

経産省 **SCS評価制度** の全体像と実務対応

情報システム部門が今取り組むべきアクションとは



会社概要

社名	株式会社NSD
設立	1969年4月8日(昭和44年4月8日)
資本金	72億5百万円
従業員数	4,555名(連結)(2026年3月末日時点)
業務内容	システム開発事業 (1) ITコンサルティング (2) システムの企画・設計・開発 (3) ITインフラの構築 ソリューション事業 (1) ITを利用したサービスの提供 (2) ソフトウェア・プロダクトの販売
上場取引所	東京証券取引所 プライム市場
売上高	117,813百万円(連結)(2026年3月期)
事業所	東京(本社)、大阪、名古屋、福岡、札幌、仙台、広島



PMI®ATPロゴは、Project Management Institute, Inc. の登録商標です。



本日のゴール

お持ち帰りいただきたい3つのこと

01

SCS評価制度の全体像を掴む

なぜ今この制度が生まれるのか。何が評価され、いつ始まるのか。

02

★3／★4で求められる対策を理解する

44項目の構造と「3つの観点(経営／SC防御／IT基盤)」を整理。

03

情報システム部門として何から着手すべきかを決める

今すぐやること／余裕があれば／様子見、を切り分けてお持ち帰り。

PART 1

SCS評価制度とは何か

背景・目的・スケジュール

なぜ今、この制度なのか

サプライチェーン経由のサイバー攻撃が「他人事」ではなくなった



問題の所在

委託先・取引先を踏み台にした攻撃が急増。

ある情報処理サービス企業の事例では、ランサムウェア感染をきっかけに、自治体・大手メーカーなど複数の委託元へ被害が拡大(最大103万件規模の情報漏えい)。

「自社だけ守る」では取引が守れない時代に。



制度の狙い

経済産業省が主導する任意の評価制度。

サプライチェーン上の各社のセキュリティ対策状況を「★」で見える化し、取引時の共通基準として機能させる狙い。

業種横断で活用できる「ものさし」を作り、全体の底上げを目指す。

★3～★5の3段階評価

★4が標準的な目標。中心となるのは★3・★4。

正式名称: 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)

★3 Basic

最低限満たすべき基準

自己評価(専門家確認あり)

有効期間: 1年

基礎的な組織対策とシステム防御。
「土台を示す」段階。

★4 Standard

標準的に目指すべき基準

第三者評価(文書+実地+技術)

有効期間: 3年

ガバナンス・取引先管理・多層防御・
検知が動いている段階。

★5 Advanced

重要インフラ向け(検討中)

詳細は2026年度以降に検討

ISMS等との整合性も考慮

国際規格ベースのベストプラクティス。
当面は様子見でOK。

制度スケジュール

2027年3月頃の運用開始へ。準備期間は実質1年弱。



「様子見」できる猶予は、事実上あと半年～1年。

★4の対策実施には相応の準備期間が必要。制度開始後に動き出してからでは間に合わない可能性が高い。

PART 2

制度で求められる対策の中身

7分類・44項目を3つの観点で整理する

対策は「7分類・44項目」で構成

NIST CSFの6機能 + 取引先管理 という整理

NIST CSF ベース: 6機能

- ① ガバナンスの整備
- ③ リスクの特定
- ④ 攻撃等の防御
- ⑤ 攻撃等の検知
- ⑥ インシデントへの対応
- ⑦ インシデントからの復旧



SCS制度独自: 取引先管理

② 取引先管理

サプライチェーンを構成する企業同士で「誰と、何を、どう」やり取りしているかを可視化・把握することを求める分類。

本制度の「肝」となる部分。

★3と★4の違いを「3観点」で整理する

★3＝土台を示す段階、★4＝具体的対策が動いている段階

	★3(Basic)	★4(Standard)
① 経営の責任	組織体制の基礎構築／IT資産の可視化	リスク対策体制の構築／IT資産の課題是正
② サプライチェーンの 防御	管理方針の明確化(ルール策定)	サプライチェーンの状況を可視化・把握
③ IT基盤の防御	基礎的な防御策(ID管理・パッチ等)	多層防御・異常検知(暗号化・分離・ログ分析)

★3は「姿勢・土台」を示す段階／★4は「具体的な対策が実際に動いている」段階

制度の「肝」—— 取引先管理(★4)

★4ではサプライチェーン全体の可視化が必須条件

①



誰と・何を・どう やり取りしているか

(No.8)取引先リスト+通信手段+情報資産の一覧化

例:受発注EDI/メール/ファイル共有/API連携

②



重要取引先のセキュリティ対策状況を把握

(No.10)年1回以上、対策状況を確認(アンケートベースで可)

例:チェックシート回答受領/訪問点検/認証取得状況確認

③



インシデント時の役割・責任を明確化

(No.11)通知義務/緊急連絡先/再発防止策の協議方法を文書化

例:契約書・覚書への反映/CSIRT連絡フロー整備

PART 3

制度はどこまで決まったのか

2026年3月:「案」から「確定版」へ

確定した点と、まだ流動的な点

確定した部分から動き始めるのが現実的



確定(動いてOK)

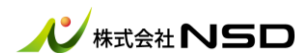
- ★3／★4の要求事項・評価基準
- 評価取得の基本フロー・審査日数
- 適用範囲:IT基盤(クラウド含む)
- 対象外:OT／提供製品
- 有効期限:★3=1年／★4=3年
- 制度開始時期:2027年3月頃



流動的(様子見でOK)

- ★5の要求事項・評価基準
- 評価機関の具体的なリスト
- 審査費用の相場(市場形成前)
- ISMS等との相互認証
- 評価ガイド(2026年秋頃公表予定)
- ★4評価機関の指定(2026年12月頃)

確定版(2026年3月)で具体化したポイント



具体化したポイント5点をピックアップ



制度開始時期

2027年3月頃の運用開始想定。準備期間は1年を切っている。



評価取得フロー

★3は自己評価＋専門家確認、★4は文書確認＋実地審査＋技術検証。



適用範囲(IT基盤)

サーバー群／エンドポイント／NW境界／クラウドが対象。
OT・未接続機器は対象外。



要求事項の見直し

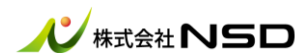
★3から復旧対策が必須化(バックアップ等)。NIST CSFと整合性確保。



中小企業支援

サイバーセキュリティお助け隊サービス(新類型)で★3取得を支援。

パブコメ：現場からはこんな声



93者から569件。「実務寄り」の意見が中心。

93

意見提出者(社)

569

意見総数(件)

負担への懸念



「監査対応・証跡準備の負担が大きい。中小企業には対応が困難」

制度運用への懸念



「取引条件として過剰要求される可能性。優越的地位の濫用にならないか」

制度設計への要望



「ISO/ISMS等との重複を避け、整合性を確保してほしい」

PART 4

情報システム部門は、今から何をすべきか

やること・やらなくていいこと の見極め

情シス部門が直面する5つの実務論点

どれも「他人事」ではなく、情シスが旗振り役になる

01



IT資産の棚卸し

★3・★4の評価範囲を決めるため、クラウド・リモート環境含めて漏れなく把握

02



スケジュール把握と経営報告

申請受付:2027年3月頃。評価ガイド公開:2026年秋頃。逆算で計画

03



★3「専門家確認」の手配

登録セキスぺ等の社外専門家確認が必須。社内担当者だけでは取得不可

04



取引上の立場に応じた方針整理

発注側／受注側で動き方が違う。法務・調達との連携が前提

05



統制点の整備(クラウド・ID・ログ)

★4想定を検知・対応体制づくり。ID管理・ログ監視・異常検知

優先度で整理する3つのレイヤー

全部を一気にやる必要はない。確定領域から

すぐやる

1～3ヶ月以内

- 現状のギャップ分析
(★3／★4要求事項との差分)
- IT資産台帳の整備
(エンドポイント含む全資産の棚卸し)
- 経営層への報告・予算確保の相談
- 関係部門(法務・調達)との連携体制構築

余裕があれば

3～6ヶ月以内

- 取引先管理プロセスの設計
(評価基準・質問票)
- ログ取得・保管体制の見直し
- インシデント対応手順の文書化
- 復旧目標(RTO／RPO)の設定

様子見

制度確定後に対応

- ★5への対応検討
(要求事項が未公表)
- 評価機関の選定・審査依頼
(認定プロセス進行中)
- 高額コンサル契約
(制度詳細が固まってから)
- 他制度との相互認証対応

今は「頑張りすぎなくていい」こと

オーバースペックな投資・対応は、むしろ実務を圧迫する



未確定領域への先行投資

★5の対応や評価機関選定など、制度詳細が固まる前の高額契約は避ける。



認証取得そのものの目的化

目的は「取引継続」。★の取得は手段。まず「説明できる状態」を作ることが先決。



全取引先への一律要求

全委託先に★4を一律要求すると現場が崩壊。重要度・機密情報の有無で段階的に。



完璧主義の追求

100点を目指すより、80点で早く形にして、運用しながら改善の方が実務的。

最初の一步は「現状把握」

やみくもに対策する前に、ギャップを見極める



自社は今、★3・★4の要求事項のうち、どこまで満たせているか？

この一問が出発点。漠然と「セキュリティ強化」と言っても、何をどこまでやるべきかは決まらない。

ギャップ分析でわかること



適用範囲の確定

IT基盤・組織・対象システム
の線引き



7分類別の充足度

44項目に対する自社の現在地



課題と対応コスト

優先度・難易度・工数の試算



ロードマップ

★4取得までの現実的なスケ
ジュール

本日のまとめ

1

制度は「構想」から「実装」フェーズへ

2027年3月開始想定。準備期間は1を切った。今から動く必要がある。

2

目指すのは「説明できる状態」

認証取得そのものではなく、取引継続のための体制構築。完璧より80点で早く形に。

3

情シス単独では完結しない全社プロジェクト

法務・調達・事業部門との連携が必須。経営層への報告と予算確保を早期に。

まずは「現状ギャップ分析」と「IT資産台帳の整備」から着手を

ちょこっただけ宣伝させてください！

よろしくお願いします



経済産業省 SCS評価制度 情報セキュリティアセスメント



まずは、お気軽にご相談ください。

株式会社NSD
市場開拓事業部
SCS評価制度アセスメント担当
products@nsd.co.jp

制度開始は令和8年度末頃 — 今すぐの現状把握が鍵

★3・★4の対策実施には相応の準備期間が必要です。制度開始後の対応では間に合いません。
早期のアセスメントで、計画的な取得を実現しましょう。

アセスメント サービス内容

SERVICE DETAILS

① 現状評価・ギャップ分析

- ▶ 事前資料確認(規程・体制図・NW構成図等)
- ▶ 関係者ヒアリング(経営層・IT担当・業務担当)
- ▶ 要求事項との照合(★3:26件 / ★4:43件)
- ▶ 適用範囲の確認(IT基盤・組織・システム)

② 課題整理と改善提案

- ▶ 不足点・不適合リスクの洗い出し
- ▶ 優先度・難易度・効果の整理
- ▶ 対応コスト・工数の試算
- ▶ 報告会による経営層への合意形成支援

成果物:改善提案書

適用範囲 / 7分類別充足度 / 課題一覧 / 改善提案 / マスタスケジュール / 経営層向け要約

4,000名超の技術者集団

55年以上、お客様の業務を理解し寄り添ってシステム開発を行ってきた実績と、豊富な技術者集団により最適なアセスメントをご提供いたします。

一貫した支援体制

アセスメントして終わりではなく、改善対応まで伴走可能。
製品選定から販売・導入、保守までワンストップで支援いたします。

専門資格保有者50名以上在籍

SCS評価制度に関するアセスメントサービスの提供体制として、★3認定に対応可能な登録セキスベ(情報処理安全確保支援士)が50名以上在籍しています。なお、★3認定の実施に必要な所定講習についても、順次受講・資格取得を進めていきます。

セキュリティ

Cyber Security

20年以上、セキュリティを中心とした製品を取り扱っております。

自社開発製品、国内外屈指のセキュリティ商材を発掘、
製品の販売・提供だけでなく、構築、保守サポート、
連携ツールの開発まで一貫して提供いたします。

その豊富な実績から、各メーカーのパートナーランクは最上位。

NSDはセキュリティのスペシャリストとして幅広いご提案が可能です。

お気軽にご相談ください。

- エンドポイント (NGAV・EDR・MDR)
- SOCサービス
- SASE
- モバイルセキュリティ
- メールセキュリティ
- 標的型攻撃メール訓練
- メール誤送信対策
- 特権ID管理
- ログ管理
- 内部不正対策
- 脆弱性診断
- 資産管理
- パッチ管理

etc...

お客様の幅広いニーズに対応！統合型IT資産管理ツール「SS1」



顧客満足度No. 1^{*}の統合型IT資産管理ツールです。

IT資産管理、セキュリティ対策、労務管理、運用支援・ヘルプデスク対応など、SSI独自の機能でお客様の幅広いニーズにお応えします。**オンプレ/クラウド**を選択可能なため、お客様のご要望に合わせて柔軟にご検討頂けます。機能が選べて**導入コスト**が**安価**でオプションは後から追加OK！初期投資を抑えることができます。

* ITreviewカテゴリーレポート「IT資産管理ツール」「ログ管理システム」(2024 Spring)による評価

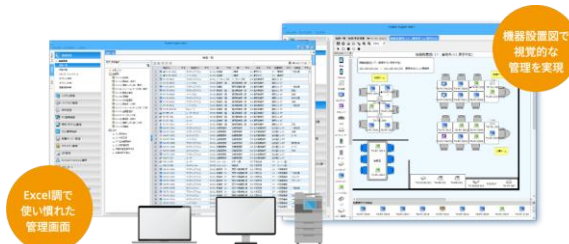
ここが“すごい”よSS1！

IT資産管理を基本とした、豊富な機能

SS1は資産管理をベースに、Windows更新管理やログ管理、リモートコントロールなど様々な機能を搭載。お客様のIT運用における課題解決をサポートします。

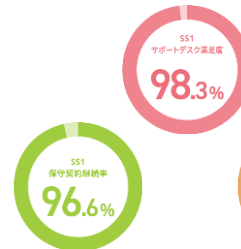


+



充実のサポート体制

お客様の環境をヒアリングし、運用開始までサポート。導入後の運用についても充実した保守サービスで、SS1のご活用を支援します。



守りすぎる最強エンドポイントセキュリティ！「SOPHOS」



導入者数 **28,000社** を突破！あらゆる第三者評価機関にて **トップクラス** の評価を獲得！

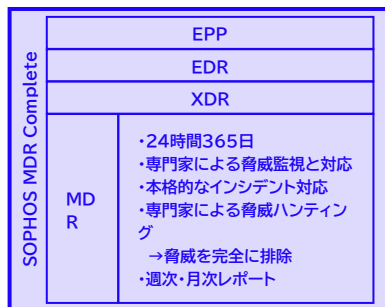
他社と比較して、圧倒的に **守備範囲が広い** 最強エンドポイントセキュリティです。

NGAV、EDR/XDR、MDR までを **オールインワン** でご提供！

必要な機能を **1ライセンス** から提供できるため、自社の運用や予算に合わせた導入が可能です。

ここが “すごい” よ SOPHOS !

- 管理者さまの負担激減！
NGAV・XDR・SOCサービス まで
オールインワン で提供



エンドポイントセキュリティに必要な機能を1ライセンスで提供

- トップクラスの評価
Gartner Peer Insights にて最高評価
MITRE ATT&CK® で指定されている攻撃の10段階すべてにおいて脅威を迅速かつ正確に検知し、対応する優れた能力があることが実証



あらゆる第三者評価機関にてトップクラスの評価を獲得。

- お客様環境との **統合！**



- NSDは **プラチナパートナー**



- サイバー保険は最大 **100万ドル** 保障

特権アクセス管理の課題はこれ1つですべて解決！「iDoperation」



11年連続シェアNo. 1^{*1} の特権アクセス管理ツール。

Administratorやrootなどの **特権アクセスを 誰が 使うのか** を **適正に管理** する製品です。
特権アクセスの貸し出しから問題発見までを自動化、企業の安全・安心、そして効率的なIT運用環境を実化します。

クラウド/オンプレ ともに対応！ **監査対応実績100%**^{*2} を誇ります。

*1：出典：富士キメラ総研「2014～2024 ネットワーク セキュリティビジネス調査総覧」（2013年度～2023年度）

*2：2012年からのNTTテクノクロス株式会社の実績

ここが “すごい” よ iDoperation !

特権アクセスに求められるすべての機能をオールインワンでご提供！必要な機能を選んで導入可能！



NSDは、iDoperation の
ゴールドパートナーです。

ご清聴ありがとうございました

まずはお気軽にご相談ください



株式会社NSD

市場開拓事業部 SCS評価制度アセスメント担当



products@nsd.co.jp