中堅・中小企業を応援！
経営の最新トレンドと実務ノウハウをお届けする
ビジネス情報誌

MJS
Monthly
Report
マンスリーレポート

特別版

Feature

サプライチェーン全体でセキュリティを考える時代へ

「セキュリティ対策評価制度」で求められる中小企業・会計事務所の対応

概要

近年、サイバー攻撃による情報流出や物流停止など、サプライチェーン全体へ被害が出る事件が多発しています。このため、委託元・委託先を含めたサプライチェーン全体のサイバーセキュリティ対策が求められています。
そこで、委託元と委託先の双方で対策の状況を把握しやすくなるよう、経済産業省および内閣官房国家サイバー統括室が制度構築方針を公表し、独立行政法人情報処理推進機構（IPA）が運営主体となる「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（SCS評価制度）」が、2026年度末頃の開始を目指して準備されています。
本稿では、制度の全体像と、企業・会計事務所が押さえるべきポイントをお伝えします。
※本稿は2026年6月15日時点の情報に基づいて作成しています。

『Monthly Report』は、MJS税経システム研究所が制作するユーザー向け月刊誌です。
毎号、税務・商事法・会計・経営などの最新トレンドと実務ノウハウをタイムリーにお届けしています。
この冊子は、本誌の記事を抜粋し、1テーマをコンパクトにまとめた特別版です。ぜひお役立てください。

MJS
編集制作
株式会社ミロク情報サービス
税経システム研究所

MJS
Monthly
Report

特別版

2026 August
No.211

Feature

2

サプライチェーン全体でセキュリティを考える時代へ

「セキュリティ対策評価制度」で求められる中小企業・会計事務所の対応

税経システム研究所　客員講師　上ヶ平IT事務所 代表
ITコーディネータ、情報処理安全確保支援士、上級ウェブ解析士　上ヶ平裕彦

Feature

サプライチェーン全体でセキュリティを考える時代へ

「セキュリティ対策評価制度」で求められる中小企業・会計事務所の対応

近年、サイバー攻撃による情報流出や物流停止など、サプライチェーン全体へ被害が出る事件が多発しています。このため、委託元・委託先を含めたサプライチェーン全体のサイバーセキュリティ対策が求められています。そこで、委託元と委託先の双方で対策の状況を把握しやすくなるよう、経済産業省および内閣官房国家サイバー統括室が制度構築方針を公表し、独立行政法人情報処理推進機構（IPA）が運営主体となる「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（SCS 評価制度）」が、2026 年度末頃の開始を目指して準備されています。本稿では、制度の全体像と、企業・会計事務所が押さえるべきポイントをお伝えします。
※本稿は 2026 年 6 月 15 日時点の情報に基づいて作成しています。

税経システム研究所 客員講師　上ヶ平 IT 事務所 代表
IT コーディネータ、情報処理安全確保支援士、上級ウェブ解析士
上ヶ平裕彦 [かみがひら・ひろひこ]
沖電気工業で開発技術者として勤務。その後、誠文堂新光社やインプレスで出版編集を支援、富士通グループで SE（富士通 BSC）・コンサルタント（富士通総研）・マーケター（富士通本社）を歴任。2019 年に IT コーディネータ資格を取得、上ヶ平 IT 事務所を開業。自治体や企業の IT 支援を行っている。

1 なぜ今「サプライチェーン × サイバーセキュリティ」なのか

(1)近年増加するサプライチェーン攻撃

サイバーセキュリティという言葉を一般報道で見る機会がとても多くなりました。私たち個人レベルでも、オンライン詐欺の被害に遭う機会が珍しくなくなっています。直近数年で海外から日本語で接触してくる攻撃者が目立つようになっていることにお気づきの方も少なくないでしょう。これは、生成AIを使った機械翻訳が圧倒的な精度で世界中から簡単に利用できるようになったことが一因です。日本語はこれまで世界的にも特殊で習得が難しい言語といわれていましたし、日本国内は諸外国に比べ治安が良いことでも定評がありました。それが生成AIにより、海外の攻撃者が自然な日本語で私たち日本人に接触してくる時代が来てしまったのです。

同じく企業のセキュリティリスクも高まっています。独立行政法人 情報処理推進機構（IPA）が報告する「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」によれば、中小企業の11.4％がこれまでにサイバー被害を受けたことがあると回答しています。さらに警察庁の「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」によれば、ランサムウェアに限定すれば被害を受けた企業の約66％が中小企業であり、調査・復旧に要した費用の総額は1,000万～5,000万円に及んだケースが被害企業の約41％に及び、１億円以上に達した企業も約８％ありました。さらに、前述のIPAの調査では、取引先や委託先のサイバーリスク対策の管理を行っていない事態を問題視しています。大企業でも中小企業でも管理のできていない企業は40％以上にのぼりますが、従業員数が少ない企業ほど比率が高くなる傾向にあります。

報道された事故事例では、2022年にトヨタ自動車のサプライチェーン（供給網）に連なる自動車

部品メーカーがランサムウェア（身代金要求型ウイルス）に感染したことをきっかけとし、トヨタ自動車の国内全14工場の28ラインが止まりました。2025年には、アサヒグループホールディングスやアスクルなどがランサムウェアの攻撃の影響を受け、受注・出荷業務や物流に大きな支障が生じたと報じられました。前者ではアサヒグループの物流網を利用していた他の飲料メーカー、後者では一般の事務用品だけでなく衛生・医療・介護用品を利用していた中小クリニックや介護施設などにも被害が及び、大きな社会問題になったことは記憶に新しいところです。

士業法人でも被害事例があります。2024年６月には税理士法人および監査法人がランサムウェアによるサイバー攻撃を受け、同事務所に業務委託していた損害保険会社や銀行などが顧客の個人情報（約6.3万件以上）の漏えいのおそれを公表する事例がありました。顧客個人の連絡先や税務関連情報が流出データに含まれている可能性もあり、顧客個人が新たな犯罪に巻き込まれるリスクも高まります。

2023年６月には、社会保険労務士向けシステムがランサムウェアのサイバー攻撃を受け、個人情報保護委員会への報告が行われました。

2026年５月には、大手クラウド会計ソフトが不正アクセスを受け、銀行口座との連携機能が停止するなど、サービス利用で影響を受ける事態となりました。

(2)ビジネス現場で起きている２つの問題

以上のように、サイバー攻撃によるサプライチェーンの停止・分断は、攻撃を受けた企業組織に留まらず多くの取引先や顧客に被害を及ぼします。そのため委託先を含めたサプライチェーン全体のセキュリティ対策が求められています。ここで２つの課題が表面化しつつあります。

まず、委託元企業においては、委託先におけるセキュリティ対策が可視化しづらく、要求事項（チェックリスト等）に適合させることが難しくなっています。

また、委託先企業においては、複雑なサプライチェーン下でさまざまな委託元から多様な要求事項を求められ、過度な負担につながっています。特にサプライチェーンの末端に位置する中小企業が重い負担を被りやすい構図です。

(3)経済産業省等が制度化に踏み切った背景

以上のような問題を鑑み、経済産業省等は、解決の施策として「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）」の構築を進めています。各事業者が★マークの取得を通じて適切なセキュリティ対策を実施し、サプライチェーン全体でのセキュリティ向上を図るものとなっています。業務委託先へのサイバー攻撃を起因とした自社事業・サービスの提供途絶や機密情報漏えいなどのリスクに備えます。

具体的には、２社間の取引契約などにおいて、委託元が、委託先に適切なレベル（★マーク）を提示し、示された対策を促すとともに実施状況の確認をすることなどが想定されています。再委託先については、委託元から見た直接の管理対象にはなりませんが、直接の委託先を通じて再委託先も必要に応じ管理することが想定されています。

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」とは

(1)制度の基本コンセプト

この制度では、発注者・受注者双方にとって、共通のものさしを作り、必要なセキュリティ対策の決定や対策状況の説明が容易で適切になることを目的としています。これにより、互いのサプライチェーン・リスクの低減や、経済・社会全体でのサイバーレジリエンス（サイバー攻撃・侵害を予測し、それらに耐え、回復し、適応する能力）の強化が期待されます。

なお、格付け制度のように事業者間でセキュリティ対策レベルを競わせることを目的とした制度ではありません。必要な対策範囲を定めて取引先間で合意していくことが望ましい姿です。この制度で期待される効果は以下のものがあります。

発注企業においては、取引先に求めるセキュリティ対策について、その内容や水準を決定しやすくなります。対策の実施がどのような状況にあるか、

把握が容易になります。また、取引先から被る自社リスクの低減が期待されます。

受注企業においては、自社に必要なセキュリティ対策が明確化され、意思決定がしやすくなります。そして発注企業に対して、セキュリティ対策に関する説明の説得力向上と、利用するセキュリティサービスが標準化されることで選択肢を増やしコスト低減も期待されます。

さらに社会全体で、サイバー攻撃への備えがある企業への適切な評価が広まります。お互いの取引コスト低減から社会全体での効率化が図られます。そして、セキュリティ製品やサービスの市場拡大と競争力向上も期待されます。

総じて、共通した基準で企業間の取引実務に使える制度であることが、目指すところとなります。

(2)評価制度の全体像（★1～★5）

図表1に示す概要のとおり、既存のSECURITY ACTION制度（★1・★2）を踏まえ、SCS評価制度として★3・★4が具体化され、★5は今後検討されます。今回のSCS評価制度では、**図表2**に示す内容で要求事項名とそれぞれの評価項目数が設定されています。各評価項目の具体的な内容は、IPAよりWebで公開されている「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（SCS評価制度）」の「★3・★4　要求事項・評価基準」からExcelシートでダウンロードして見ることができます。

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）要求事項・評価基準
https://www.ipa.go.jp/security/scs/requirements-criteria.html

主な内容を見ていきましょう。

①★1、★2

2017年より始まったSECURITY ACTION制度で定められました。

情報セキュリティ対策に取り組むという自己宣言を促す制度であり、セキュリティリスク対策と

図表1　SCS評価制度★1～★5の概要

	★1	★2	★3	★4	★5
実施時期	2017年より開始済	2017年より開始済	2026年度末より開始予定	2026年度末より開始予定	（今後検討することを想定）
	SECURITY ACTION制度		SCS評価制度		
想定される脅威	（想定せず）	（想定せず）	一般的なサイバー攻撃（広く認知された脆弱性等を悪用）	サプライチェーンに大きな影響（供給停止など）をもたらす企業への攻撃 情報漏えいにより大きな影響をもたらす資産（機密情報など）への攻撃	高度なサイバー攻撃（未知の攻撃も含む）
対策の基本的な考え方	「情報セキュリティ6か条」の取組み宣言	「5分でできる！情報セキュリティ自社診断」で自社の状況を把握し、「情報セキュリティ基本方針」を定め、外部に公開	最低限のセキュリティ対策（基礎的な組織的対策とシステム防御策）	標準的なセキュリティ対策（組織ガバナンス・取引先管理、システム防御・検知、インシデント対策等包括的な対策）	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プロセス。現時点でのベストプラクティスに基づくシステム対策）
脅威に対する達成水準（イメージ）	・社内で情報セキュリティ対策に取り組む意識や機運を高めている。	・情報セキュリティ対策に本格的に取り組んでいる。	・組織内の役割と責任が定まっている。 ・自社IT基盤での対策、インシデント発生時の対応手順が定まり実施されている。	・取引先のシステムやデータを含む内外への被害拡大、攻撃者による目的遂行、これらリスクを低減する対策が講じられている。 ・事業継続に向けた取組や取引先の対策状況の把握など、自社の位置付けに適合したサプライチェーン強靭化策が講じられている。	・国際規格等に基づくマネジメントシステムが確立されている。 ・ベストプラクティスに基づくサイバーレジリエンス確保策が講じられている。 ・取引先等への指導や共同での訓練の実施など、自社サプライチェーン全体の対策水準向上に資する対策が講じられている。
要求項目数	6件	25件＋1件	26件	43件	（今後検討することを想定）
評価スキーム	自己評価	自己評価	専門家確認付き自己評価	第三者評価	第三者評価
有効期間	未設定	未設定	1年間	3年間（自己評価結果を評価機関に毎年提出）	（今後検討することを想定）

（独立行政法人情報処理推進機構（IPA）の資料などから筆者作成）

図表 2　SCS 評価制度★3 と★4 の要求事項名と評価項目数

大分類		中分類		要求事項名		評価項目数	
						★3	★4
1	ガバナンスの整備	1-1	組織の状況	1-1-1	1 社内ルール	0	3
		1-2	役割、責任、権限	1-2-1	セキュリティ推進活動部門	3	4
				1-2-2	サイバー攻撃の監視・分析体制	0	2
				1-2-3	守秘義務のルール	2	4
		1-3	ポリシー	1-3-1	セキュリティ対応方針の策定	3	4
		1-4	監督	1-4-1	セキュリティ対策推進計画	0	2
2	取引先管理	2-1	サイバーセキュリティサプライチェーンリスクマネジメント	2-1-1	取引先とのビジネス又はシステム上の関係	2	3
				2-1-2	機密情報の取扱い	1	1
				2-1-3	取引先のセキュリティ対策状況	0	1
				2-1-4	セキュリティインシデント発生時の役割・責任	1	1
				2-1-5	機密情報の回収・破棄	0	1
3	リスクの特定	3-1	資産管理	3-1-1	情報機器、OS 及びソフトウェアに関する情報の把握	4	7
				3-1-2	ネットワークに関する情報の把握	2	4
				3-1-3	外部情報サービスの管理	2	2
				3-1-4	機密区分に応じた情報の管理	3	8
				3-1-5	リモートワークにおけるルール	0	3
		3-2	リスクアセスメント	3-2-1	脆弱性の管理体制	0	5
4	攻撃等の防御	4-1	アイデンティティ管理、認証、アクセス制御	4-1-1	ユーザ ID の管理手続	4	4
				4-1-2	管理者 ID の管理手続	8	8
				4-1-3	認証の強度・実装方法の決定	4	5
				4-1-4	アカウントロック制御	2	2
				4-1-5	パスワード設定ルール	5	5
				4-1-6	パスワード管理ルール	3	3
				4-1-7	アクセス権の管理ルール	1	6
				4-1-8	サーバ設置エリアへの入退室管理	0	4
				4-1-9	可搬媒体の制限	0	3
		4-2	意識向上とトレーニング	4-2-1	セキュリティの意識向上のための教育・研修	0	5
				4-2-2	セキュリティインシデント発生時の教育・訓練	3	3
		4-3	データセキュリティ	4-3-1	データの暗号化	0	2
				4-3-2	データの保管ルール	0	1
				4-3-3	取引先との情報共有ルール	0	1
				4-3-4	適切なバックアップ	3	3
		4-4	プラットフォームセキュリティ	4-4-1	情報機器、OS 及びソフトウェアの安全な構成	3	6
				4-4-2	サポート期限の切れた OS 及びソフトウェアへの対策	0	1
				4-4-3	ログの取得	0	3
				4-4-4	セキュリティパッチ・アップデートの手続	2	3
				4-4-5	マルウェア感染からの保護	3	5
		4-5	技術インフラのレジリエンス	4-5-1	ネットワーク境界防護	7	9
5	攻撃等の検知	5-1	継続的監視	5-1-1	ネットワーク接続・データの監視	3	3
				5-1-2	情報機器及びソフトウェアの挙動監視	0	3
		5-2	有害事象の分析	5-2-1	セキュリティインシデントのレベルごとの対象範囲	0	2
6	インシデントへの対応	6-1	インシデント管理	6-1-1	インシデント対応手順	6	6
7	インシデントからの復旧	7-1	インシデント復旧計画の実行	7-1-1	事業継続要件に沿った復旧準備	1	2
合計						81	153

※★ 4 の評価項目数は、★ 4 取得時に満たすべき評価基準の合計数。★ 3 の項目数も包含されていて、★ 3 との差分を示すものではない。
（「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）要求事項・評価基準」をもとに筆者作成）

しての実効性を問うものではありませんが、SCS制度へ進むための基礎的な取り組みとして位置づけられます。中小企業向けのIT導入補助金などで採択の加点要素とされたため、取得している企業も多いようです。

②★3

最低限ここまでは対応することが望ましいとされる基礎的な内容になっています。

「1 ガバナンスの整備」と「2 取引先管理」で評価項目数が設定されている要求事項は、すでに何らかの形で対応している企業もあるでしょう。

「3 リスクの特定」では、自社IT環境の基本情報を把握し、**図表３**の「情報資産管理台帳」として整理することが必要です。

「4 攻撃等の防御」では、「4-1 アイデンティティ管理、認証、アクセス制御」が主にユーザーIDや管理者IDとパスワードの管理を評価するものです。その多くは★4と共通する評価基準で、重要かつ攻撃耐性に直結しています。IDについては、同じIDを複数の利用者で使い回している現場は今も少なからず存在しています。特に派遣社員やアルバイト人員、受け入れ出向者でIDの使い回しが起こりやすく、社内での過失や不正行為が起こった場

図表 3　情報資産管理台帳の記入例

① 業務分類	② 情報資産名称	③ 備考	④ 利用者範囲	⑤ 管理部署	⑥ 管理者名	⑦ 管理者連絡先	⑧ 媒体・保存先	⑨　評価値			重要度	⑩ 保存期限	⑪ 登録日
								機密性	完全性	可用性			
人事	社員名簿	社員基本情報	人事部	人事部	○○ ○	090-XXXX-XXXX	事務所 PC	3	1	1	3		2026/4/1
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部	○○ ○	090-XXXX-XXXX	書類	3	3	2	3	5年	2026/4/1
経理	給与システムデータ	税務署提出用源泉徴収票	給与計算担当	人事部	○○ ○	090-XXXX-XXXX	事務所 PC	3	3	2	3	7年	2026/4/1
経理	当社宛請求書	当社宛請求書の原本（過去3年分）	総務部	総務部	△△ △	090-XXXX-XXXX	書類	2	2	2	2		2026/4/1
共通	電子メールデータ	Gmailに転送	担当者	総務部	△△ △	090-XXXX-XXXX	社外サーバー	3	3	3	3		2026/4/1
営業	顧客リスト	得意先（直近5年間に実績があるもの）	営業部	営業部	×× ×	090-XXXX-XXXX	可搬電子媒体	3	2	2	3		2026/4/1
営業	顧客リスト	得意先（直近5年間に実績があるもの）	営業部	営業部	×× ×	090-XXXX-XXXX	モバイル機器	3	2	2	3		2026/4/1
営業	受注契約書	受注契約書原本（過去10年分）	営業部	営業部	×× ×	090-XXXX-XXXX	書類	2	3	2	3		2026/4/1
営業	製品カタログ	現役製品カタログ一式	営業部	営業部	×× ×	090-XXXX-XXXX	社内サーバー	1	2	2	2		2026/4/1
調達	委託先リスト	外部委託先（直近5年間に実績があるもの）	総務部	総務部	□□ □	090-XXXX-XXXX	社内サーバー	1	2	2	2		2026/4/1
技術	製品設計図	現役製品の設計図	開発部	開発部	●● ●	090-XXXX-XXXX	書類	3	3	3	3		2026/4/1

＜記入内容についての解説＞

① 業務分類　情報資産に関連する業務や部署名を記入します。
情報資産は業務に関連して発生しますので、まず関連業務や部署を特定し、その業務や部署で利用している情報を洗い出すと記入漏れが少なくなります。
② 情報資産名称　情報資産の内容を簡潔に記入します。正式名称がないものは社内の通称で構いません。管理方法や重要度が同じものは1行にまとめます。
③ 備考　必要に応じて説明等を記入します。
④ 利用者範囲　情報資産を利用してよい部署等を記入します。
⑤ 管理部署　情報資産の管理責任がある部署等を記入します。小規模事業者であれば担当者名を記入しても構いません。
⑥ 管理者名　情報資産に対して情報セキュリティ上の管理責任がある管理者名を記入してください。
⑦ 管理者連絡先　管理者の連絡先を記入してください。
⑧ 媒体・保存先　情報資産の媒体や保存場所を記入します。書類と電子データの両方で保存している場合は、それぞれ完全性・可用性（機密性は同一）や脅威・脆弱性が異なるので2行に分けて記入します。
例）見積書「電子データを事務所PCに保存」「印刷して書類を保管」（この項目から脅威と脆弱性を想定します）
⑨ 評価値・重要度　情報資産の機密性、完全性、可用性それぞれの評価値を記入します。3種類の評価値から重要度が表示されます。
⑩ 保存期限　法定文書は法律で定められた保存期限を、それ以外は利用が完了して廃棄、消去が必要となる期限を記入します。
必要な期間以上に保有し続けるより廃棄・消去したほうがリスクが小さくなる場合に利用します。
⑪ 登録日　登録した日付を記入します。内容を更新した場合は更新日に修正します。

（独立行政法人情報処理推進機構（IPA）「中小企業の情報セキュリティ対策ガイドライン 第 4.0 版」より引用）

合に、誰によるものかの追跡を難しくします。また、予測しやすいパスワード（よくある例では電話番号や生年月日など）を設定していると、外部から特定され侵入されてしまう危険性を高めます。リスト攻撃といって、どこかのサービスから流失したIDとパスワードのリストを使い、別のサービスに不正ログインを試みるサイバー攻撃もあります。これは多くのユーザーが複数のサイトで同じパスワードを使い回している実態を突いた、攻撃者に悪用されやすい手法です。2026年度末から開始予定のSCS評価制度ではログイン時にスマートフォンのショートメッセージ（SMS）通知や指紋などの生体情報を併用する方式（多要素認証）などを利用したうえでパスワードの長さを8文字以上とし、多要素認証などを利用できない場合は、パスワードは英大文字および英小文字と数字を含めた10文字以上とする旨が示されています。これについては、2025年7月に米国NIST（国立標準技術研究所）から新たなガイドラインが発表されており、今後SCS評価制度の評価基準に対しても見直しが入ることが考えられます。

「4-2 意識向上とトレーニング」では、セキュリティインシデント発生時の対応に関する教育・訓練を年1回以上行うことが示されています。インシデントが発生したときに備え、取引先を含む社内外関係各所への報告・共有に必要な最低限の手順を定義、実施されていることが必要です。なお、この報告・共有ルートや初動・復旧等の対応手順については「6-1-1 インシデント対応手順」に記載されています。

「4-3 データセキュリティ」では、データが消失や改ざんされる事態に備え、バックアップの実施と復旧手順の整備も定められています。重要な機密情報については、機器の設置場所から離れた遠隔地でのバックアップの実施が示されています。クラウドサービスなどを活用すると良いでしょう。

「4-4 プラットフォームセキュリティ」では、パソコンやサーバ、スマートフォンなどの機器に、利用を許可していないソフトウェアがインストールできないよう、制限することが示されています。セキュリティ更新プログラムの適用はリリースされてから14日以内と示されているので、頻度を見直しましょう。ネットワークに接続しているパソコンやサーバには、マルウェア（ウイルス等）対策ソフトウェアを導入する、パターンファイルの更新を行うなどの対策を検討しましょう。

「4-5 技術インフラのレジリエンス」では、ファイアウォールやルータ等によるネットワーク境界防護、認証されていない通信の遮断、境界設定の管理などが示されています。加えて、「5-1-1 ネットワーク接続・データの監視」では不正アクセスをリアルタイムで検知・遮断する仕組みの導入が示されています。

UTM（Unified Threat Management：統合脅威管理。複数のセキュリティ機能を統合して運用管理し、社内ネットワーク全体を保護する）と呼ばれる機器か同様の防御機能を持つ機器・サービスを利用することも選択肢の一つです。ただし、制度上、特定製品の導入が必須とされているわけではありません。後述する公的支援制度を活用したり、ITベンダーに相談して自社の規模に合った機器を選定したりしても良いでしょう。異常事態の発生を見逃さないよう、セキュリティ担当者や管理者には、機器からのログやアラートの分析と、インシデントに該当するかの判断を行うことが示されています。

以上は、セキュリティ専門家による確認付きでの自己評価を行うことで、★3マークを取得できます。ここでいうセキュリティ専門家とは、情報処理安全確保支援士などの資格保持者のうち、所定の研修を受講した者が想定され、2027年1月頃にIPAから詳細が公表される予定です。

◆専門家の視点

2026年1月にIPA主催で実施されたSCS評価制度の実証研修セミナーを筆者が受講し体験したロールプレイによれば、要求事項・評価基準の網羅性はとても優れている反面、個々の評価基準においてどこまでを良しとするかは専門家それぞれよって判断のブレを生じかねず、やや曖昧な印象がありました。この点は制度試行を通じて、より厳密な基準に改められていくのではないかと思います。なお、IPAからは、評価用ガイド類（要求事項・評価基準の解説書や★の取得ガイド等）が2026年10月頃に公開予定、とする回答が2026年6月時点でありました。

③★4

標準的なセキュリティ対策として実施すべき水準です。★3にはなかった評価項目を見ていきましょう。

「1 ガバナンスの整備」では、自社に関係する法令や所管省庁および関係団体（工業会や業界団体など）が定める基準を把握したうえで社内ルールを定め、年1回以上の頻度で法令や基準を確認して社内ルールを点検し、役員・従業員・派遣・受け入れ出向者などへ周知することが示されています。重要なのは、社内の情報セキュリティ委員会などに経営層が参加し、予算・人員計画や事故対応など経営判断が必要な場面に備えた体制を作ることです。

「2 取引先管理」では、子会社や取引先に年1回以上の頻度でセキュリティ対策状況を把握することが示されています。訪問での点検やチェックシートの回答を受領するなど、実効性ある点検の実施方法が例示されています。

「3 リスクの特定」では、自社IT環境の構成情報を★3よりも詳細に確認する必要があります。「3-1-4 機密区分に応じた情報の管理」では、人員の退職や任期満了時には機密情報やIT機器、印刷物、IDや鍵なども回収することとされています。パソコンやサーバ、スマートフォンなどを廃棄するときは、データを復元できないように確実な抹消処理を実施します。「3-1-5 リモートワークにおけるルール」も★3にはなかった要求事項が加わります。「3-2 リスクアセスメント」ではパソコンなどのIT機器について、ソフトウェアの脆弱性（プログラムの欠陥などでサイバー攻撃を受けうる弱点）の情報収集から対応までを行う管理体制を定めることとされています。専門的な技術知識と作業時間が必要なため、中小企業の社内要員だけで賄うのは難しいかもしれません。ITベンダーなどの情報提供サービスを利用するか、取引先との共同チームを作って対応することも考えられます。後述する公的支援制度を活用する方法もあります。

「4 攻撃等の防御」では、「4-1-7 アクセス権の管理ルール」でアクセス権の棚卸しを年1回以上の頻度で行うなどの運用体制が示されています。「4-1-8 サーバ設置エリアへの入退室管理」や「4-1-9 可搬媒体の制限」、「4-2-1 セキュリティの意識向上のための教育・研修」も★3にはなかった要求事項ですが、基本的な管理策としてすでに運用されている企業もあると思います。「4-3-1 データの暗号化」や「4-3-2 データの保管ルール」、「4-3-3 取引先との情報共有ルール」も、取引先から見れば、実施してほしいと感じる項目でしょう。「4-4-3 ログの取得」と「4-5-1 ネットワーク境界防護」はIT機器の追加投資を要することになりやすく、中小企業には負担が重いかもしれません。ここも、後述する公的支援制度を活用したり、ITベンダーに相談し、自社の規模に合った機器を選定するなどを検討しましょう。

「5 攻撃等の検知」では、「5-1-2 情報機器及びソフトウェアの挙動監視」にて会社支給の各パソコンにインストールされているソフトウェアを年1回以上の頻度で点検する必要があります。人手で点検を行うのは時間と手間を要する上に作業漏れが起こりやすいため、PC管理ツールの活用も有効です。「5-2 有害事象の分析」ではログイン失敗などの不審なアラートをチェックし、インシデントに該当するかを判断することが示されています。

「7 インシデントからの復旧」では、「7-1-1 事業継続要件に沿った復旧準備」でバックアップからのシステム復旧が手順通りに実行でき、目標時間内に復旧できることを確認することが示されています。システムの運用が何年間も続くと、保存データが増えて復旧も長時間に及ぶことが少なくありません。長期運用を見越したバックアップ設計と点検が必要ですし、できることなら訓練的にシステム復旧を実際に行ってみることが望ましいと言えます。

以上は、評価機関によるヒアリングや規程などの確認審査および技術検証といった第三者評価を経て、★4マークを取得できます。ここでいう評価機関とは、2026年12月末を目途にIPAから公表される予定です。

④★5

高度なサイバー攻撃を想定した内容です。★5は今後、要求事項・評価基準や評価スキームの具

体化が検討される予定です。具体的な対策実装は、産業界で実績のあるガイドライン（例：自工会サイバーセキュリティガイドライン（Lv３））等から対策を選定することが想定されています。また、ISMS適合性評価制度との整合も配慮されるようです。

3 中小企業や会計事務所の実務にどう関係するのか

(1)中小企業や会計事務所も対象となっている制度

サプライチェーンというと、製造業や流通業が主な対象業種と思われそうですが、製造業・流通業に限らず、サプライチェーンを構成する幅広い事業者のIT基盤が対象となり得ます。したがって、一般企業に加えて、会計事務所や監査法人、サービス業なども範囲に入ってきます。特に個人情報や経営秘密情報の流出はどの企業においても大きなリスクになり得ます。最近増えてきた三重・四重脅迫型ランサムウェアと呼ばれるサイバー攻撃は、データの暗号化、窃取、暴露に加え、窃取したデータを使って取引先や顧客にも直接脅迫を行います。DDoS（Distributed Denial of Service：分散型サービス妨害）と呼ばれる方法で社外接続ネットワークへの妨害を行い、企業を孤立させ復旧を邪魔する攻撃も現れてきました。被害企業は身代金支払いや事業停止での経済損失に加え、対外的な信用失墜や関係各所への損害拡大を招き、事業継続の危機に陥るリスクが非常に高いものです。

会計事務所は企業規模としては中小であっても、扱う情報の重要性（財務・役員・顧客情報など）が格段に高いため、重要性の高い機密を預かる委託先として、サイバー攻撃にも強い体制を整えることが望ましいでしょう。

取引先（クライアント）の特性・業種別優先順位で、より高度な対応を求められそうなのは上場企業や外資企業、金融・証券企業です。発注側企業として年１回以上のリスク評価を行うため、発注先企業にもSCS評価制度への対応を求めることが考えられます。次に優先順位が高いのは、製造業、建設業、IT・システム開発企業です。多重下請け構造からサプライチェーンが複雑で、ランサムウェアなどの標的になりやすい業種です。続いて、医療・福祉、流通・小売、インフラ関連企業も、大量の個人情報や生活に直結するシステムを持つため、高いセキュリティ水準が求められ始めていると考えられます。

企業内で適切なセキュリティ対策を施すことは、コストとともに人員時間も費やすことになるので、経営者がセキュリティ対策を「戦略的先行投資」だと意識改革していくことも大切です。

(2)関係しながら制度の対象外となるもの

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）システムは、SCS評価制度の対象外となっています。また、発注元等に提供する製品も対象外です。それらはサプライチェーン全体での共通化が難しい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いた対策が行われると想定されています。

(3)ISMS適合性評価制度との関係

情報セキュリティマネジメントシステム（ISMS）適合性評価制度は、情報セキュリティの運用管理状況を可視化するものとして以前から活用されてきました。これは、国際規格ISO/IEC 27001に基づく国際的な整合性をとるもので、情報セキュリティマネジメントシステムに対する第三者適合性評価制度です。対象とするのが情報セキュリティであるため、今回のSCS評価制度とも共通する部分がありますが、両者を比較すると違いがあります。

まず目的の違いです。ISMS適合性評価制度は、本制度の認証を希望する組織において、諸外国からも信頼を得られる情報セキュリティレベルを達成することを目的としています。SCS評価制度は、サプライチェーン全体でのセキュリティ水準の底上げを図ることを目的としています。

対象にも違いがあります。ISMS適合性評価制度はISMSを運用する組織が対象ですが、SCS評価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を含むIT基盤を対象とします。

管理策にも違いがあります。ISMS適合性評価

制度は、組織が実施したリスク評価結果に基づいて、必要な情報セキュリティ管理策を選定します。つまり、ここまで対策しなければならないといった統一基準ではなく、それぞれの組織が自社で適切な管理策を定めます。対してSCS評価制度は、代表的な脅威や国内外制度を踏まえて定められた共通の要求事項・評価基準に基づき、セキュリティ対策の実施状況を評価するとされています。つまり、発注企業と受注企業が共通のものさしによってセキュリティ対策の実施状況を可視化し、管理策を検討することができます。

ISMS適合性評価制度とSCS評価制度は、相互補完的な役割があります。

(4)中小企業や会計事務所特有の課題と解決策

①紙とクラウドが混在するハイブリッド環境

デジタルデータだけでなく物理的なセキュリティ（★4では「4-1-9 可搬媒体の制限」にて印刷物の持ち込み・持ち出しルールを定める必要がある）もSCS評価制度の対象です。机上に試算表が放置してある、通路などに書類が詰まった段ボールが積み上げてある、といった状態は不適合理由となる可能性があります。机の引き出しや書棚の施錠管理も事故を防ぐ第一歩です。サイバー攻撃はネットワークから電子的に侵入して行われるものだけではありません。内部の人による情報流出以外にも、警察官を騙る詐欺電話などで従業員や役員を騙す手法もみられます。印刷物から個人情報の漏えいや金銭被害につながる危険性も考えておきましょう。

②クラウドサービス（SaaS）の管理外利用と権限管理

個人で勝手に導入したチャットツールや共有フォルダなどの管理外（野良）ITが頻発しがちです。退職者のアカウントや契約終了した顧客のアクセス権を放置せず、定期的なアカウントの棚卸しを行う運用が望ましいでしょう。

③職員のITリテラシーの格差と利便性の衝突

多要素認証の導入などに対し、職員から業務スピードが落ちるという不満や反発が出がちです。単にルールを押し付けるのではなく、漏えい時のリスクを説明する職員研修をセットで行い、理解を得ることをおすすめします。

④兼務IT担当者の限界

通常業務の傍らでIT担当を兼務しているケースが多く、専門的な知識や対応時間が不足しがちです。社内ですべてを対応しようとせず、外部のITベンダーやセキュリティ専門家の活用も検討すると良いでしょう。

(5)SCS評価制度の活用が想定される実務シーン

①取引継続や新規獲得の条件になりうる

上場企業や公共調達に絡むクライアントは将来、★3や★4を取得している企業をよりリスクが少ない取引相手と判断し、健全な財務状況などと同じような評価材料にしていくことが考えられます。

②個別セキュリティ調査対応の負担軽減

現在、クライアントごとに異なる書式でセキュリティ調査票が届き、それらの対応に多くの時間が割かれているとすれば、本制度が普及すれば「当事務所は★3を取得しています」といった公的な証明を説明の共通土台として活用でき、個別対応の負担を軽減できる可能性があります。

③セキュリティに強い中小企業・会計事務所としてのビジネスチャンス

SCS評価制度の対応経験を通じてノウハウを蓄積することにより、クライアントの中小企業に対して「SCS評価制度の★取得支援」のような新たなコンサルティングサービスを提供していく展開も考えられます。

(6)SCS評価制度の対応有無により取引先として選別される可能性について

2026年4月27日に経済産業省より「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」とする文書がリリースされています。「SCS評価を取得していな

いと商取引が規制される」「今すぐ評価を取得しないと入札から除外される」といった業者の営業活動による、製品・サービスの勧誘が報告されているとのことです。

SCS評価制度は、発注者と受注者の間でセキュリティ対策の実施状況を確認しやすくすることを想定した任意の制度です。個社間の商取引に関し国が規制措置を講じるものではありません。また、SCS評価制度の評価基準を達成するにあたっては、機能の要件はあっても、特定のセキュリティ対策製品の導入が必須とされているものではありません。

2026年1月に施行された中小受託取引適正化法（取適法、旧下請法）では、発注側の優越的地位を利用した中小受託事業者への不当な要求が禁止されています。この点からも、SCS評価制度には慎重な運用が求められるでしょう。

4 会計事務所や中小企業は、いつから何に取り組むべきか

(1)スケジュール

経済産業省およびIPAが発表している制度スケジュールは、**図表４**のとおりです。2025年４月から実証事業が始まり、2025年12月に制度構築方針（案）が公表され、2026年３月に制度構築方針が公表されました。2026年８月頃には運用規程などが公表される予定です。制度の開始時期は2026年度末（2027年３月末）が予定されています。

会計事務所が新しいことに取り組むときの一番の壁は、確定申告期、企業決算期などの繁忙期です。時間が比較的確保しやすい時期を大切に使いましょう。

(2)取り組むべきこと

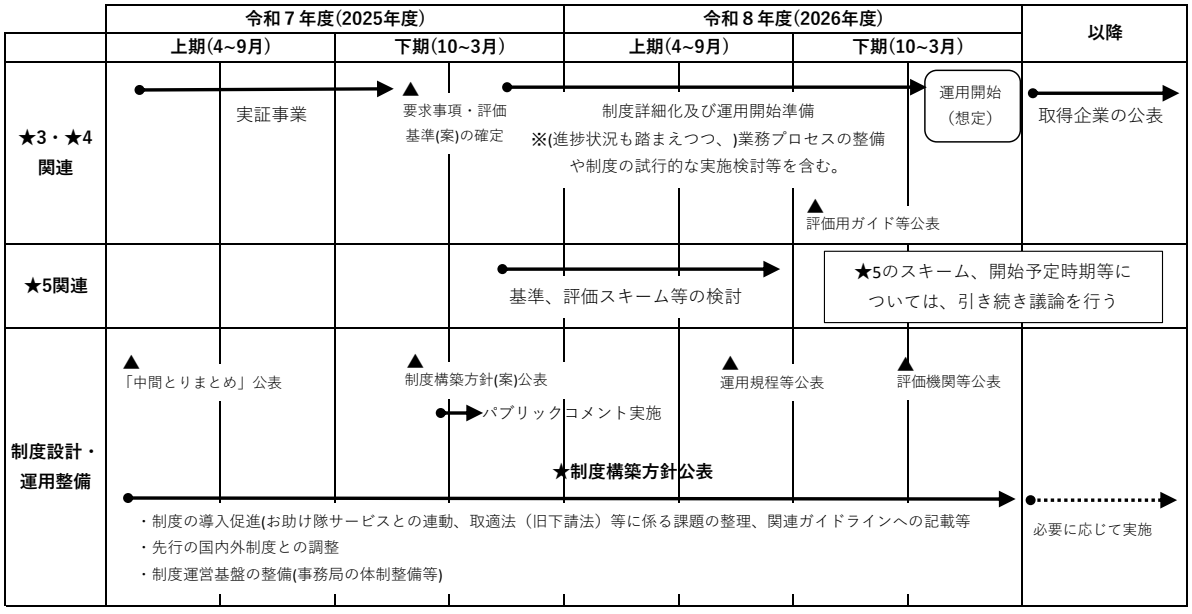
①現状把握とレベル設定：今すぐ（2026年中盤）

IPAのSECURITY ACTION（★２）の対応状況を確認し、将来的に専門家による確認が必要な★３または第三者評価が必要な★４の取得を見据えた計画を立てましょう。

②IT資産の棚卸しとルール化：2026年夏～秋

前掲の**図表３**に示すような情報資産管理台帳を作り、社内・事務所内のPC、スマートフォン、使用している全クラウドサービスなどを洗い出します。この作業は、業務や使用実態を把握している企業組織内部の人の主体的な関与が欠かせないうえに、情報を網羅するためにはある程度の期間が必要なため、早期に着手したい作業です。台帳の項目のうち「⑨評価値」の重要度は後ほど専門家のアドバイスを受けてから記入しても良いでしょう。並

図表 ４　制度運用のスケジュール



出典：「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」令和 8 年 3 月、
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サプワーキンググループ 事務局

行して、社内・事務所内のIT環境でSCS評価制度の対応に不足する機器などを見積もり、調達を検討します。必要であれば、公的支援制度や補助金の活用と合わせた金融機関への相談も行いたいところです。また、ファイルサーバの共有フォルダなどに設定しているアカウントやアクセス権限を見直し、PCやサーバのソフトウェアアップデートなどの防御を行いましょう。

③SCS評価の取得と取引先対応：2026年秋～冬

自己評価に向けた準備や不足項目の是正、専門家への相談などを進め、申請受付開始後に登録申請を行いましょう。

5 ★3や★4の取得にあたっての公的支援制度

これまで述べてきたように、SCS評価制度の★3や★4取得には、社内ルールの見直しや管理を徹底するとともに、IT機器やネットワークなどのセキュリティ強化も必要となるかもしれません。しかし、「対応したいけれど、何をすれば良いかわからない」という中小企業・会計事務所の方もおられるのではないでしょうか。そこで、SCS評価制度に基づくセキュリティ対策を中小企業・会計事務所でもスムーズに実施できるよう、新たな支援策が検討されています。

たとえば、「サイバーセキュリティお助け隊サービス」という、国が認定した民間事業者のサービスがあります。現行のサービスでは、24時間の異常監視、緊急時の駆け付け支援、相談窓口の設置、簡易サイバー保険などの基本的なセキュリティサービスがワンパッケージで、かつ、安価（例としては月額1万円以内）で提供されています。さらに、中小企業がSCS評価制度の★3及び★4を安価かつ簡便に取得できるよう、新たな支援策として「サイバーセキュリティお助け隊サービス」（新類型）が創設される予定で、詳細は今後具体化される見込みです。2026年8月頃から実証事業が開始し、2027年3月末頃のSCS評価制度開始に合わせて、新類型サービスの基準案を公表し、先行版としてサービスインされる予定です。

独立行政法人中小企業基盤整備機構により採択されるデジタル・AI導入補助金「セキュリティ対策推進枠」では、所定の要件を満たし採択された事業者を対象として、最大150万円まで、中小企業は導入費用の1/2（小規模事業者は2/3）の補助を受けられます。

6 経済的視点からのレジリエンス

SCS評価制度の説明において、「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に関する制度構築方針」などでは「レジリエンス」という言葉が用いられています。防災の分野などで使われてきた言葉で、困難やストレス、被災などから「しなやかに回復し、適応する力」を意味します。レジリエンスは際限なく強くすれば良いのではなく、費用対効果から導かれる最適な施策が求められます。たとえば、大津波に耐えられる高い堤防を作る費用と、津波が届かない場所まで建物などを移転する費用とその効果とを比べ、どの方法でどこまで対応すべきか最適判断を下すことです。

サイバーセキュリティにも同じことが言えるでしょう。セキュリティ機器やサービスにどこまで投資するのか、そもそも機密情報をそこで保管することが適切なのか。これらを検討するためには、十分に網羅された情報資産管理台帳が重要です。情報資産管理台帳の内容は持続的に更新し、実態と一致した資料として維持していくことで、管理の精度向上やセキュリティ対策の適切な運用につながります。地味に根気の要る作業ですが、企業規模や業種に関係なく、多くの企業にとって整備しておきたい資料です。レジリエンスの本質はここで決まります。情報資産管理台帳をもとに、SCS評価制度の★取得に向けて動きやすくなり、取引先との信頼関係構築やサプライチェーンの安定化につながるでしょう。

セキュリティ対策のため新たなIT機器やサービスを導入する際は、企業の身の丈に合ったものを選ぶことをおすすめします。公的支援制度により費用を抑えて高度な対策を打てたとしても、それらを導入して終わりではありません。翌年以降に

も運用費やセキュリティ警告に対応する時間を要します。だからこそ、長期を見据えて自社が運用できる範囲の投資が大切です。

SCS評価制度の活用により、多くの企業でサイバー攻撃に屈しない体制が整い、サプライチェーン全体のレジリエンス向上につながることを期待します。本稿が、SCS評価制度への理解を深め、ポイントを押さえていただく一助になれば幸いです。

参考文献

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（SCS評価制度）、独立行政法人 情報処理推進機構（IPA）
https://www.ipa.go.jp/security/scs/index.html
2）「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」報告書について、独立行政法人 情報処理推進機構（IPA）
https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html
3）「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 8 年 3 月、警察庁サイバー警察局
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf
4）中小企業の情報セキュリティ対策ガイドライン、独立行政法人 情報処理推進機構（IPA）
https://www.ipa.go.jp/security/guide/sme/about.html
5）SECURITY ACTION、独立行政法人 情報処理推進機構（IPA）
https://www.ipa.go.jp/security/security-action/
6）サイバーセキュリティお助け隊サービス（新類型）、経済産業省
https://www.meti.go.jp/policy/netsecurity/otasuketai_jissho.html
7）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、経済産業省
https://www.meti.go.jp/policy/netsecurity/20260427_scs.html
8）「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」、令和８年３月、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サブワーキンググループ事務局
https://www.meti.go.jp/files/900017305.pdf
9）「『レジリエンス社会の実現』に向けた産業政策の方向性」、経済産業省 経済産業政策局
https://www.meti.go.jp/shingikai/sankoshin/shin_kijiku/pdf/014_06_00.pdf

● MEMO ●

● MEMO ●

● MEMO ●

［執筆者紹介 ］

上ヶ平　裕彦
（かみがひら　ひろひこ）

税経システム研究所 客員講師　上ヶ平 IT 事務所 代表
IT コーディネータ、情報処理安全確保支援士、上級ウェブ解析士
沖電気工業で開発技術者として勤務。その後、誠文堂新光社やインプレスで出版編集を支援、富士通グループで SE（富士通 BSC）・コンサルタント（富士通総研）・マーケター（富士通本社）を歴任。2019 年に IT コーディネータ資格を取得、上ヶ平 IT 事務所を開業。自治体や企業の IT 支援を行っている。

※執筆者について詳しく知りたい方は MJS 税経システム研究所のページをご覧ください。
https://www.mjs.co.jp/outline/zeikei/concept/

［ 初出 ］

2026 年 8 月（No.211）

Monthly Report 特別版
サプライチェーン全体でセキュリティを考える時代へ 「セキュリティ対策評価制度」で求められる中小企業・会計事務所の対応
(No.211 より抜粋)
2026 年 9 月 1 日発行

編　集：MJS税経システム研究所
〒160-0004 東京都新宿区四谷 4-30-13 クロスシー新宿御苑前ビル 6 階
TEL：03(6626)9060
本誌の内容に関するお問い合わせは、お問い合わせフォームまでお願いいたします。
https://www.mjs.co.jp/form/zeikei_info

発行：株式会社ミロク情報サービス