

2026 年 10 月 7 日
株式会社ソフトクリエイト

「情報セキュリティ実態アンケート 2026」を公開

～ SCS 評価制度への対応が本格化、十分なインシデント対応体制を整備する企業は 1 割未満～

株式会社ソフトクリエイト（本社：東京都渋谷区／代表取締役社長：林 宗治、以下 ソフトクリエイト）は、企業・団体等の情報システム部門におけるセキュリティ対策の実態を把握するため、「情報セキュリティ実態アンケート 2026」を実施しました。調査結果をまとめたレポート「数字で見る情シスとセキュリティ対策 2026」を、情報システム部門向けメディア「情シスレスキュー隊」で公開しました。

本調査から、セキュリティインシデントを経験した企業は 37.1%にのぼる一方、対応手順や復旧手順を整備し、訓練まで実施している企業は 7.6%にとどまることが明らかになりました。

また、2027 年 3 月頃の運用開始が予定される「SCS 評価制度」について、「準備を進めている」企業は前回調査の 8.3%から 18.7%へと 2 倍以上に増加しており、企業の関心が情報収集から具体的な対応へ移りつつあることも示されました。

◆調査概要

調査期間：2026 年 6 月 22 日（月）～ 2026 年 7 月 6 日（月）

調査方法：自社ハウスデータベース上でのオンラインパネル調査

調査対象：Web メディア「情シスレスキュー隊」のメルマガ購読者で自社の IT システム運用に関与する方
回答者数：523 名

調査企画/実施：株式会社ソフトクリエイト

調査結果資料：<https://www.softcreate.co.jp/rescue/document/detail/security-survey-report-2026>

◆サマリー



エグゼクティブサマリー

総 評

- 7 割の企業でセキュリティ対策は「情シスが主導」、人材・知見不足は 4 割台
- 4 割弱がインシデントを経験、その対策レベルは 7 割が「レベル 1～2」で足踏み
- 6 割がシステム導入前からセキュリティ対策、役割・責任は“情シス任せ”が 5 割
- SCS 評価制度「準備を進めている」は 8%から 19%へ。半年で 2 倍超に

◆4 割弱がインシデントを経験、十分な対応体制を整備する企業は1割未満

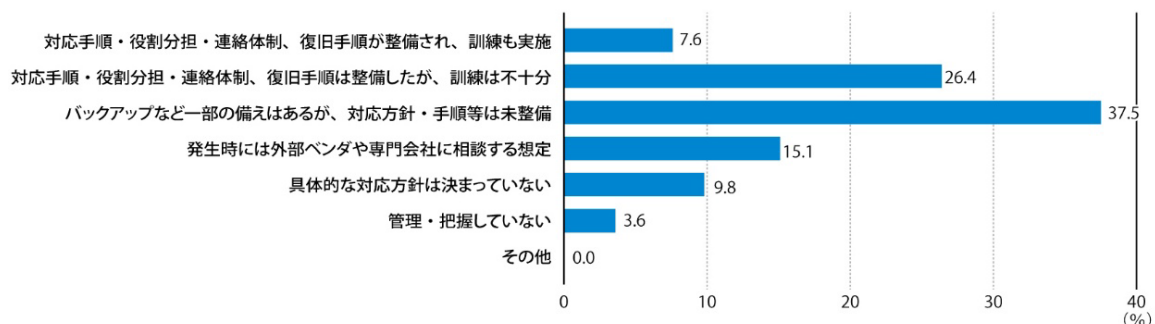
セキュリティインシデントを「経験あり」とした企業は37.1%でした。経験した内容は、「クライアントPCのウイルス感染」(49.0%)が最多で、「サーバ・社内システムのウイルス感染・不正アクセス」(26.3%)、「ランサムウェア攻撃」(25.8%)が続きました。

インシデントによる被害で特に不安を感じる点としては、「重要データや業務システムが利用できなくなる」とが最も多く挙げられました。端末の感染にとどまらず、サーバや社内システムへの攻撃、ランサムウェアによる業務停止が現実的なリスクとして認識されていることがうかがえます。

一方、インシデント発生時に備え、「対応手順・役割分担・連絡体制、復旧手順が整備され、訓練も実施」している企業は7.6%にとどまりました。被害への不安が広がる中、手順や体制を定めるだけでなく、訓練を通じて実効性を高めることが課題となっています。

「訓練も実施」している企業は1割未満、「備えあり」の中身はバックアップなど一部のみ

セキュリティインシデントにより被害が発生した場合の対応について

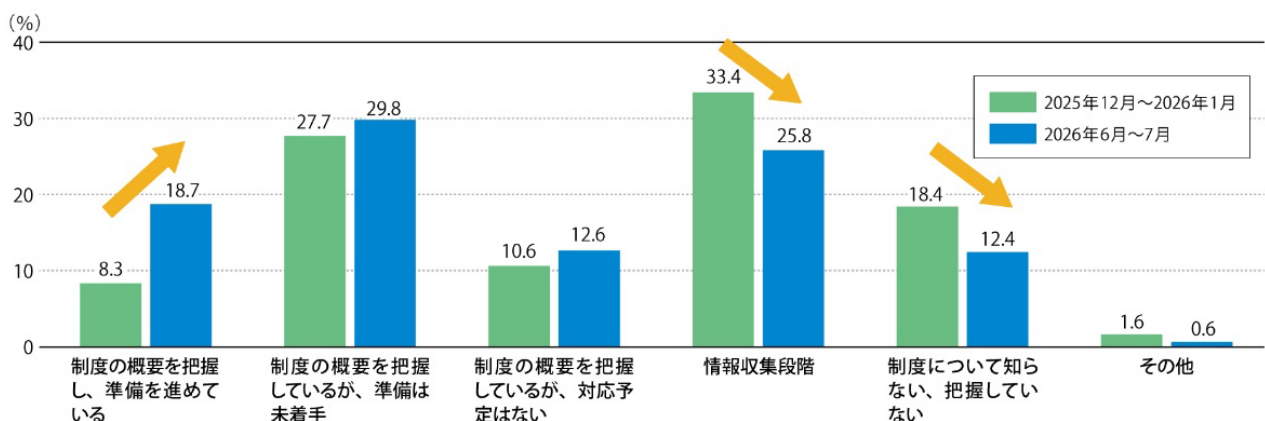


◆SCS 評価制度「準備を進めている」は半年で2倍超、対策レベルによって準備状況に差

2027年3月頃に運用開始が予定されている「SCS 評価制度（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、「制度の概要を把握し、準備を進めている」企業は、前回調査（2025年12月～2026年1月）の8.3%から18.7%へと2倍以上に増加しました。「情報収集段階」は33.4%から25.8%、「制度について知らない、把握していない」は18.4%から12.4%へと低下しており、企業の関心が情報収集から具体的な準備へ移り始めていることがうかがえます。

SCS 評価制度への理解・準備が進む、「準備中」の企業は約半年で2倍以上に

経済産業省の「SCS 評価制度」に向けた対策状況（年次推移）

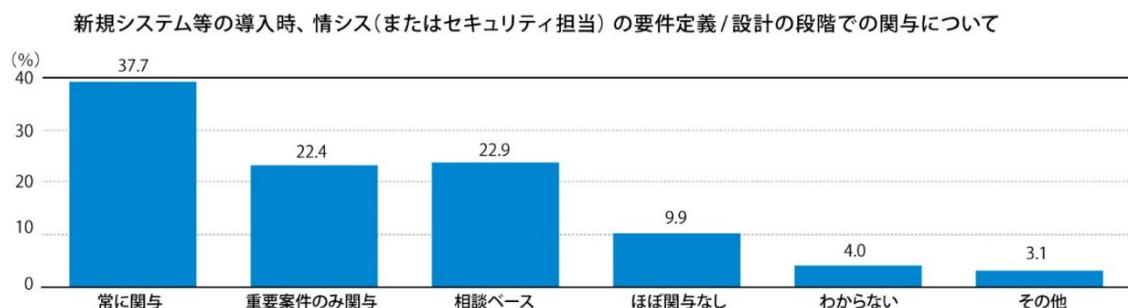


◆6 割がシステム導入前からセキュリティを検討、役割・責任は過半数が「情シス任せ」

新規システム等の導入時に、情シス（またはセキュリティ担当）が要件定義・設計段階から関与している企業は、「常に関与」と「重要案件のみ関与」を合わせて 60.1%となりました。「相談ベース」も含めると 8 割超の企業で、何らかの形で上流工程からセキュリティの検討に関わっています。

上流工程からセキュリティを検討する企業が増える一方、役割や責任の所在は依然として情シスに偏っており、組織横断で取り組む体制整備が課題であることが明らかになりました。

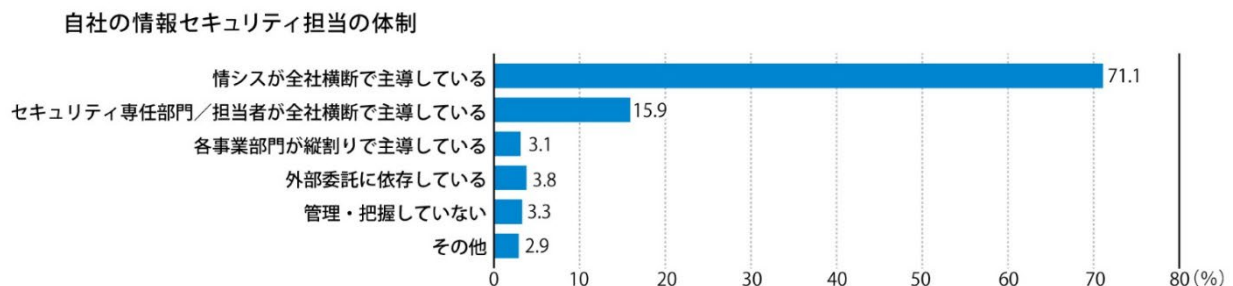
新規システム等の導入時に、情シスまたはセキュリティ担当が「常に関与」は 4 割



◆7 割の企業で情シスがセキュリティ対策を主導、課題は「専門知識」「人材」の不足

セキュリティ対策の担当体制は、「情シスが全社横断で主導している」が 71.1%と突出し、「セキュリティ専任部門／担当者が全社横断で主導している」の 15.9%を大きく上回りました。一方、体制・運用面の課題では「自社内のセキュリティに関する専門知識や知見が不足している」（45.7%）、「セキュリティ対策できる体制・人材・リソースが無い」（43.6%）が上位を占め、「最新の脅威への対応ができない」（33.7%）、「緊急時の対処、インシデント対応について対応フロー等の準備ができていない」（32.1%）も前回から増加しました。少人数の情シスがセキュリティ対策の中心を担う中、専門知識や人材の不足、新たな脅威への対応に課題を抱えている実態がつかえます。

セキュリティ対策は「情シスが全社横断で主導」が 7 割



◆全ての調査結果は、以下調査結果資料よりご覧いただけます。

数字で見る情シスとセキュリティ対策 2026

[情報セキュリティ実態アンケート 2026 調査結果の概要]



URL :

<https://www.softcreate.co.jp/rescue/document/detail/security-survey-report-2026>

<調査項目概要>

- ・エグゼクティブサマリー
- ・情報セキュリティ対策の現状について
- ・セキュリティインシデントへの取り組みについて
- ・セキュリティ対策を意識したシステム設計について
- ・外部評価・認証・ガイドラインについて

◆「情シスレスキュー隊」について

株式会社ソフトクリエイイトが運営する情報システム担当向けのメディア。情シスを中心に、情報システムを扱う中小企業の担当者の悩みを解決するメディアサイトです。生成 AI をはじめ、IT インフラ、システム運用、セキュリティなど幅広いテーマを取り扱います。

URL : <https://www.softcreate.co.jp/rescue>

■株式会社ソフトクリエイイトについて

ソフトクリエイイトは、お客様の変革に不可欠なベストパートナーを目指し、企業向けの総合的な IT サービスを提供しています。クラウド、セキュリティ強化、AI・DX 支援、IT インフラ構築を主要な事業とし、最適なテクノロジーを通じた「価値の提供」でお客様のビジネスを支援します。40 年以上にわたり、お客様と共に培った経験を生かし、日本全国の企業へサービスを届けていきます。

<会社概要>

会社名：株式会社ソフトクリエイイト

代表者：代表取締役社長 林 宗治

設 立：2012 年 10 月

資本金：2 億円（2026 年 3 月 31 日現在）

所在地：〒150-0002 東京都渋谷区渋谷 2-15-1 渋谷クロスタワー

U R L : <https://www.softcreate.co.jp/>

※ 記載している会社名、商品名は各社の商標または登録商標です。



SOFT CREATE

進化し続ける IT、明日も未来も一緒に。

株式会社ソフトクリエイイト

SOFTCREATE CORP.

〒150-0002 東京都渋谷区渋谷 2 丁目 15 番 1 号 渋谷クロスタワー

■プレスリリースについて

企画統括部 佐藤

Tel : 03-3486-1520

Mail : sc-contact@softcreate.co.jp