サイバーセキュリティお助け隊サービスの新たな類型の創設に向けた検討について

1. **サプライチェーン強化に向けたセキュリティ対策評価制度について**
2. 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について
3. 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のための実証事業について
4. (参考)中小企業のサイバーセキュリティ対策の実態

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を提示しつつ、その状況を可視化する仕組みを構築。※2
- **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
- 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] 企業等のIT基盤が対象。また、評価は取得又は更新の時点において定められた水準を満たしているかを示すものであり、完全なセキュリティの確保等を保証するものではない。
[※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。

構築する評価制度

	★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
要求事項	26件	43件	（今後検討）
有効期間	1年	3年（毎年自己評価を実施し結果を評価機関へ提出）	
評価スキーム	**専門家確認付き自己評価** ※4	**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。

[※4] 専門家：登録セキスペ、CISSP等の資格を有し、かつ制度が定める研修を受講したセキュリティ専門家
[※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

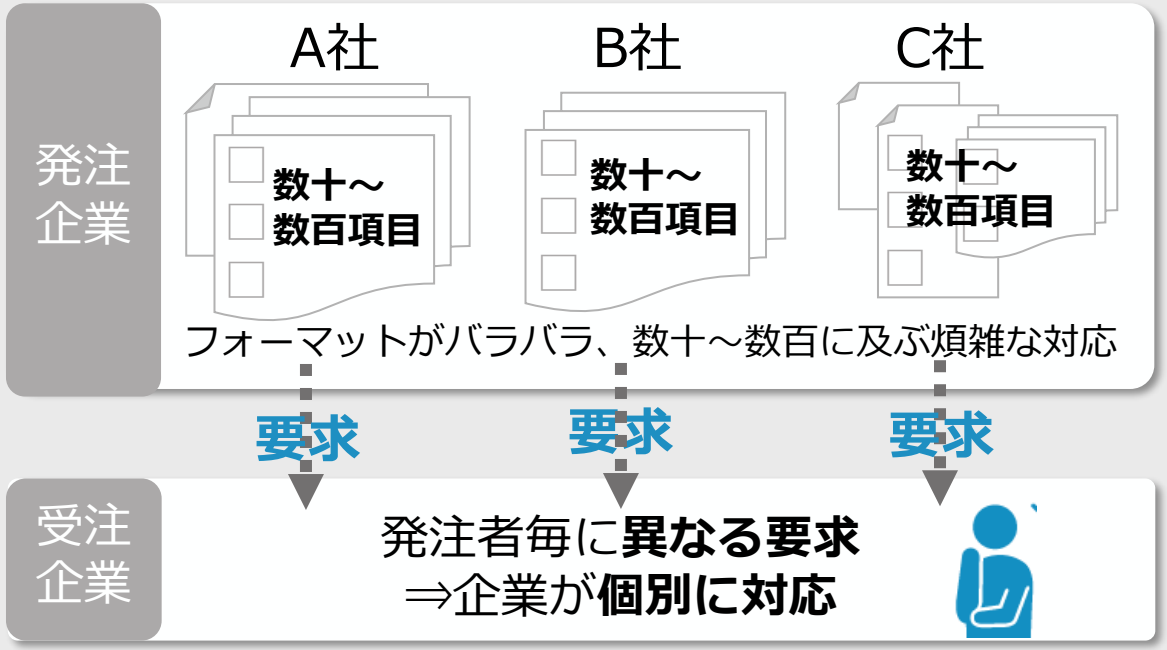
普及施策の例

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
施策の概要	**サイバーセキュリティお助け隊サービス（新類型）の創設** ★3・★4取得を目的とした、サイバーセキュリティお助け隊サービス（新類型）を創設し、安価な”★”取得を実現	**中小企業ガイドライン整備** 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	**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」の整備により、中小企業と専門家とのマッチングを促進	**取引先への要請等に係る考え方の整理** 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により、費用に係る円満な価格交渉を促進

中小企業にとって★を取得するメリット

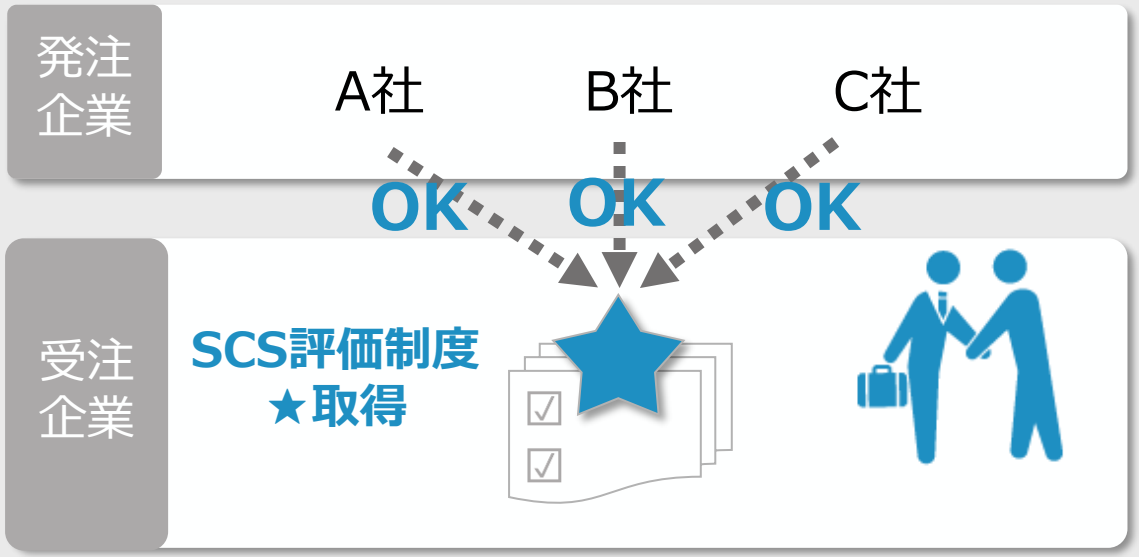
発注者ごとに異なる要求…対応が煩雑で非効率

- ✓ 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

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

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

※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8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

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

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

SECURITY ACTION

一つ星・二つ星

	★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
要求事項 有効期間	26件 1年	43件 3年（毎年自己評価を実施し結果を評価機関へ提出）
評価スキーム	専門家確認付き自己評価 ※4	第三者評価

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)

（参考）導入促進策の全体像

- ★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		

1. サプライチェーン強化に向けたセキュリティ対策評価制度について
2. **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について**
3. 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のための実証事業について
4. (参考)中小企業のサイバーセキュリティ対策の実態

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評価制度開始にあわせて、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**項目要件をすべて充足することで★を取得**

1. サプライチェーン強化に向けたセキュリティ対策評価制度について
2. 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について
3. **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のための実証事業について**
4. (参考)中小企業のサイバーセキュリティ対策の実態

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

- 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無償で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12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

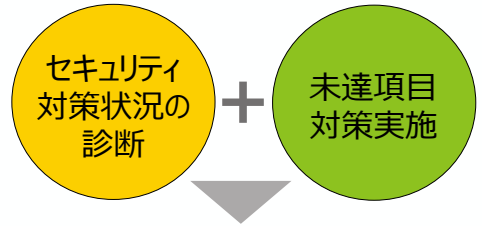
1. **組織的対策を含むセキュリティ対策を無料**で実施（実証期間中最大1年程度）
2. SCS評価制度開始後の**★取得要請への備え**が可能
3. サプライチェーン対策に取り組む企業として、**取引先との信頼性向上**に繋がる

（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12月時点で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

実証事業の目的

中小企業が★取得するために必要となる機器・サービス内容・品質水準・価格の検証

SCS評価制度の品質を維持しつつ数多くの中小企業に提供できるサービスとするために、
・★取得のために必要なITツールは何か
・どの業務にどの程度の人的・物的コストがかかるか
などを検証する

サービス提供事業者にとって採算が取れるサービス設計

中小企業が継続利用できる価格としつつ、サービス提供事業者にとってビジネスとなるサービス設計となることを目指す（※）

（※）以下を検証し、サービス提供事業社にとって継続的なサービス設計を目指す
- ✓ 人的支援を不要とするサービス範囲の検討（例：オンライン支援（ウェブ会議）の導入、FAQやチャットボットの活用、教育にｅ-ラーニングを導入など）
- ✓ SCS評価制度の達成状況により導入・運用コストが変動するため、実証を通じて実際にかかったコスト感を調査
- ✓ 多くの中小企業が導入する場合、ITツール活用によるコスト削減の検証

実証事業参加のメリット

組織的対策を含むセキュリティ対策を無料※で実施

・SCS評価制度の★取得に必要なセキュリティサービスを国の支援※で受けられる
・インシデント体制整備などの組織的対策の支援も受けられる
・サイバー攻撃のリスクを低減できる

SCS評価制度の★取得の支援が受けられる

実証に参加することによって、SCS評価制度の★取得に向けた支援を受けられ、発注者企業の要求に対応できる

SCS評価制度は発注者企業からの期待が高く、施行後は★取得を要求されることが想定される

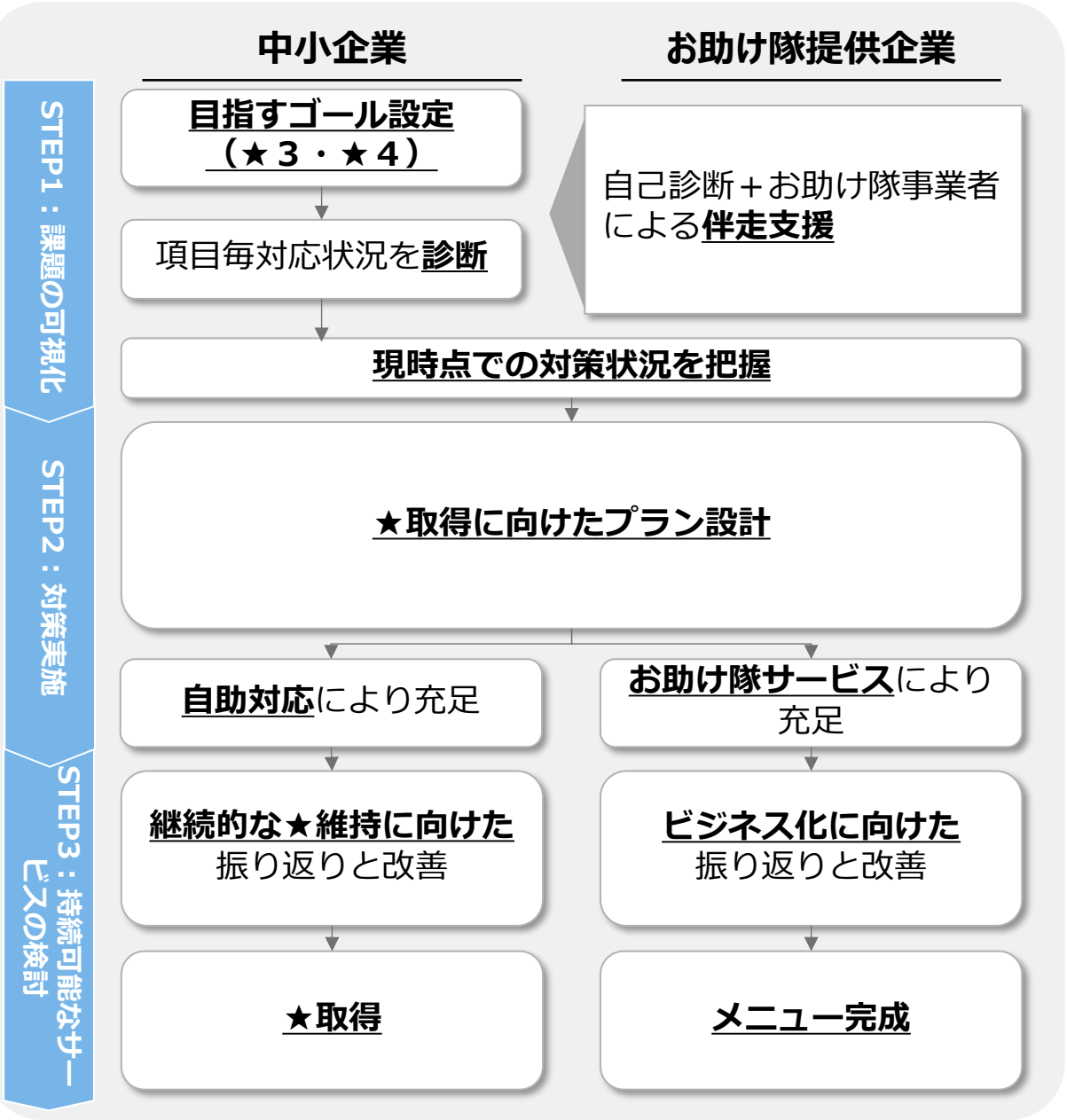
取引先との信頼性向上につながる

SCS評価制度の★を取得している企業は、サプライチェーン対策が進んでいる企業として信頼されやすく、新たな取引や継続的な取引につながる

※　SCS評価制度の対策の範囲で、実証期間中（最大で１年程度）に限ります

サイバーセキュリティお助け隊サービス（新類型）

実証プロセス



STEP1：課題の可視化

- ✓ **目指すゴール**（★３取得、★４取得、取得済の★の継続、★３から★４へステップアップ）を設定
- ✓ 項目の[充足/未充足]状況を**1項目ずつ確認**
- ✓ セキュリティ対策における**課題を可視化**

STEP2：対策実施

- ✓ 未充足項目に対して、自助対応とお助け隊サービスの役割を整理し、**中小企業向けプランを設計**
- ✓ **予算額に応じて優先度を付け、機器導入の要否を判断**
- ✓ セキュリティポリシー整備、インシデント手順書作成、セキュリティ教育など**非機器対応も含め総合的に検討**

STEP3：持続可能なサービスの検討

中小企業
提供企業

- ✓ **次年度更新に向け**、自助対応可能な項目を増やし、ステップアップを検討
- ✓ 負荷が高い場合、対応策を再検討し**メニューを最適化**

中小企業
提供企業

- ✓ SCS評価制度の★３もしくは★４の**項目要件をすべて充足することで★を取得**
- ✓ 実証を通して、**お助け隊サービス（新類型）のメニュー完成**

実証ゴール

提供事業者向け

- SCS評価制度★3、4を取得するためのルート（ツールの対応or手順による対応、ツールの指定など）は制限しないため、実証で様々なパターンを実施し、**お助け隊サービス提供事業者ごとに実証を通じてメニューを完成**させる。
- 実証を通じて、**お助け隊サービスの提供基準を完成**させる。

お助け隊提供企業毎に支援メニュー完成

例）A社のお助け隊サービスメニュー

SCS評価制度★3（★４）の要求No.

No	中小企業規模	
	大（N人以上）	小
1		
…	IT資産管理ツールによる管理	Excelによる管理
…	自社の教育コンテンツ（動画）による学習を利用	
…	UTM導入による対応	手順書による対応

✓ SCS評価制度★3（★４）の要求No.ごとに、中小企業の規模に応じて、どのような手段で要求を満たすかを項目別に設定し、お助け隊メニューを完成させる

お助け隊サービス（新類型）の提供基準完成

お助け隊サービス（新類型）の提供基準案

事業者	サービス名
目的（★３取得を目指すor★４取得を目指すor★維持等）	価格（初期費用・月額費用）XX円～XXX円
対象地域	導入可能機器（UTM、IT資産ツール等）
パートナー有無	提供実績（実証の数含む）
中小企業でも導入・運用できる簡単さ	・・・

✓ お助け隊提供企業毎のメニューをヒアリングし、お助け隊サービス(新類型)の提供基準（提供事業者の認定基準）に盛り込む基準を設定

実証でやりたいこと

必要な支援レベルの検証

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）は、機器導入では充足とならない項目もあるため、お助け隊サービスとして必要な支援レベルを検証します。

サービス内容の検証

お助け隊サービスを利用する全ての企業が、SCS評価制度の★を取得できるサービス内容であるかどうかを検証します。

幅広い業種への対応を検証

SCS評価制度は、特定業種に限定されないため、幅広い業種（※1）に対応可能かを検証します。

（※1）製造業のほか、情報通信業、金融業、運送業、サービス業、医療業界など

お願い事項

- ✓ 実証後に無理なく導入できたかのアンケートや実証期間中にサービスを利用するにあたって検知した情報の提供（※2）にご協力ください。
- ✓ SCS評価制度で取得した★を持続いただくため、実証後もお助け隊サービスの利用を継続いただけると幸いです。

（※2）シグネチャや通信情報などを含む場合があります。

実証参加要件

以下は実証参加要件の一部のご紹介となります

提供事業者向け

セキュリティ人材の配置

✓ 社内には、**セキュリティ人材**（登録セキスペ等）**が配置**されていること。

責任の所在の明確化

✓ 機器提供、診断、人的支援を異なる企業が担当する場合でも、**サービス提供の責任はサービス提供主体が負う**こと

サービス提供の継続

✓ **実証事業終了後**も、**サービス提供を継続できる**体制であること

相談窓口の設置

✓ 中小企業・小規模事業者向けに、サービス内容や申込方法、技術的な問合せを含む、**サービス全般の相談窓口が設置**されていること

ITツールの機能説明

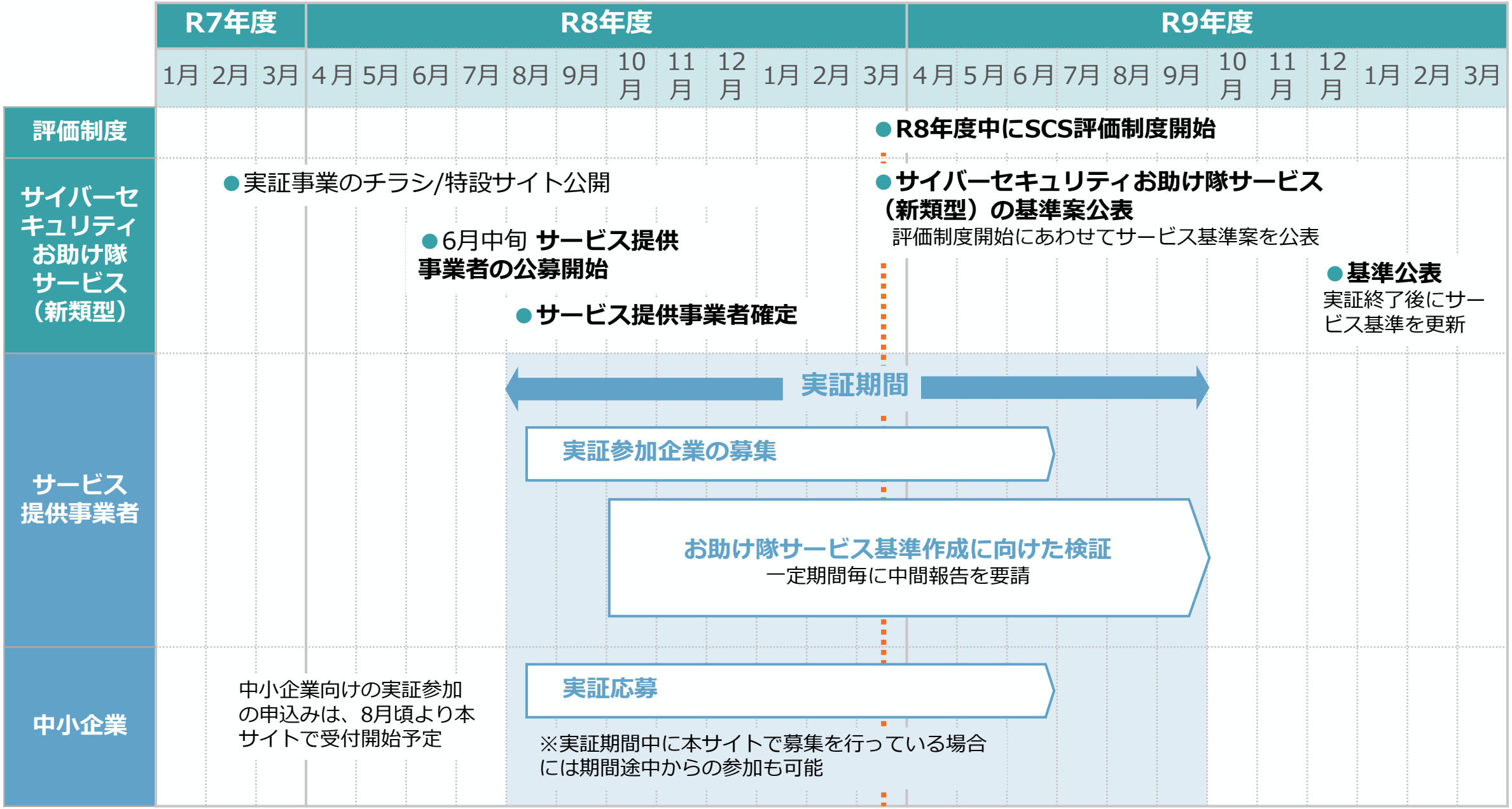
✓ 要件対応にITツールを使用する場合、**提案時に具体的なツール名、機能、対応可能な要件を明示**すること

レポートの提出・情報提供への協力

✓ 制度検討のための**検討会への参加、導入状況**（シグネチャ・通信情報等含む）の**提出**、サービス化に関する**レポート提出**などに協力できること

サイバーセキュリティお助け隊サービス（新類型）

実証スケジュール



1. サプライチェーン強化に向けたセキュリティ対策評価制度について
2. 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について
3. 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のための実証事業について
4. **(参考)中小企業のサイバーセキュリティ対策の実態**

（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

初選出

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

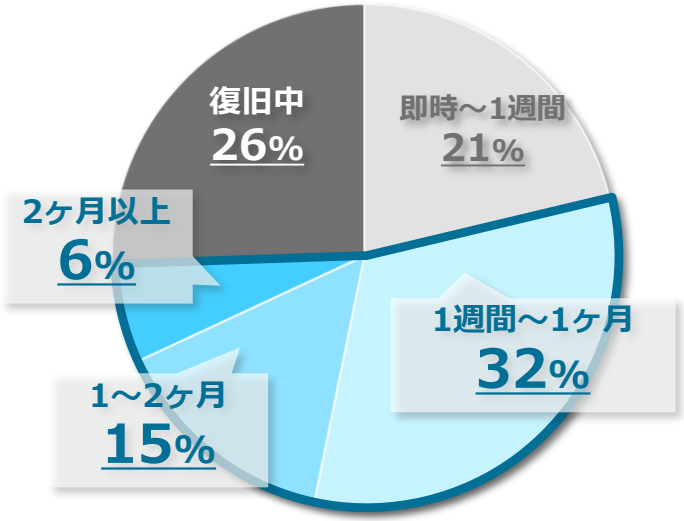
（出典）独立行政法人情報処理推進機構（IPA）「情報セキュリティ10大脅威2026」、
警察庁「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について（令和７年９月）」を基に作成。

サイバー攻撃の現状と中小企業への攻撃

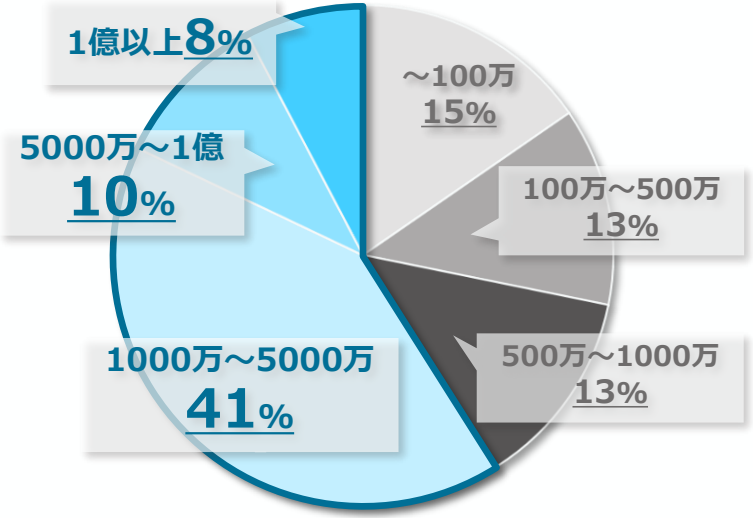
- ランサムウェアの被害として、復旧に要する時間や復旧費用が高額化しており、実際に、**１か月以上を要するケースや数千万円規模の被害が生じるケースが５割を超えている。**
- ランサムウェア被害の**６割以上が中小企業**とされているところ、**中小企業が狙われる状況**は**過去最多**となっている。 中小企業においてもランサムウェアに対する備えが必要。

ランサムウエア被害（復旧に要した時間、調査費用総額）

【復旧に要した時間】

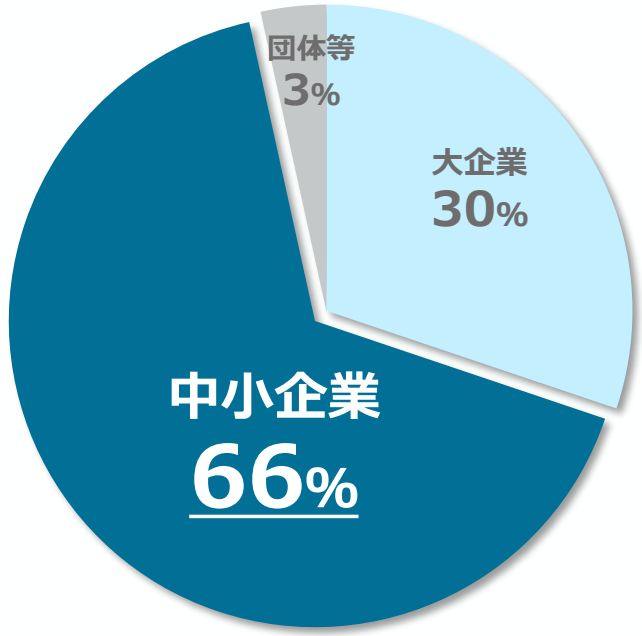


【調査費用総額】



➡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%**(令和6年から9ポイント増加)

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
(令和６年から３ポイント増加)

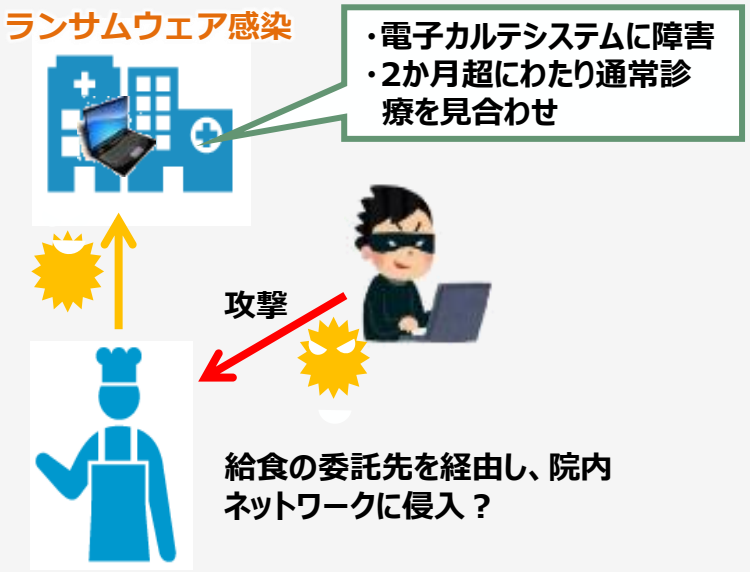
出典：警察庁「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について（令和７年９月）」を基に経済産業省作成

顧客・取引先にも影響が及ぶ

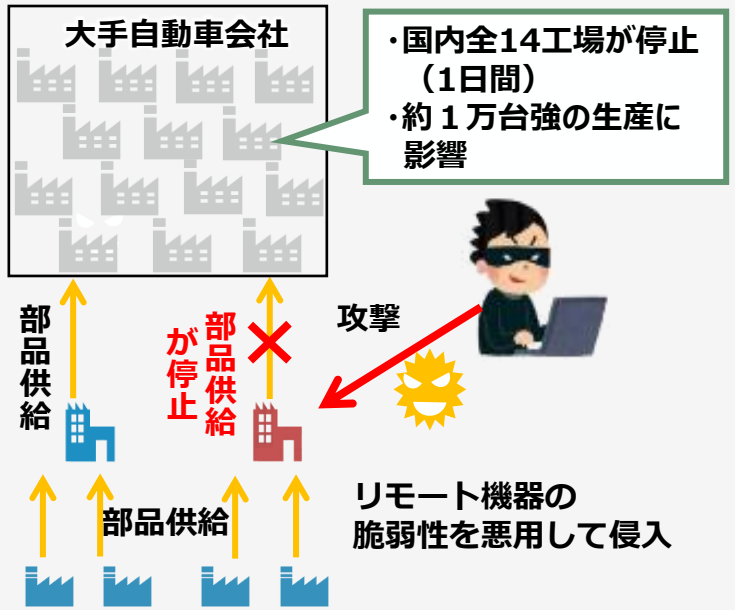
- 攻撃者は、**防御レベルの低い組織**を狙う。サイバー被害は**自社だけの問題では済まない。**

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

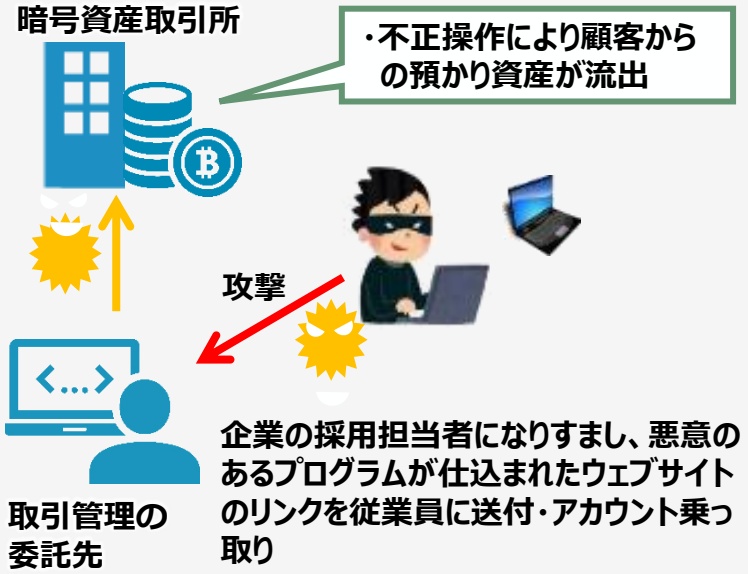
事例①：委託先の給食業者を通じた公立病院への侵入・通常診療見合せ



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

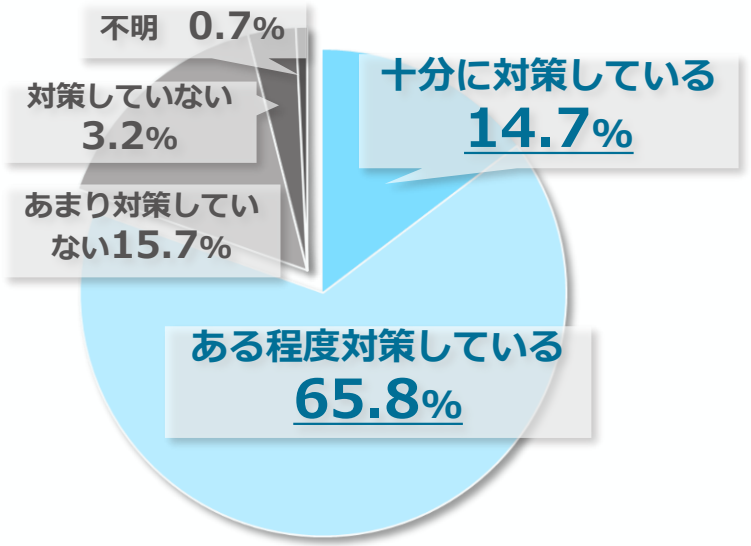
中小企業のサイバーセキュリティ対策状況と課題

【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。
- 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」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。**中小企業が組織的対策を実施できるための環境整備が必要**。

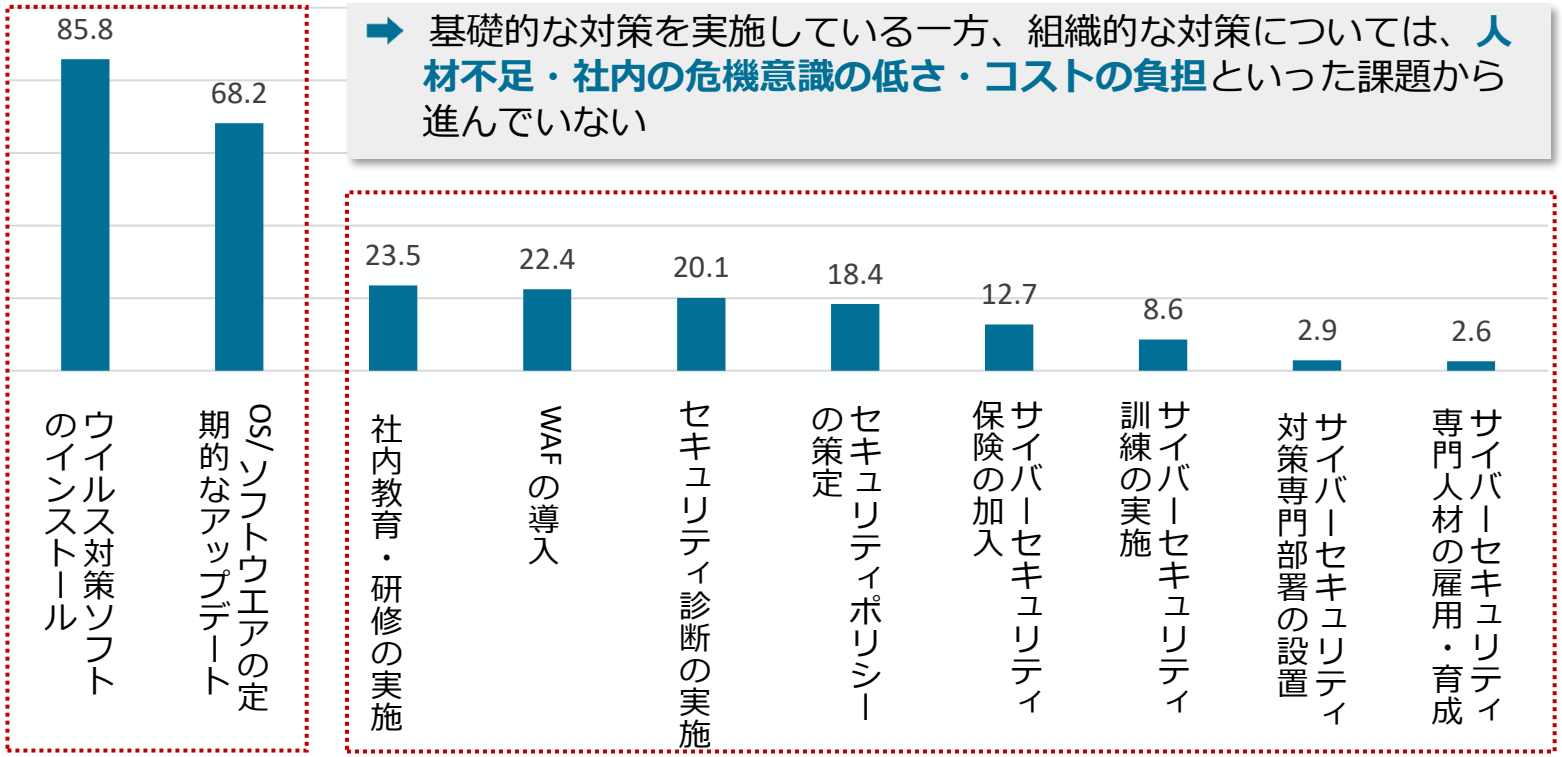
サイバーセキュリティ対策の状況

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

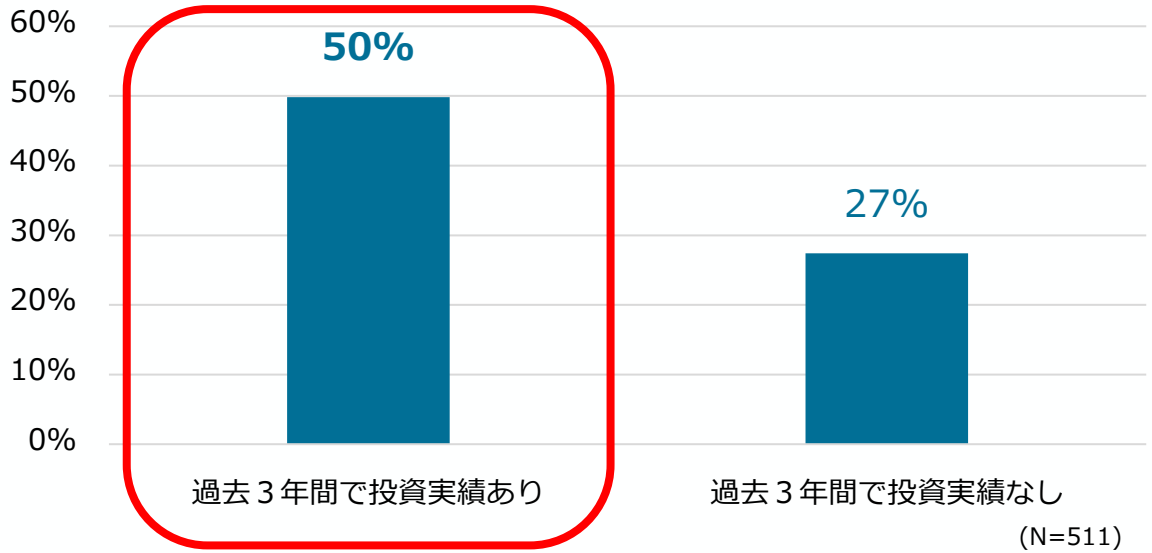
「中小企業のデジタルシフト・DX実態調査集計結果」（2025年1月10日） 中小企業のデジタルシフト・DX推進委員会（東京商工会議所ホームページ掲載資料に基づき、経済産業省において作成）

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

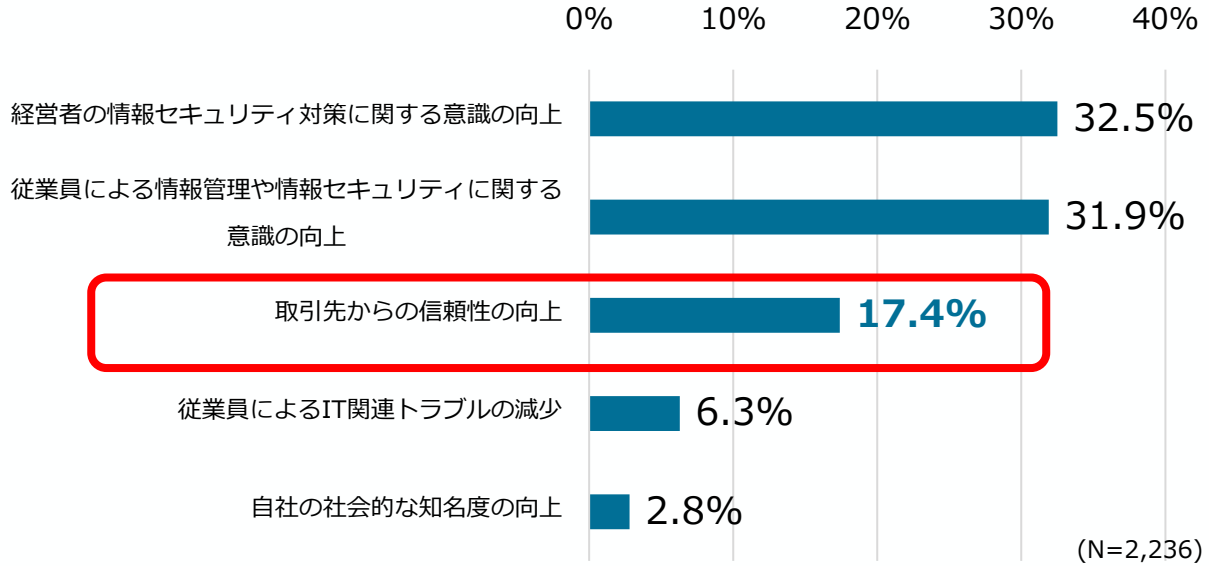


⇒サイバーセキュリティ対策投資を行っている中小企業等の方が、取引につながったと考える割合が高い。

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

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：独立行政法人情報処理推進機構「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

（参考）中小企業に有効なサイバーセキュリティ取組（実態調査結果）

- 業種問わず効果的なサイバーセキュリティ対策として、**①SECURITY ACTION 二つ星に掲げる対策項目を多く実施すること（→インシデント被害の低減が期待される）**、**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すること（→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。
- その上で、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）。
- 中小企業4,191社を対象に実施した「中小企業実態調査」の結果では、上記に係る**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**。「中小企業の情報セキュリティ対策ガイドライン」の実践例として参考にしていただきたい。

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、「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」**