

2026 年 9 月 30 日 全 7 頁

SCS 評価制度の「★」、問われるのは"取得"より"維持"

体制・人材・運用が、取引の信頼を左右する

イノベーション企画部 シニア IT リサーチャー 大橋 哲行

はじめに

「御社のセキュリティ対策は★（星）いくつですか」——取引先からそう問われる日が、やがて来るかもしれない。経済産業省および内閣官房国家サイバー統括室が整備を進める「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（以下、SCS 評価制度）」は、2026 年度末頃の制度開始を予定しており、企業のセキュリティ対策状況を「★」の数で段階的に「見える化」する仕組みである¹。

制度開始を控え、関心は急速に高まっている。取引先から対応を求められる可能性が指摘され、早期の取得を促す動きも出始めた。もっとも、本制度はあくまで任意であり、★の取得が制度上義務づけられるわけではない。あたかも制度が強制力を持つかのように装って取得を急がせる不適切な勧誘には、経済産業省も注意喚起を発している²。過度な不安も、「取ればよい」という短絡も、いずれも実態を見誤らせかねない。

そこで本稿は、まずこの過熱から一步引くところから始めたい。SCS 評価制度は、事業者を優劣で競わせる「格付け」ではなく、対策状況を共通の基準で可視化し、サプライチェーン全体の底上げを図る仕組みである。これを踏まえ、企業経営に携わる方々やセキュリティ戦略の立案・策定を担う方々に向けて、本稿では二つの問いを立てたい。すなわち、「★は取引の"参入資格"になるのか」、そして「★さえ取得すれば、それで安泰なのか」である。

結論を先取りすれば、★は今後、取引先を選定する際の確認項目として重みを増していく可能性が高い。しかし、より重要なのは第二の問いである。継続的な取引とセキュリティ水準の維持を左右するのは、★という評価結果そのものではなく、それを支える組織体制・人材・運用プロセスの整備にほかならない。

¹ 経済産業省 [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関する制度構築方針](#)

² 経済産業省 [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）に関する注意喚起](#)

SCS 評価制度の全体像

議論の前提として、制度の骨格を簡潔に確認しておく（制度の詳細は既刊レポートを参照されたい³）。

SCS 評価制度は、企業のセキュリティ対策状況を共通の基準で評価・可視化する仕組みである。共通の評価基準を用いることで、発注側は取引先の対策状況を確認しやすくなり、受注側も自社の取り組みを示しやすくなる。

具体的には、2 社間の取引契約等において、委託元が委託先に求める段階（★）を示し、その対策の実施を促すとともに、実施状況を確認することが想定されている。制度上の段階は★1 から★5 まだが想定されており、このうち SCS 評価制度で新たに整備されるのは★3・★4 である。その位置づけと評価方法は図表 1 のとおりである。

図表 1 SCS 評価制度における各評価レベルの概要

	★ 3	★ 4	★ 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	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など	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	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	サプライチェーン企業等がさらに目指すべき高度なセキュリティ対策
評価方法	専門家による確認付きの自己評価	第三者評価	
有効期間	1年	3年 (1年ごとに自己評価を実施)	検討中
運用開始時期	2026年度末頃		未定(2027年度以降)

(注) ★1・★2 は、IPA が 2017 年から実施している自己宣言制度「SECURITY ACTION」の二段階であり、SCS 評価制度で新たに整備されるのは★3・★4（★5 は今後検討）。なお、本稿の制度内容は 2026 年 9 月時点で公表されている情報に基づく。今後の制度具体化や運営基盤の整備状況等により、開始時期や評価方法などが変更される可能性がある。

(出所) 横平健「SCS 評価制度とは何か」(2026) (脚注 3) の図表 6 を引用

ここで着目すべきは、★3・★4 が「一度取得すれば終わり」ではない点である。図表 1 に示すとおり、いずれの段階にも有効期間が設けられ、定期的な再評価や自己評価の報告が想定されている。この事実こそが、本稿の後段で論じる「体制」の重要性に直結する。

³ 横平健 [SCS 評価制度とは何か](#) (大和総研レポート、2026 年 6 月 2 日)

★は"参入資格"になるのか？

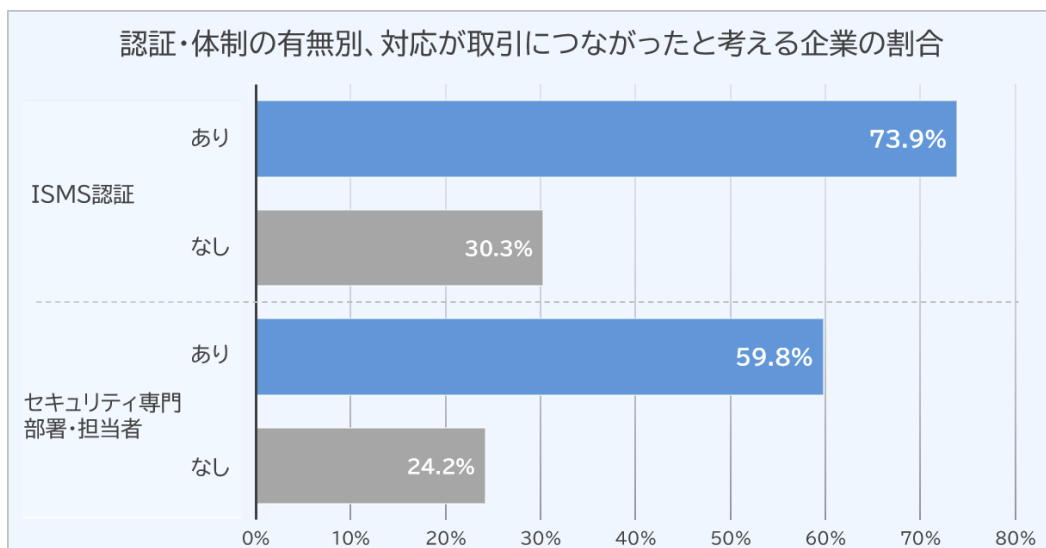
第一の問い、「★は取引の参入資格になるのか」から考えたい。

結論として、制度が普及すれば、★が取引先を選定する際の確認項目の一つとして活用される場面が増える可能性が高い。SCS 評価制度は、2 社間の取引契約等において、委託元が委託先に適切な段階（★）を提示し、実施状況を確認する運用を想定している。発注側が取引の開始や継続の条件として★を求める場面は、自然に増えていくと考えられる。かつてプライバシーマークや ISMS 認証が、多くの取引や入札の事実上の要件とされる場面が増えていった経緯を思い起こせば、★も同じ道をたどる可能性は十分にある。

ただし、ここで一点、留意しておきたいことがある。発注側にとって★は、取引相手を見極める際の「入口」にあたる。★は今後、参入に際して求められる条件の一つとなる可能性があるが、それだけで取引の継続が保証されるものではない。サイバーセキュリティの観点から発注側が最終的に信頼を寄せるのは、★の背後にある対策の実態であり、日々の運用の証跡であり、いざという時のインシデント対応力である。

これらの点は、企業を対象とした調査結果からもうかがえる。IPA が全国の中小企業を対象に実施した調査⁴は、取引に先立って発注元から情報セキュリティ対策——秘密保持契約や認証取得など——を求められた経験のある企業に対し、その対策を行ったことが取引につながった大きな要因だと思うかを尋ねている。回答割合は、認証の取得状況や体制の整備状況によって差が見られる（図表 2）。

図表 2 取引への効果の実感は、認証・体制の有無で差が見られる



（注）母数は、取引に先立ち発注元から情報セキュリティ対策の要請を受けた経験がある企業（n=511）。そのなかで、要請された対策への対応が取引の大きな要因になったと回答した割合を比較

（出所）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」（脚注 4）（図 5-21・図 5-34）をもとに大和総研作成

⁴ 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-報告書-](#)

ISMSを取得済みの企業では、対応が取引につながったと考える割合が73.9%に上るのに対し、未取得の企業では30.3%にとどまる。セキュリティの専門部署・担当者を置く企業（59.8%）と、置いていない（組織的な対応を行っていない）企業（24.2%）との間にも、同様の差が見られる。認証を取得している企業や体制を整えている企業では、セキュリティ対策が取引につながったと認識する割合が高い。

同調査も、第三者評価制度の取得を取引上のメリットがある対策と位置づけるとともに、セキュリティ体制の整備についても同じくメリットがあると結論づけている。企業間取引の中で自社の信頼を示す企業にとって、★の取得とそれを支える体制の双方が意味を持つのである。

★は今後、取引相手を判断する「入口」としての重みを増していく可能性は高い。しかし、その先で問われるのは、★を支える対策の実態である。

なぜ「取って終わり」にできないのか——制度が求める"継続運用"

ここで第二の問い、「★さえ取得すれば安泰なのか」に移る。

取得して終わり、と考えたくなるかもしれない。だが、制度設計の観点からも、そうとはい切れない。先に触れたとおり、SCS 評価制度の★3・★4には有効期間が設けられ、定期的な再評価や自己評価の報告が求められる。★は一度揭げれば恒久的に有効な看板ではなく、対策を継続していることを定期的に示すことで、初めて維持できるものである。

SCS 評価制度が問うのは、評価を受ける際に一時的に体裁を整える能力ではない。求められるのは、セキュリティ対策が日々の業務の中で実際に運用され、その証跡が積み重なっているという実態である。担当者を明確にし、方針・手順を定め、それに沿って運用を回し、記録を残す——こうした地道な営みは、一夜漬けで作れるものではない。

したがって、経営が向き合うべき論点も変わってくる。「★を取得できるか」ではなく、「★を維持し続けられるか」。言い換えれば、「その運用を、誰が、どのように回し続けるのか」という体制の問題である。

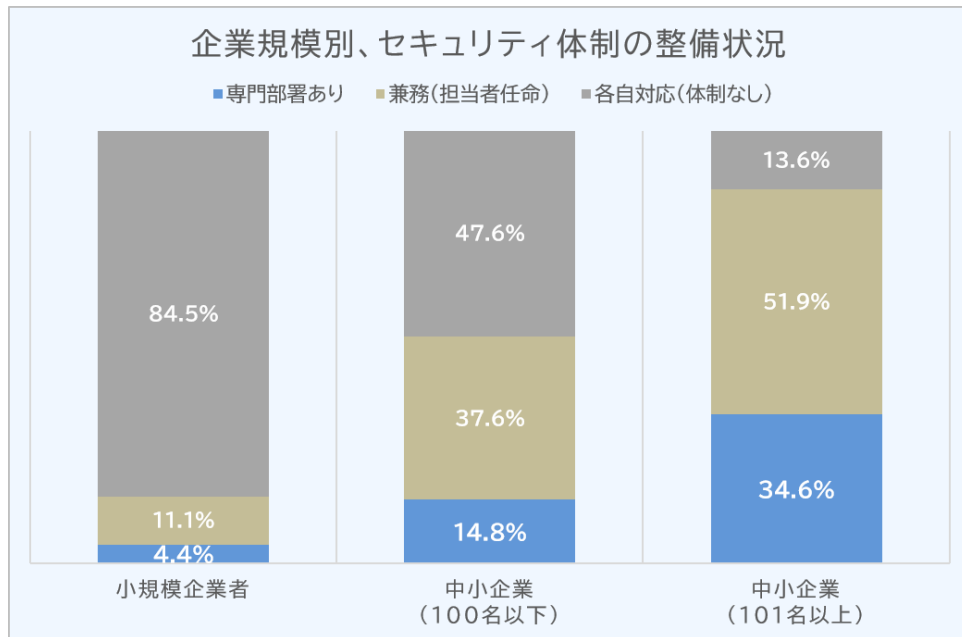
では、その体制を支える人員は、実際のところどれだけ確保されているのだろうか。その実態を、企業の人員体制に関するデータから確認したい。

"一人情シス"に依存しない体制をどうつくるか

ここで直視すべきは、多くの企業でセキュリティを担う人員が、必ずしも潤沢ではないという現実である。

その象徴が、いわゆる「一人情シス」である。これは、情報システムの企画から導入、運用、セキュリティ対応までを、一人の担当者が担う状態を指す。以下の調査は「一人情シス」の企業数を直接示すものではないが、セキュリティを専任で担う体制が限られている実態を示している。IPAによれば、情報セキュリティの専門部署や専任担当者を置く企業の割合は、従業員100名以下で14.8%、101名以上でも34.6%にとどまる（図表3）。一定の規模を持つ企業であっても、専門の体制を備えているのは3社に1社程度にすぎず、多くは兼任、あるいは各自の対応に委ねているのが実態である。

図表3 企業規模別に見たセキュリティ体制の整備状況——企業規模が大きくても専任体制は限定的



(注) n=4,191 (小規模企業者(商業・サービス業は5名以下、製造業その他は20名以下) 2,775社、中小企業(100名以下) 1,121社、中小企業(101名以上) 295社)

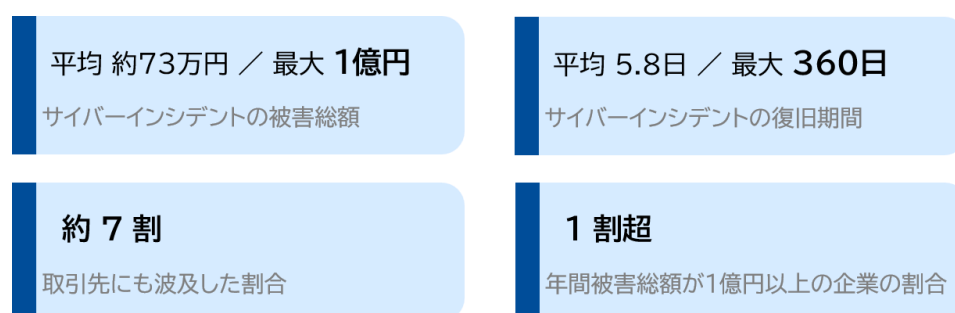
(出所) 前掲 IPA 調査(図 3-121)をもとに大和総研作成

こうした体制は、SCS 評価制度が求める「継続運用」を支えるうえで課題を抱える。担当者が限られれば、対策や設定は特定の個人に依存しやすく、その担当者の退職・休職によって運用の継続が難しくなるおそれがある。複数の視点で確認する仕組みが十分でなければ、設定の不備や対応漏れを見落とす可能性もある。制度への対応に必要な日々の運用と証跡の積み重ねを支えるには、社内の役割分担や外部専門家の活用など、特定の担当者だけに依存しない仕組みが求められる。

だからこそ、SCS 評価制度への対応を、単なる★取得の作業として捉えるだけでは不十分である。制度への対応を、自社のセキュリティ体制そのものを見直す契機とする必要がある。

その必要性は、インシデントがもたらす損失からも明らかである。IPA の調査では、被害総額は平均で約 73 万円だが、100 万円以上の被害を受けた企業が 9.4%、最大では 1 億円に達する。復旧期間も平均 5.8 日に対し、最長では 360 日を要した企業がある。平均値の背後にある分布の広がりこそが、この問題の本質を示している。さらに、被害を受けた企業の約 7 割が、自社にとどまらず取引先にも影響が及んだと回答している。近年の上場企業を対象とした民間調査でも、年間の被害総額が 1 億円以上に達した企業が初めて 1 割を超えた⁵（図表 4）。

図表 4 サイバーインシデント被害の実態——損失は「取引先」にまで及ぶ



（注 1）被害総額・復旧期間・取引先への波及は、サイバーインシデントの被害を経験した企業（n=975）を母数とする。被害総額・復旧期間は過去 3 期の集計

（注 2）「取引先にも波及した割合」は、被害による影響が取引先にも及んだと回答した企業の割合

（注 3）「年間被害総額が 1 億円以上の企業の割合」は KPMG ジャパンと日本経済新聞社による国内上場企業を対象とした調査（回答 424 社、当該設問の有効回答 128 社）による。他の 3 項目とは調査対象・調査期間・設問が異なるため、単純な比較はできない

（出所）前掲 IPA 調査（表 3-2・図 3-45）および KPMG ジャパン「サイバーセキュリティサーベイ 2026 の主要な調査結果」（脚注 5）をもとに大和総研作成

こうした損失に至る前に、平時のうちに対策を打っておくことが肝要である。平時であれば余裕を持って整えられたはずの体制も、混乱のさなかで慌てて作るのは容易ではない。損失に加え、復旧や説明対応、さらには体制を立て直す負担を考えれば、平時から計画的に体制を整備することの意義は大きい。SCS 評価制度への対応はその一步を踏み出す格好の機会となる。

おわりに

本稿では、SCS 評価制度をめぐる二つの問いについて考えてきた。★は今後、取引相手を判断する「入口」としての重みを増していくだろう。一方で、★の取得だけで信頼が保証されるわけではない。重要なのは、その背後にある対策を継続し、★を維持できる組織体制・人材・運用プロセスである。

⁵ KPMG ジャパン [「サイバーセキュリティサーベイ 2026」の主要な調査結果を発表](#)

SCS 評価制度への対応は、目前の★取得にとどまらず、自社の「守る力」を組織に根づかせる取り組みとして捉えるべきである。体制の整備には時間を要するからこそ、制度開始を待たず、自社の現状と課題を把握するところから着手する意味がある。

もっとも、自社だけで現状を的確に把握し、あるべき体制を描くことは、必ずしも容易ではない。自社だけでの対応が難しい場合には、必要に応じて外部の専門家を活用することも選択肢となる⁶。

「御社のセキュリティ対策は★いくつですか」——その問いに、自信を持って答えられる企業であるために。いまこそ、★の先を見据えた備えを始めたい。

以上

⁶ 大和総研では、SCS 評価制度への対応に関する現状把握から改善計画の策定、対策の実行等を伴走支援するサービスを提供している。詳細は[当社ウェブサイト](#)を参照。
