP		講習受講、業務経験、書籍通読等を通じて更新に必要なCPEポイントを取得する。
CISM		
CISA		
ISO27001 主任審査員		- 審査実績の提出 15hの継続的専門能力開発(CPD)実績の提出

！ セキュリティ専門家及び作業従事者を対象とした研修

目的	本制度に関する概要や専門家業務を行うにあたっての注意事項を理解することで、円滑に助言・確認できるようになる。
研修項目	- 本制度に関する知見 - 専門家業務を行うに当たっての注意事項 等

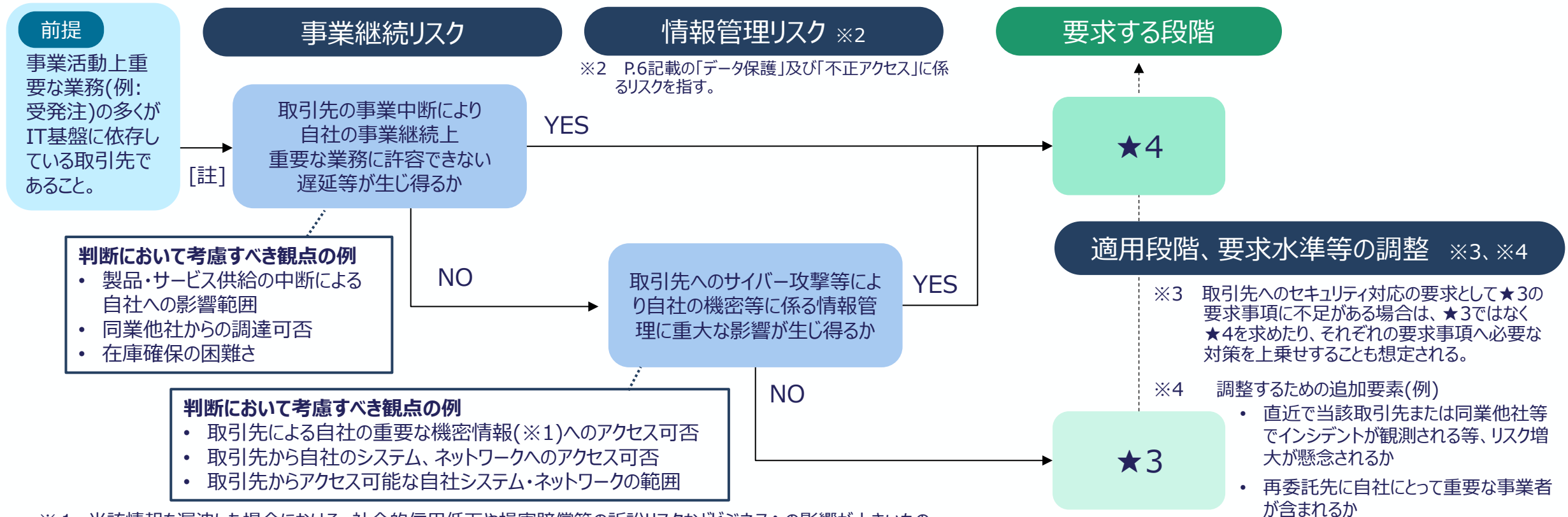
※ セキュリティ専門家に対して研修を実施する研修事業者の要件は、事業者の「実施体制」及び「研修コンテンツ」の観点で設定することとし、上記研修内容を含め、研修事業者募集までの間に具体化を図る予定。

(参考) 制度において設ける段階 ★3・★4適用の考え方(例)

- 取引先への適用に当たっては、例えば以下のように、取引先を★4又は★3の段階に割り当てたり、必要に応じて適用段階、要求水準等を調整することが考えられる。

(※)★5適用の考え方については、対策基準や評価スキームの具体的なあり方等と同様、令和8年度以降に具体化を進める予定。

■ ★3・★4適用の考え方(例)



※1 当該情報を漏洩した場合における、社会的信用低下や損害賠償等の訴訟リスクなどビジネスへの影響が大きいもの

[註] 単発・一過性の調達や、市販品など市場で容易に代替可能な製品・サービスの調達等のうち、重要度が相対的に高いとは言えないものについては、本フローの対象から外すことも考えられる。

リスクベースアプローチとSCS評価制度の違い

リスクベース



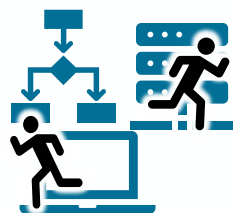
①リスク分析

保有する情報、対策状況、脅威等からリスクを分析



②リスク対応計画策定

分析の結果をふまえ、対策の洗い出しと優先順位付け



③対策実施

優先順位付けに基づき、対策を順次実施



④実施状況確認

実施状況を確認し、必要に応じ是正

各企業が実施する範囲

○ メリット

1. 自社の事情に即し、優先度をつけて対策できる
2. 過不足無く、投資対効果を高めやすい
3. リスクに応じた高度な対策を選択しやすい

× デメリット

1. オーダーメイドであり相当の専門性、工数、期間が必要
2. 個社最適になりやすく、発注者の要求水準と合致しづらい
3. リスクを低く見積もるインセンティブが働きやすい

SCS評価制度（ベースライン）



①横断的リスク分析

サプライチェーン企業の一般的なセキュリティリスクから共通的な対策水準を導出



②共通の基準策定

サプライチェーン企業で共通的に求められる対策の水準(★3・4)を策定



③共助/公助を伴った対策実施

★3・4の基準に達するよう、共助/公助を上手に活用しつつ対策を実施



④★取得

専門家の確認又は評価機関による評価を経て、★を取得

制度として実施済の範囲

各企業が実施する範囲

○ メリット

1. 対策完了までのスピードが速く、高い専門性も不要
2. 対策状況にバラツキが無くなる
3. 「共通のものさし」により対策が明確になり、サプライチェーン全体の底上げにつながる

× デメリット

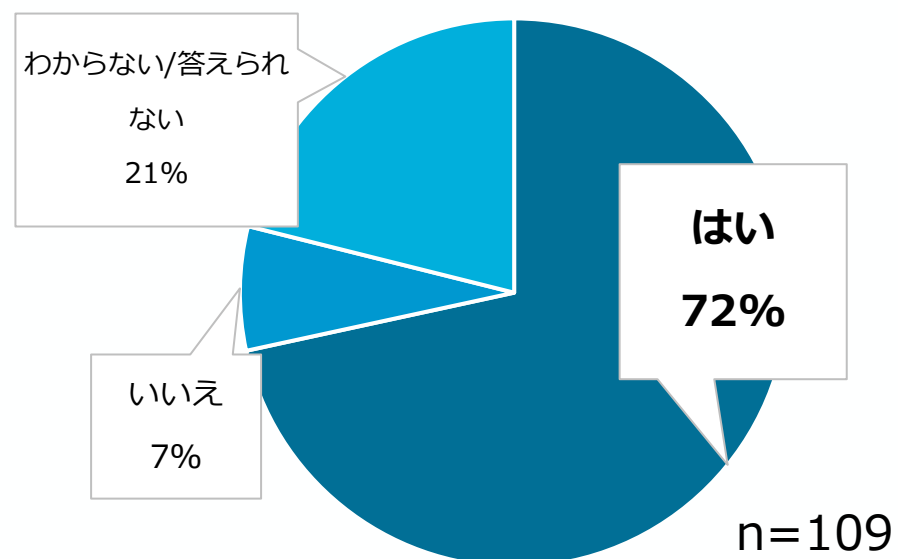
1. 個社ごとの特性や高リスク領域への対応には限界がある
2. 基準適合が目的化すると、実際のリスクに応じた対策が不十分となるおそれ

※ いずれの方式にも得手/不得手があり、企業の状況や目的に応じ、適切に使い分けことが重要

(参考) SCS評価制度の活用意向 (民間調査結果)

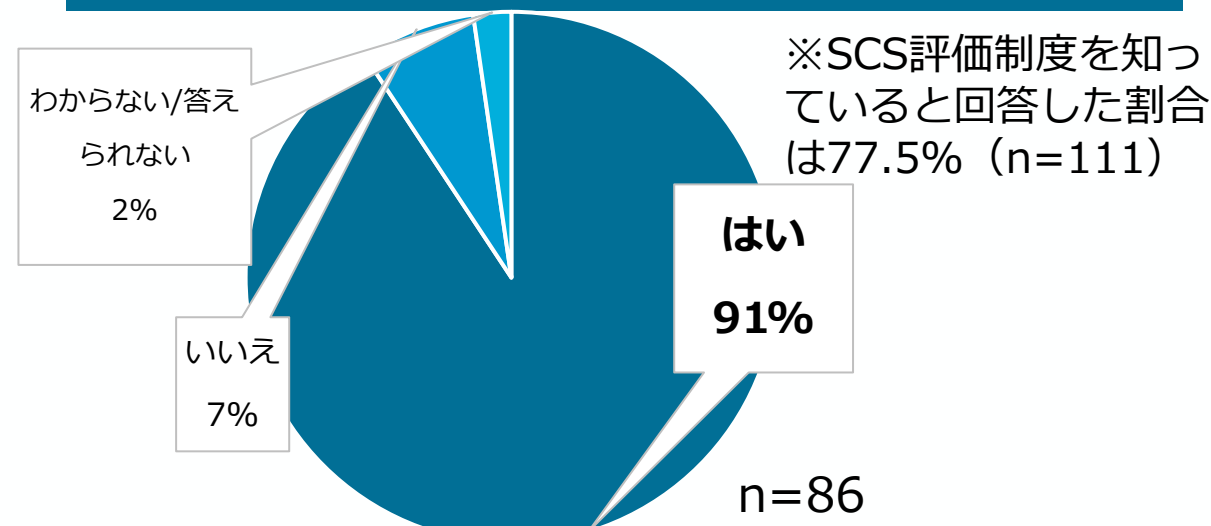
- 7割以上の発注者が、SCS評価制度の★取得を取引条件に組み込む意向
- 9割以上のサプライヤーが、SCS評価制度の★取得に向けた準備を推進

＜発注者側への質問＞あなたは、SCS評価制度の★評価を、取引先への取引条件に組み込む意向がありますか。



※従業員1,000名以上の企業のサプライチェーン管理・調達・セキュリティ推進担当者が調査対象

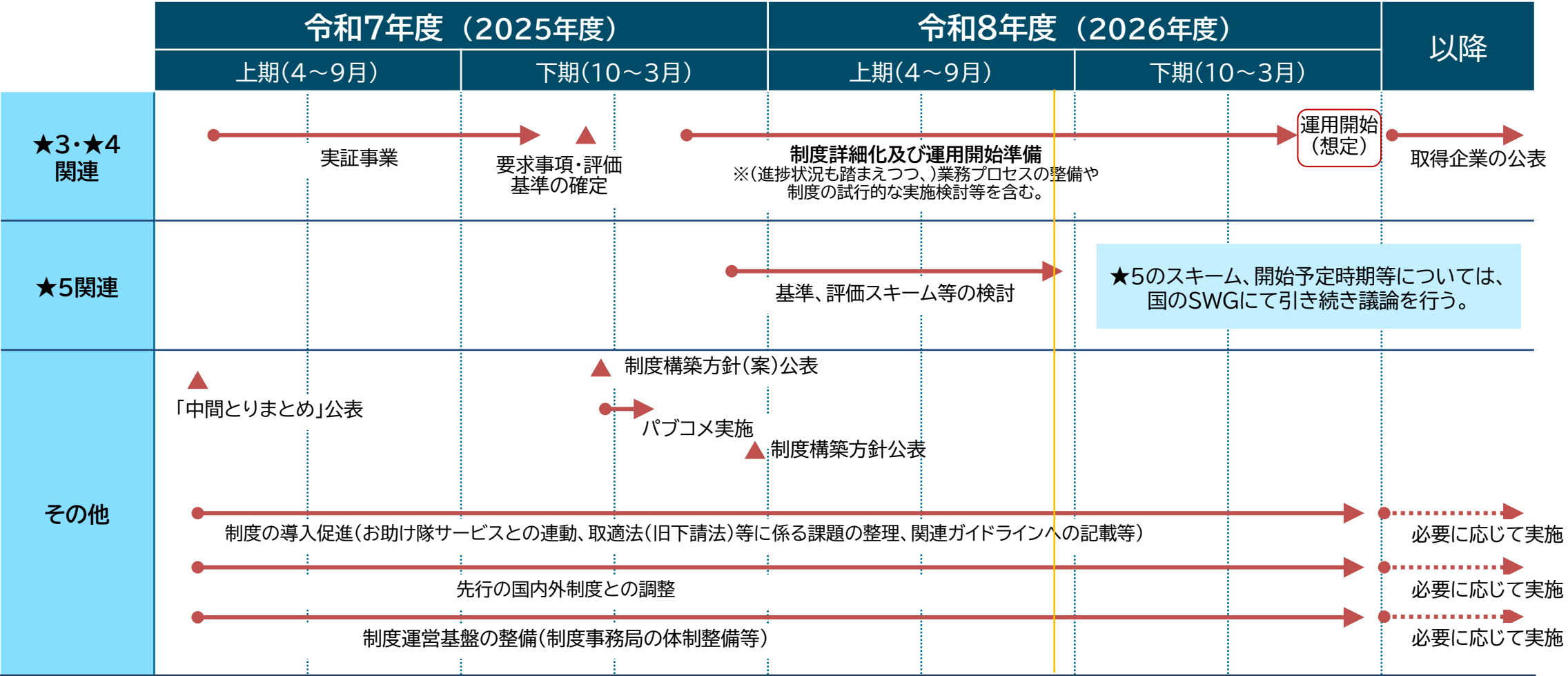
＜サプライヤー側への質問＞（SCS評価制度を知っていると回答した企業に対して）あなたの会社では、★3又は★4取得に向けた準備を進めていますか。



※SCS評価制度を知っていると回答した割合は77.5% (n=111)
※製造業・物流業に勤める従業員300～1,000名規模の企業のセキュリティ担当者が調査対象

今後のスケジュール

- 令和8年度末頃の制度開始を目指し、制度運営基盤の整備や利用促進等を進めていく。



SCS評価制度を中心とした中小企業支援策の新たな体系

- サプライチェーンに属する中小企業等が必要なサイバーセキュリティ対策(SCS評価制度★3～4水準)を
取得するための施策を総動員し、相互に連関/展開させる

①

★3～4実装のための
人的支援
(登録セキスペとのマッチング)

②

★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
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	専門家確認付き自己評価	第三者評価

③

★3～4を取得負担を軽減する
“お助け隊サービス”(新類型)の創設

④

★3～4取得につながる
実践方策+
規程類ひな形

⑤

サイバー対策要請時の、
関係法令の適用関係明確化

⑥

支援機関等と連携した
面的な普及展開活動

【地域SECURITY】

地域SECURITYのコンセプト

地域SECURITYがない状態 → 地域SECURITY形成 → コラボレーション・プラットフォームを全国に展開

(参考) 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26,453人**（令和8年4月1日時点）。
- 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。

※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）、サプライチェーン評価制度での活用等を推進



「中小企業向けサイバーセキュリティ対策支援者リスト」の活用

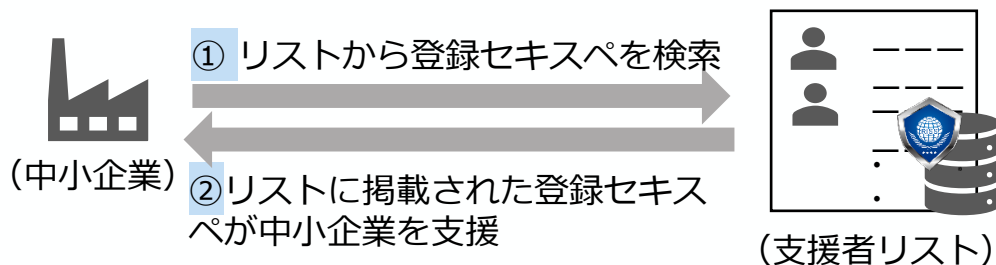
- 社内のセキュリティ人材育成に課題を抱える中小企業にとって、セキュリティ対策にあたって**外部のセキュリティ専門家の活用**が効果的。
- 商工会等の支援機関や中小企業が、外部専門人材として登録セキスペを効率的に探索することができるよう、**中小企業向けのサイバーセキュリティ対策支援が実施できる登録セキスペをリスト化した「中小企業向けサイバーセキュリティ対策支援者リスト」を作成し、IPAのホームページで公開。**

リストの使い方

中小企業自身による活用と支援機関を通じた活用の2通りを想定。

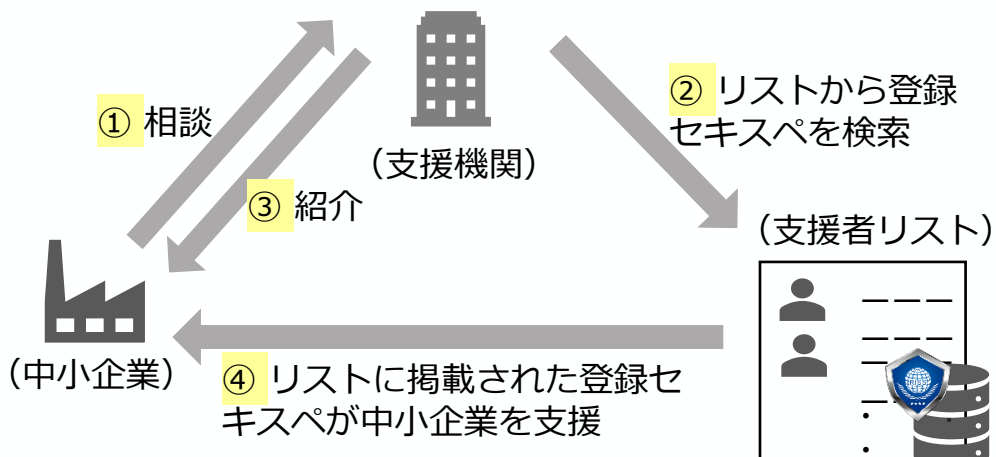
1. 中小企業自身によるリスト活用

中小企業自らがリストから登録セキスペを検索し、リストに掲載されている登録セキスペへ直接相談・業務依頼を行う。



2. 支援機関等を通じたリスト活用

中小企業からサイバーセキュリティ対策に関する相談を受けた支援機関等が、リストから登録セキスペを検索し、中小企業へ紹介する。



リストを活用するメリット

中小企業のメリット

- ✓ リストの中から外部のセキュリティ専門家を探すことができるため、相談先の選定にかかる負担を大幅に減らせる。
- ✓ 登録セキスペから、自社の状況に合わせた※具体的な支援を受けられるため、効果的なセキュリティ対策を進めやすくなる。

支援機関等のメリット

- ✓ 中小企業へ外部のセキュリティ専門家を紹介する際、リストから適切な※専門家を迅速に検索できるため、相談先選定にかかる手間と負担を軽減できる。

※受けられる支援のテーマ

- 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

*「セキュリティアセスメント」を追加予定

(参考) 中小企業向けサイバーセキュリティ対策支援者リスト

- 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、各登録セキスぺの個票（HTML形式）表示を実現。



登録セキスぺ活用ページ

マネジメント指導テーマ（5テーマ）

マネジメント指導業務の達成目標と成果物

【達成目標1】実践における自社の情報セキュリティの強化
【達成目標2】実践における自社の情報セキュリティの強化
【達成目標3】実践における自社の情報セキュリティの強化

注：達成目標1～3は、実践における自社の情報セキュリティの強化を目的としたものである。

セキュリティ専門家リスト

指導事例集（ベストプラクティス）

【簡易検索】
・支援対象地域別（10地域）
・得意業種別（8業種）

専門家個票

【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					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	緊急対応	製品選定・導入		
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	可	可	可	20,000円以上～30,000円未満		可	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					2件/10年	関東、甲信越、静岡県	金融業/医療/教育	可	可	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

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	〇〇〇株式会社
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 可 1年以上の長期支援(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(補正事項) 有
支援可能な形態	訪問によるコンサルティング 可 オンラインコンサルティング 可 講演・研修 可 インシデント発生時の緊急対応支援 可 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 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、検知後の運用指定		[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	

「サイバーセキュリティお助け隊サービス」(新類型)

- SCS評価制度の★3～4の取得支援を目的とし、令和8年度中
- 対策項目のうち**未達成の項目について、お助け隊サービス(新たな類型)の導入により達成させる**
- STEP1として、SCS評価制度の★取得及び更新時に中小企業の対策状況を評価することをサービスに含める
- STEP2として、SCS評価制度のITツール導入や人的支援により達成できる対策項目について、それぞれ「ITツールによる支援」のほか「ITツール以外の支援」を組み合わせ提供

お助け隊サービス(新類型)のイメージ

STEP1:課題の可視化

- ✓ SCS評価制度の要件項目毎に中小企業の対策状況を診断
- ✓ SCS評価制度の更新時に、各対策項目の対策状況を評価

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

STEP3:★取得

- ✓ SCS評価制度の★3／★4の項目要件をすべて充足することで★を取得

STEP1・STEP2の支援サービスを一定の価格要件の下で提供



「サイバーセキュリティお助け隊サービス」(新類型)実証事業概要

- 全国約十数社のITベンダが、**中小企業に無償でサービスを提供**、技術/価格要件を検証（R8年度中に開始予定）
- 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

中小企業のメリット

- 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(★取得要請への備えが可能)
- 3 サプライチェーンセキュリティ対策に取り組む企業として、**信頼性向上**に繋がる



検証項目 (ITベンダ向け)

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(提供内容・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

(参考)「サイバーセキュリティお助け隊サービス」既存類型との違い

既存類型 セキュリティに不安な中小企業へ、**最低限必要な対策**を安価に提供

(9,200件の導入実績<R7.12時点>)



見守り



駆付け



保険

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可視化し、項目達成まで伴走支援

STEP1
課題の
可視化

STEP2
対応実施

SCS評価制度の★取得

実証事業サービス提供事業者一覧

現時点版
(9/18)

地域カバー範囲（※変更となる可能性があります。）

事業者名	北海道	東北	関東	中部	近畿	中国	四国	九州	沖縄
株式会社NTTデータ									
大阪商工会議所									
三井物産セキュアディレクション株式会社									
株式会社アクシス									
富士フイルムビジネスイノベーション ジャパン株式会社									
NTTドコモビジネス株式会社									
株式会社オプティム									
株式会社NTT Risk Manager									
株式会社セキュアイノベーション									
ちばぎんコンピューターサービス株式会社									
株式会社イシマル									
GMOサイバーセキュリティbyイエラエ 株式会社									
SOMPOリスクマネジメント株式会社									
リコージャパン株式会社									
株式会社フォーバル									

出典：情報処理推進機構（IPA）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HPより作成：
<https://www.ipa.go.jp/security/sme/otasuke-scs.html>

実証スケジュール



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実施。

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

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

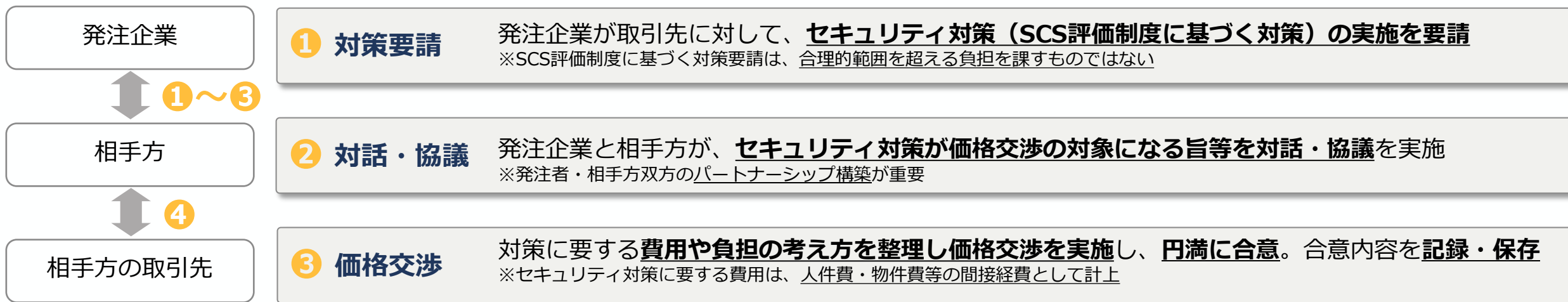
- ✓ **規程類のサンプル・ひな型についてSCS評価制度に対応する形で拡充。**
- ✓ 実践的方策ガイドについて、ガイドライン改訂案を踏まえ企業へのヒアリングを実施し、**取組事例の収録や分かりやすい表現を用いることで、中小企業が活用しやすい形で整理し、付録「中小企業のためのセキュリティ人材確保・育成の実践ガイドブック」として整理。**

サプライチェーン全体のサイバーセキュリティ向上に向けた取引先とのパートナーシップ構築

○2025年12月26日に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。

サプライチェーンにおけるパートナーシップ構築のイメージ



※ **4** 発注者から**要請がない場合でも**、受注側から価格交渉を申し入れることが可能
困った場合は、支援機関や相談窓口（取引かけこみ寺や公正取引委員会の相談窓口等）を活用できる

Point



セキュリティ対策に関する費用は**価格交渉の対象となり得る**



パートナーシップに基づき対話・協議を行うことが重要



対策による**人件費・物件費含め、双方で十分協議**し合意する



要請が無い場合でも価格交渉を申し入れることが可能

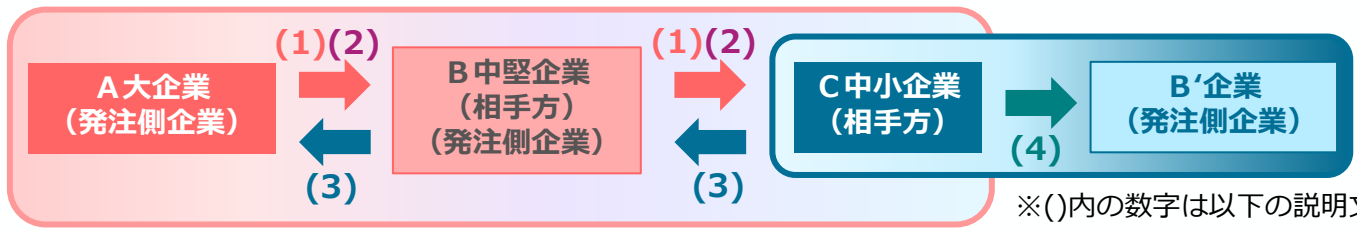
(参考) サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップ構築促進に向けた想定事例及び解説 (概要)

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. DXの進展は、経営の効率化・スピード化をもたらしたが、
「サイバー攻撃のうま味」も増加させた
2. まさにDXが進みつつある中小企業が狙われており、取引先に影響が及ぶ
→ サプライチェーンの危機
3. 経済産業省では、SCS評価制度を構築して対応
また、中小企業を中心に、様々な支援施策も構築中
(例:「サイバーセキュリティお助け隊サービス(新類型)」で簡便に★取得が可能)



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>

最新情報は↓で検索！

METI SCS評価制度

検索

