WHITE PAPER ／ SCS評価制度対応

SCS評価制度対応 現在地把握ガイド

IPO準備・取引先審査・サプライチェーン強化に、"見せられる"セキュリティの現在地をつくる

ホワイトペーパー第4版（2026-07-10改訂・SecuROI）
想定読者：自社のセキュリティ体制を外部（審査・取引先・監査・投資家）に示す必要が出てきた企業の経営・情シス。IPO準備企業を主軸に、取引先要件・サプライチェーン対応の企業も対象。
※本資料の制度に関する記述は、経済産業省・IPAの公開一次情報に基づく概要です。SCS評価制度は詳細確定途上（★3・★4の解説書は2026年10月頃公表予定）のため、正確・最新の要求事項は必ず公式（IPA/METI）をご確認ください。

はじめに：きっかけは違っても、問われるのは同じ「現在地」

IPO準備、大企業や官公庁との取引先審査、サプライチェーン強化、資金調達やM&Aのデューデリジェンス――。近年、企業が「自社のセキュリティ体制を、**外部に"見せられる形"で示す**」必要に迫られる場面が、急速に増えています。

きっかけは様々でも、問われている本質は同じです。「**御社のセキュリティは今どの水準で、継続的に良くなっているか**」――つまり"現在地"と"軌跡"です。

そしてこの流れを一段押し上げるのが、国が進める **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）** です。本ガイドは、この制度の要点を整理し、**評価に備えて自社の現在地をどう把握・可視化すればよいか**を、実務目線でまとめました。

第1章：SCS評価制度とは（要点整理）

何のための制度か

SCS評価制度は、経済産業省と内閣官房国家サイバー統括室がまとめた制度構築方針（2026年3月27日公表）に基づき、**サプライチェーン全体のセキュリティ水準を底上げする**ことを目的に、IPAが運営主体となって整備が進む制度です。2社間の取引契約等で、委託元が委託先に適切な段階（★）を提示し、対策を促す・実施状況を確認する――という活用が想定されています。

★重要な位置づけ：この制度は**企業の格付けや優劣を決めるものではありません**（経産省公式資料に明記）。「委託元が委託先に求めるセキュリティ水準を共通化・可視化する」ための、共通のものさしです。

「任意」だが、"取引の条件"として求められ始める

SCS評価制度の取得は、法律で一律に義務づけられた制度ではありません。その意味では**任意**です。

しかし、ここが実務上の要点です。SCSは**「委託元が委託先に、必要な★の水準を提示する」**という2社間取引での活用を前提に設計されています。つまり――**大企業・官公庁・重要インフラ事業者などと取引を続けたい企業は、取引先（委託元）から「★3を満たしてほしい」と求められれば、事実上それに応える必要が生じます**。すでに自動車業界（自工会・部工会ガイドライン）では、サプライチェーンにセキュリティ基準を課す動きが先行しています。

自発的に取得する企業ばかりではないでしょう。むしろ多くの企業にとっては、**「ある日、取引先の審査票やRFPに"SCS★3相当"の条件が現れる」**――そこから準備が始まる、というのが現実的な入り口になります。だからこそ、求められてから慌てるのでなく、**求められる前に現在地を把握しておく**ことに価値があります。

評価の段階（★の水準）

- **★1・★2**：IPAの「SECURITY ACTION」（自己宣言）に該当。
- **★3（一般的な脅威に対処／専門家確認付き自己評価）**
  全てのサプライチェーン企業が最低限実装すべき、基礎的な組織的対策とシステム防御。**自己評価に、セキュリティ専門家の確認が加わる**方式。要求事項は26件。まず多くの中堅・中小企業が現実的な目標とする入口です。
- **★4（標準的に目指す水準／第三者評価＋技術検証）**
  組織ガバナンス・取引先管理・防御検知・インシデント対応を包括する対策に、**指定評価機関による第三者評価と技術検証（脆弱性検査・実地審査等）**が加わる。要求事項は43件。
- **★5（高度／今後検討）**
  国際規格ベースの高度な水準。スキーム・時期は引き続き議論。

上位は下位を包含しますが、**★3取得が★4の前提ではありません**。事業上の必要性に応じて目指す水準を選べます。参考として、★3・★4は自工会・部工会ガイドラインのLv1・Lv2に対応するとされ、★4はISO/IEC27001等が参照ベンチマークに位置づけられています。

いつ動くか

★3・★4は、**2026年度（令和8年度）下期に評価用ガイド等の公表を経て、運用が開始される見込み**です（申請受付開始は2027年初頃が目安とされています）。制度が本格稼働してから慌てるのでなく、**"今のうちに現在地を把握しておく"ことが、そのまま先行準備になります。**

第2章：★3は「どう」取得するのか ―― 経営と専門家が関わる自己評価

★3の「自己評価」は、「担当者が自分でチェックして終わり」ではありません。制度上、**経営層の関与と専門家の確認**が組み込まれています。取得の流れは概ね次の通りです。

1. 取得希望組織が、★3の要求事項・評価基準に基づき**自己評価を記入**する（社内外の専門家の支援を得てもよい）。
2. **セキュリティ専門家が内容を確認**し、必要に応じて助言・修正を行い、問題なしと判断したら**署名**する（この署名のない申請は受け付けられません）。
3. 取得希望組織が、**経営層による自己適合宣誓**を含め、事務局へ提出する。
4. 事務局が問題を認めなければ、企業名・所在地・適用範囲を含む情報を**台帳に登録・公開**する。

ここで押さえたい実務的なポイントが3つあります。

- **経営層が関与する**：自己適合宣誓が求められるため、★3は"現場だけの話"では完結しません。経営が現在地を理解していることが前提になります。

- **原則すべての評価基準への適合が求められる。ただし、是正の道がある**：★3は原則として、すべての評価基準への適合を求める制度です。ただし、評価の過程で不適合が見つかっても、そこで終わりではなく、**適切に是正し専門家の了承を得られれば取得は可能**です。つまり、いきなり満点である必要はなく、**現在地を正確に把握し、優先順位をつけて不足を埋め、その改善の軌跡を残していくこと**が、取得への最も確実な道になります。
- **専門家の確認が要る**：★3の確認・署名を担う専門家には、一定の資格（情報処理安全確保支援士／公認情報セキュリティ監査人／CISSP／CISA／CISM／ISO27001主任審査員のいずれか）と制度研修の受講が求められます（研修事業者の指定・公表は2026年末頃の見込み）。

第3章：なぜ「認証を持っている」だけでは足りないのか

多くの企業が、ISMS（ISO27001）やPマークを取得しています。これらは重要な取り組みですが、SCS評価制度や取引先審査の文脈では、**それだけでは答えきれない問い**が出てきます。

認証は、いわば「**ある時点で基準に適合していた**」ことを示す"点"です。しかし審査や取引先が本当に知りたいのは、"点"よりも――

- 今この瞬間、どの水準にあるのか（**現在地**）
- 前回から良くなっているのか（**軌跡**）
- その改善は、事実で裏づけられるか（**証跡**）

――という"線"の情報です。実際、認証を維持している企業でも、セキュリティインシデントは起きています。認証が形骸化し、"点"と"点"の間が見えなくなるからです。

SCS★3が「**専門家確認付きの自己評価**」で、しかも**有効期間1年（毎年更新）**という設計をとるのも、この"継続的に機能しているか"を重視する流れの表れです。企業に必要なのは「認証を取ること」に加えて、**自社の現在地を継続的に把握し、改善の軌跡を"見せられる形"で残すこと**なのです。

第4章：★3に備える ―― 現在地把握チェックリスト

制度の最終的な要求事項・評価基準は公式（IPA）に譲りますが、**★3が問う"基礎的な組織対策とシステム防御"の観点**は、IT統制（ITGC）の必須領域と大きく重なります。

★3の要求事項は、NIST CSFの6分類（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・26要求事項**で構成されます。その内訳を見ると、**「攻撃等の防御（アクセス制御・認証・データ保護など）」が13件、「リスクの特定（資産の把握）」が4件**で、この2分類だけで**26要求事項の約3分の2**を占めます。★3対策の重心は、まず**アクセス管理・認証と、資産の把握にある**――これが数の上でもはっきりしている、という点をまず押さえてください。

そのうえで、以下の観点で自社の現在地をセルフチェックしてみてください。

A. アクセス管理・認証

- ☐ ユーザーID・管理者IDの発行／変更／削除が、申請・承認に基づいて管理されているか
- ☐ 重要システムへのアクセス権が、業務上必要な人だけに絞られているか（最小権限）
- ☐ パスワードの設定・管理ルール、端末のロック制御が定められているか

B. 資産・リスクの特定

- ☐ 情報機器・OS・ソフトウェアが把握され、一覧化されているか
- ☐ ネットワークの構成（所在・用途）が把握されているか
- ☐ 情報の機密区分に応じた管理ルールがあるか

C. 防御（プラットフォーム・データ）

- ☐ OS・ソフトウェアの安全な構成（許可外ソフトの制限等）が維持されているか
- ☐ セキュリティパッチ／アップデートの適用手順があるか
- ☐ マルウェア対策・ネットワーク境界の防護が講じられているか
- ☐ 重要データのバックアップが取得・保護され、復旧の準備があるか

D. 検知・対応・復旧

- ☐ 不正な通信をリアルタイムに検知・遮断する仕組みがあるか
- ☐ インシデント対応手順（発見・初動・調査・復旧・報告）が定められているか
- ☐ 事業継続の観点で、重要システムの復旧準備があるか

E. 取引先管理（NIST6機能に加わる第7の分類）

- ☐ 取引先・子会社・クラウド提供者との接続関係が把握されているか
- ☐ 取引先との機密情報の取扱い（利用制限・返還・破棄）が取り決められているか
- ☐ インシデント発生時の、取引先との役割・責任が明確か

F. ガバナンス・継続性

- ☐ セキュリティの責任体制・対応方針が明文化されているか
- ☐ これらの対策が、一度きりでなく定期的に見直され、改善されているか
- ☐ 改善の状況が、外部に説明できる形で記録・可視化されているか

★このチェックで「△／×」が多い領域があっても、問題ではありません。★3が求めるのは完璧さでなく「**継続的に機能する体制**」だからです。現在地を正確に把握し、優先順位をつけて改善の軌跡を残す――そこが出発点です。

第5章：現在地を"見せられる形"にする ── SecuROIという選択肢

ここまでの「現在地の把握」「改善の軌跡」「見せられる形での記録」を、**IPO準備企業をはじめとする中堅企業が、無理なく継続できる**ように設計したのが、私たちのサービス **SecuROI** です。

SecuROIがすること
- 約20問の自己診断から、NIST CSF 2.0・ITGC観点で**現在地をスコア化**（NIST6機能すべてに最低1問対応する設計）。
- 四半期ごとの**改善の軌跡（トレンド）**を残す。
- 経営が投資判断に使える**1枚のサマリー**と、監査・審査が参照できる**対応表**を出力する。
- IT全般統制（ITGC）の観点で、アクセス管理・資産管理・変更管理・運用管理の現在地を示す（※変更管理は、標準の診断が基礎的なカバーを行い、IPO準備向けには補問でさらに詳しく確認する二段構えです）。

SecuROIがしないこと（正直に）
- ★**合否は判定しません。** 同業比較や、投資額の断定もしません。
- ★SecuROIは"認証"でも"証明書"でもありません。**現在地を測る"ものさし"と、経営と現場をつなぐ"共通言語"**です。SCSの適合を判定するのは、専門家の確認と事務局の役割です。

なぜこの設計なのか。審査や取引先、監査が最終的に判断する領域を、ツールが肩代わりすべきではないからです。SecuROIは、その判断の手前にある「**自社の現在地を、事実に基づいて・継続的に・見せられる形で把握する**」部分を担います。

SCS★3との関係（どこまで重なり、どこを補うか）
前章で見たとおり、★3の重心は「攻撃等の防御（アクセス制御・認証など）」と「リスクの特定（資産の把握）」にあり、この2分類で★3要求事項の約3分の2を占めます。SecuROIの標準20問は、**まさにこの比重の大きい領域──アクセス管理・認証、資産の把握、そして検知・対応・復旧──の現在地把握のベースをカバー**します（NIST6機能に最低1問ずつ対応する設計のため、6機能側は網の目が通っています）。

一方で、★3には、標準20問より**細かい粒度で問われる領域**もあります。具体的には「取引先管理」「パスワード／ロックの運用ルール」「端末の安全な構成」「ネットワーク境界の防護」などです。SecuROIは、これらを**SCS対応向けの補問**として二段構えで補い、★3の自己評価に向けた現在地把握の土台とする方針です（標準の20問はそのまま活かし、SCS向けに必要な問いを足す設計です）。

★正直な但し書き：★3の評価基準の細部（具体的な日数・保存期間・手続きの粒度など）は、制度の解説書公表（2026年10月頃予定）で精緻化される見込みです。SecuROIは「現在地把握と継続管理」を担う道具であり、**最終的な適合判断は専門家の確認によります**。だからこそ私たちは、断定的な"適合済み"ではなく、"どこがどこまで整っているか"を正直に可視化することにこだわっています。

そして──スコアを良く見せる唯一の方法は、**実際に改善すること**です（SecuROIのスコアは決定論的で、同じ回答は同じ結果になり、取り繕えません）。"見せられる形"を追う力が、そのまま実質的な改善につながる。これが、体裁でなく実質を、しかし外部にも示せる形で、という私たちの設計思想です。

おわりに：求められる前に、現在地を

IPO準備には明確な締め切りがあります。取引先審査やRFPも、期限を伴ってやってきます。そしてSCS評価制度は、"締め切り"というより**"取引の条件"として、ある日あなたの会社に求められ始めます**。

いずれの場合も、そのとき慌てて体裁を整えるのでは間に合いません。**今のうちに現在地を把握し、四半期ごとに改善を積み、その軌跡を残しておく**。それが、締め切りにも、取引先の条件にも、最も強く・最も誠実に応える備えになります。

本ガイドが、その第一歩の地図になれば幸いです。

SecuROIについて

IPO準備・取引先審査・SCS評価制度対応に向けた、セキュリティ現在地の可視化サービス。約20問・15分の自己診断から、経営が使える投資判断レポートと、監査・審査が参照できる対応表を出力します。1ヶ月の無償トライアルをご用意しています。

▶ 詳しくは securoi.com へ

本資料の制度に関する記述は、経済産業省・IPAの公開情報に基づく概要です。正確・最新の要求事項は必ず公式情報をご確認ください。SCS評価制度は企業の格付けを目的とするものではありません。