



信頼を得られる対策を語る ～SCSが求める見直しポイントとは～

2026年度 第一回 PCNW勉強会 資料

企業IT担当者のセキュリティ実態とSCS評価制度への意向（PCNW事前アンケート集計）

回答者・企業の属性（個人情報匿名化）



全社システム管理者
(18名)

62.1%

回答者の過半数(18名)が
ITインフラ・セキュリティを
一手に担う主導的立場。

全社PC管理台数



中堅・中小企業(300台以下)が半数以上(51.7%)を
占める。

セキュリティ状況とインシデント経験



自社被害
(13.8%)



取引先被害による
業務影響
(13.8%)

サプライチェーン攻撃の現実的脅威が示されている。



ISMS
(ISO27001)
取得率

24.1% (7件)



Pマーク取得率

24.1% (7件)

- ISO27017 (3.4%)
- その他/未取得 (58.6%)

外部認証未取得が過半数、新基準(SCS)への関心が高まる背景。

SCS評価制度への意識と現場の課題



SCS評価制度(2027年本格運用予定)

48.3%

取得予定・準備中

制度開始を見据え、約半数が早期対応に意欲的。

検討中・未定
(24.1%)

取得しない
(24.1%)

取引・費用への懸念



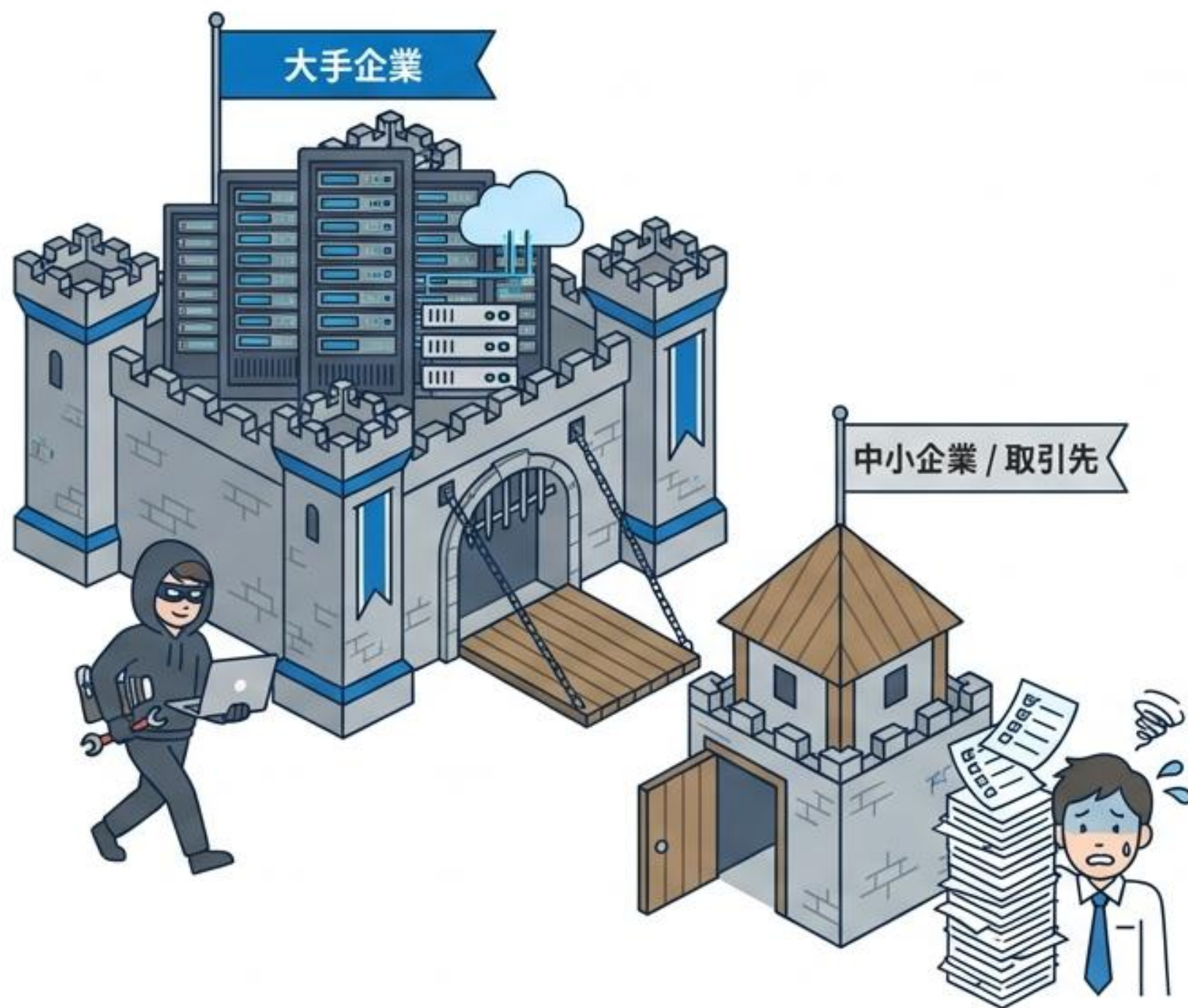
- 取引不利益(RFP除外・失注)への懸念
- 高額なコンサル費用を使わないFit&Gap分析方法の要望
- 正確な制度確定時期への不安

現場(情シス)の 3大運用課題



- ① サポート切れOS/古いNAS・機器の廃卸し
- ② IT/OT(工場系)のVLAN隔離設計
- ③ 経営陣・他部署を巻き込む推進体制の構築

なぜ今「SCS」なのか？ — 狙われるサプライチェーン



課題：

ターゲットは大企業から
「取引先（中小企業）」へ。

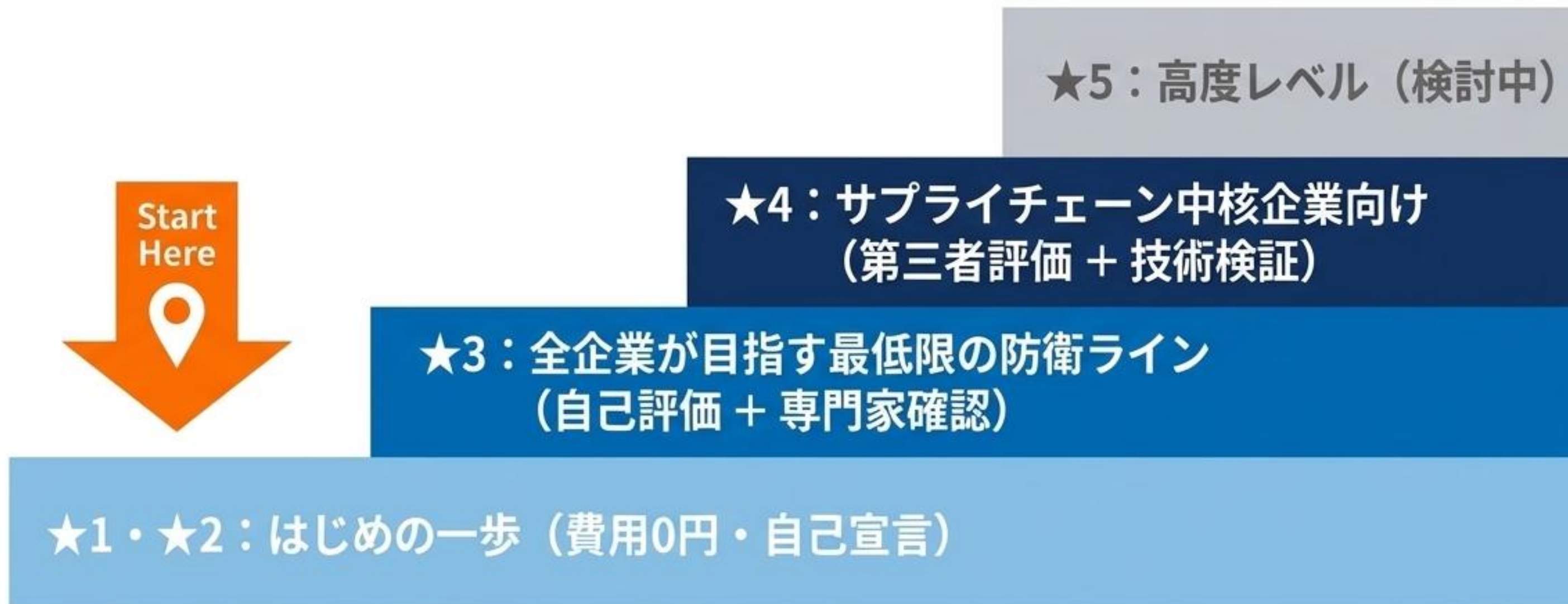
これまでの苦勞：

取引先ごとにバラバラの
セキュリティチェックシートに
回答する日々（現場の疲弊）※1

SCSの目的：

「共通のモノサシ」で対策レベルを
可視化・証明する！

SCS評価制度の全体像（★1～★5）



まずは「★2」の自社診断で、自社の抜け漏れをあぶり出す！※2

既存認証（ISMS・Pマーク）との違いと関係性

ISMS
(組織の
管理体制)

Pマーク
(個人情報)



SCS
(IT基盤の
技術的防御力
・回復力)

目的が違います：

SCSは「サイバー攻撃への技術的な
防御・回復」に特化。

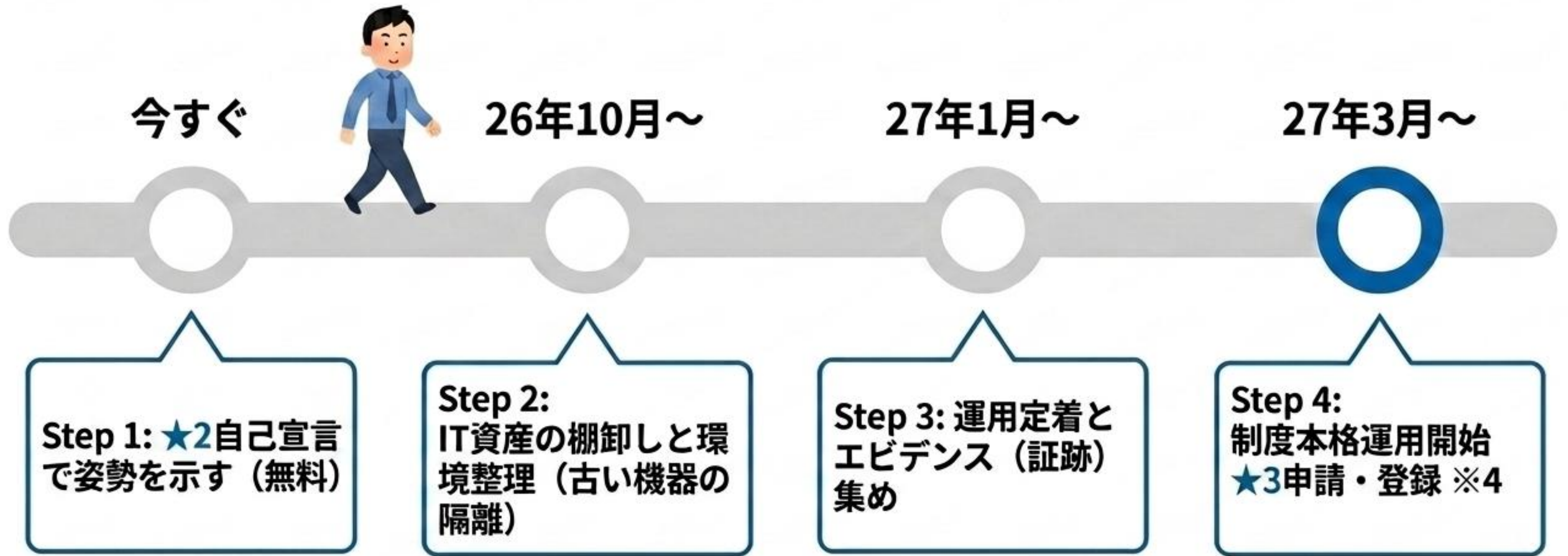
自動免除なし：

ISMS等を取得していても「みなし
取得」にはなりません。 ※3

 **ただし朗報！**

ISMS等で整備した規程・台帳は、証跡
として活用できる可能性があります。
既存認証企業は有利にスタートできます！

★3取得に向けた最短4ステップ・ロードマップ (準備が進んでいる企業の場合)



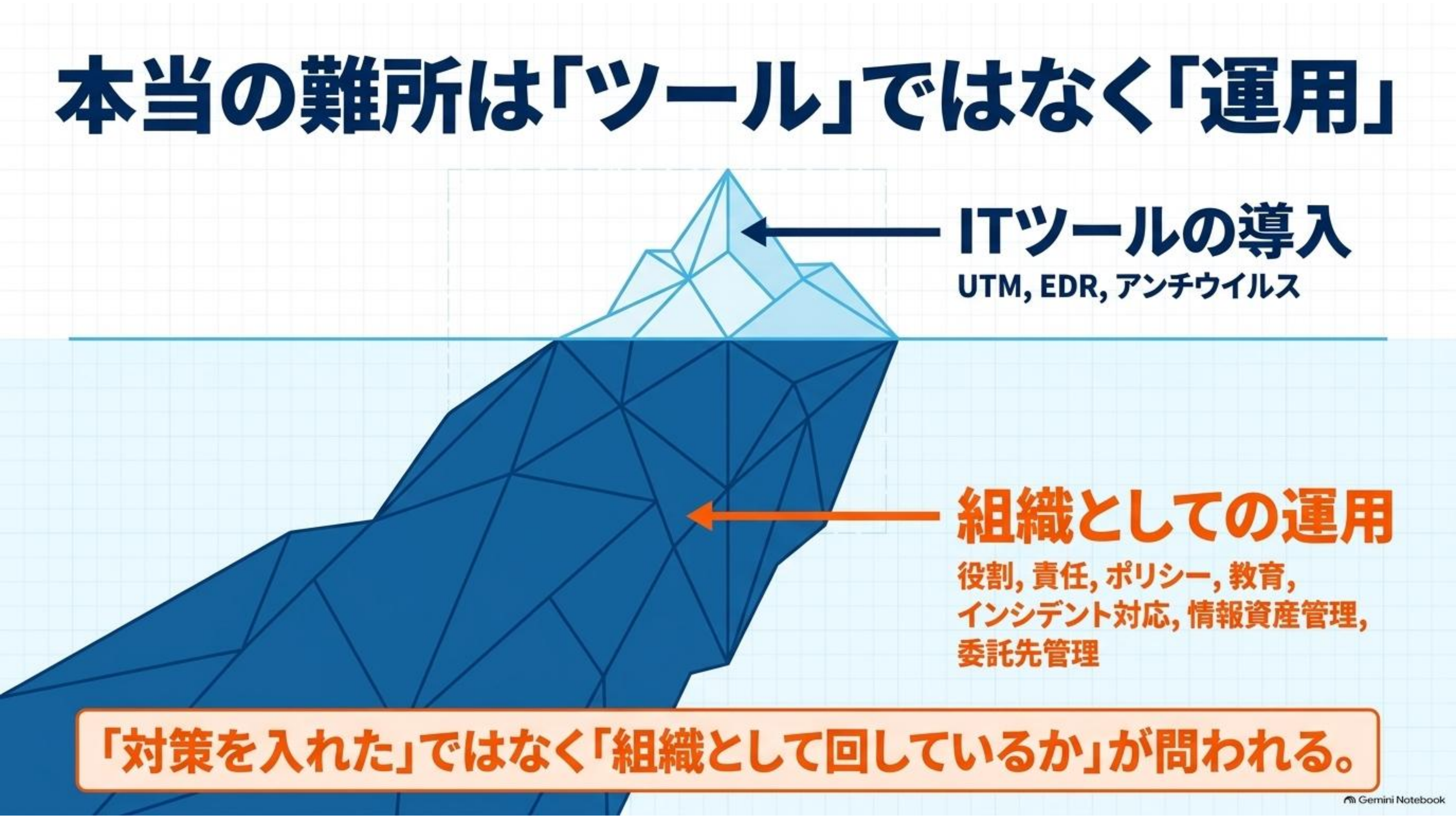
ツール導入より「運用の証拠 (ログ・台帳・設定スクショ)」を蓄積することが最大のカギ!

× 全部自社でやる ○ 主体は**自社**、一部を**専門家**



「内製化」と「専門家の活用」は両立する。
自社のことを一番よく知っているのは、自社の社員。

本当の難所は「ツール」ではなく「運用」



The diagram features an iceberg on a light blue grid background. The waterline is a horizontal line. Above the line, the tip of the iceberg is light blue and labeled 'ITツールの導入' (Introduction of IT Tools) with a black arrow pointing to it. Below the line, the much larger body of the iceberg is dark blue and labeled '組織としての運用' (Operation as an Organization) with an orange arrow pointing to it. A large orange-bordered box at the bottom contains a concluding statement in orange text.

ITツールの導入
UTM, EDR, アンチウイルス

組織としての運用
役割, 責任, ポリシー, 教育,
インシデント対応, 情報資産管理,
委託先管理

「対策を入れた」ではなく「組織として回しているか」が問われる。

セキュリティ対策ではなく 「会社の現状把握」 プロジェクト



PCは何台？

誰が管理？

ルールは？

運用状況は？

★3取得の過程こそが、会社を守る「情シスの基盤」を作る。

コンサルを呼ぶ前に「自社の現在地」を知る

「？」を潰す

(ここが最優先!)

「×」を改善する

(優先順位をつけて対応)

分類する

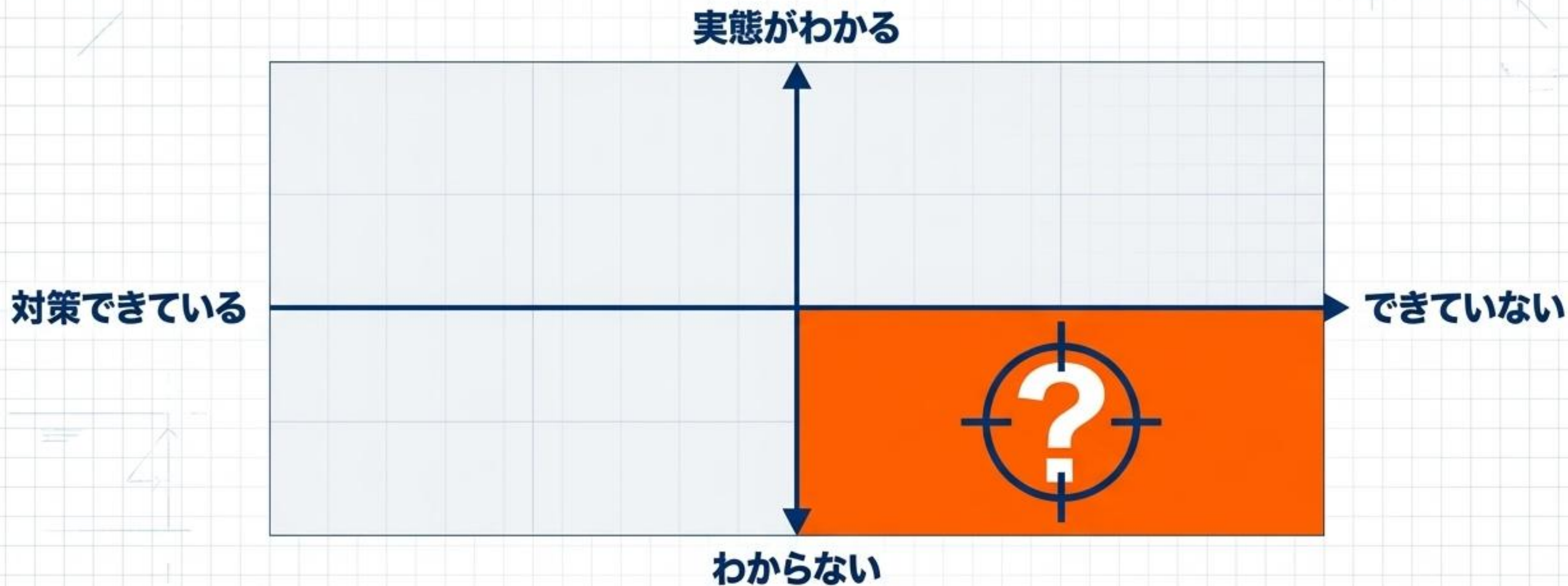
(自社を○・△・×・?に仕分け)

要求事項を読む

(現状を把握)



「わからない」を調べる過程が、最大のセキュリティ対策



「？」の実態を調べることで、台帳・ルール・責任者が自然と見えてくる。
いきなり「×」を直すより、「？」を無くすことが先決。

【ビジネスへの影響】



Q.

BtoBの中小企業ですが、★3を取らないと取引停止になりますか？

A.

即座の停止はなくても、今後の「コンペ参加条件」になる可能性大です。※5

取引先からの面倒な個別監査票への回答を「SCS登録証」でパスできるようになり、**説明コストを大幅に減らせるメリット**を取りに行きましょう。

【目標レベルの選び方】



Q.

情シスとしては、
最初から★4を狙うべきですか？

A.

基本は「まず★3」一択です。 ※6

★4は外部の脆弱性診断やログの長期保管など、費用と工数が跳ね上がります。親会社からの強い要請がない限り、まずは**全企業が最低限目指す水準の★3**を確実に取りましょう。

【IT資産の現実(レガシー機器)】



Q.

サポート切れの古いNASやOSも
評価対象に入ってしまうですか？

A.

入ります。最大の**侵入口**として
厳格に見られます。 ※7

対策は3つだけです。「①最新へ入替」「②有償ESU等でパッチ適用」「③インターネットから遮断する (さらにVLAN等で分離する)」。



Q.

社内で関心があるのは情シスだけ。
経営陣を巻き込むコツは？

A.

「ITの安全」ではなく
「受注停止リスクの回避」と
伝えてください。※8

SCSは最終的に「経営層（社長）の署名・宣言」が必要です。情シスの課題ではなく、全社的な「営業・経営課題」として予算と体制を確保しましょう。



Q.

コンサルを入れる予算がありません。
無料でできる方法は？

A.

国の「**お助け隊サービス（新類型）**」
実証事業をフル活用してください！※9

実証15事業者から自社に合うサービスを選び、
事業者へ直接連絡すれば、現状診断から規程整備、
ツール導入検討まで無償（最大1年程度）で
伴走支援を受けられます。

【ゼロスタートの現実解】



Q. 規程も運用記録もないゼロスタート企業。
明日からどう動く？

A. 今期は「★2宣言＋機器棚卸し」に
全集中してください。 ※10

運用記録がないため、半年で★3は実務上きわめて困難です。来年度の1年間をかけて
「規程策定→運用→証拠蓄積」を行い、2027年度末
の取得を目指すのが現実的な解です。

まとめ：社内稟議を通し、未来を守るために



「セキュリティのため」だけでは稟議は通らない。

SCSの本質: 単なるコストではなく
「全社的な業務効率化と安全な資産管理のための投資」です。

真のゴール: 「★3を取る」こと
ではなく、「★3を維持できる運用体制」をつくること。

情シスの使命: 何を守り、誰が、
どうやって守っているのかを「説明
できる状態」にすること。これが多
方面からの「信頼」に繋がります。

「★3を取る」のではなく、 「★3を取れる会社」をつくる

何を守るべきか。



誰が守るのか。

どうやって守っているか。



→ これを「説明できる状態」にすることが、内製化のゴールです。

※参考：2026年10月時点の公式情報に基づく 

補足説明資料 (1/3)

※1 詳細な背景

大手企業を直接狙うのではなく、セキュリティ対策が不十分な取引先（中小企業）を踏み台にする

「サプライチェーン攻撃」が激化。結果、発注元が独自のチェックシートを乱発し、受注側が対応に疲弊する「二重の課題」が発生していたため、共通のモノサシが必要となった。

※2 要求事項の構造

米国NIST CSFの6機能（統治・識別・防御・検知・対応・復旧）に「取引先管理」を加えた7分類の構造。

※3 既存認証との詳細比較

ISMSは「管理体制（マネジメントプロセス）」、Pマークは「個人情報保護」に特化。SCSはIT基盤へのサイバー攻撃に対する「技術的・組織的な防御力と回復力」を可視化する点で独自性がある。

※4 費用構造（PCNW予想）

★3の公式費用は登録料（税込1万円／年。2028年4月以降は2万円／年）のみ公表済み。専門家の確認費用は未公表。

★4は登録料6万円（3年分）に加え、第三者評価・技術検証の費用がかかる（未公表）。

補足説明資料 (2/3)

※5 ビジネスへの影響 詳細

法律上の義務を伴う制度ではないが、大手製造業、金融機関、インフラ事業者、官公庁などの調達基準やRFP（提案依頼書）の必須要件として事実上のデファクトスタンダード化する見込み。未取得は新規コンペからの排除リスクとなる。

※6 ★3と★4の具体的なハードルの違い

★4（全43要件／評価基準153件）は★3を包含する上位水準。大きな違いとして、「FW・プロキシ・認証サーバのログ6か月保管」「外部境界機器への技術検証（CVSS 7.0以上の脆弱性がないこと）」「第三者による評価（実地審査）」が加わる。

※7 レガシー機器・OT環境の扱い

工場等の制御システム（OT）や製品自体はSCSの直接の評価対象外。ただし、社内LAN（IT環境）と工場LAN（OT環境）がVLANやファイアウォールで適切に隔離され、野放しで通信できない境界制御（絶縁）ができることが前提となる見込み。

補足説明資料 (3/3)

※8 経営層の巻き込み構造

★3の取得フローは「自己評価 + 専門家確認 + 経営層の自己適合宣言」となっている。最終的に社長の署名が必要な制度構造になっているため、情シス単独のプロジェクトではなく、経営課題としてエスカレーションしやすい。

※9 サイバーセキュリティ お助け隊サービス

経済産業省とIPAが主導する実証事業。NTTデータ、リコージャパン、GMOなど主要ITベンダーが参画。現状診断（Fit&Gap）から改善計画、ITツール導入、規程整備、従業員教育、申請支援まで無償（最大1年間）でパッケージ提供される。

※10 ゼロスタートの具体的アクション

ギャップ分析（自社対策と要求事項の差分チェック）→ 対策ロードマップ策定（予算化）→ ルール整備（退職者アカウント削除やMFA適用などクイックウィンから着手）→ 運用定着（ログや証跡の蓄積）というステップを踏む。証拠蓄積には最低数ヶ月を要するため、早急な着手が必要。