Acronis

サプライチェーン強化に向けたセキュリティ対策（SCS）評価制度 ～ ★3 対応で築く、確かな備えと信頼 ～

統合型のサイバーセキュリティ、バックアップ、運用管理で、サプライチェーンに求められる対策強化を支援します。

SCS評価制度とは

日本において、サイバーセキュリティは単なるIT施策の取り組みや項目だけにとどまらず、サプライチェーン取引における重要な評価基準になりつつあります。取引先やパートナー企業は、サプライヤーがIT基盤の適切な運用管理、保護、維持に取り組み、インシデント発生時にも取引を復旧できることを重視しています。

「サプライチェーン強化に向けたセキュリティ対策（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）が主導し、独立行政法人情報処理推進機構IPA運営を担う制度で、2026年度末（2027年3月末）頃の制度開始を目指し、サプライチェーンのセキュリティ対策を評価、可視化することを目的としています。

具体的には、各企業のセキュリティ対策への取り組みとその水準に基づき、★3（三つ星）、★4（四つ星）、★5（五つ星）の評価基準が設けられます。

多くの企業にとって実務上のベースラインとなるのが、★3対応です。サプライチェーンに関わる企業が共通して取り組むべき最低限のセキュリティ対策として、基本的な組織対応、IT基盤の防御、そして復旧への備えに重点が置かれています。

まずはSCS ★3対応！次に★4

★3は、セキュリティ専門家による確認を伴う自己評価に基づく仕組みです。既知の脆弱性を悪用する一般的なサイバー攻撃に対し、必要な基本対策が整備されていることを、サプライヤーが示すことを目的としています。

★4は、サプライチェーンへの影響が大きい組織や、より高い情報リスクを抱える組織を想定した位置づけです。より広いガバナンス、取引先管理、検知、インシデント対応が求められ、第三者評価と技術的検証が加わります。

SCS ★3の特徴

SCS ★3は、実際のサプライチェーン取引を踏まえて設計された制度です。発注側は取引先に求める適切なセキュリティ水準を示しやすくなり、受注側は顧客ごとに異なるチェックリストへの個別対応の負担を抑えながら、共通の基準に基づいて自社の取り組みと対策を示しやすくなります。

これは格付け制度ではなく、特定のセキュリティ製品の導入を義務付けるものでもありません。効果的なセキュリティ対策を実装し、その実施状況を示し、確認するための枠組みです。

この制度は、次の点で役立ちます

- 取引先、パートナー企業、サプライヤーとの信頼強化
- 入札、調達、取引先評価に関する対話の支援
- ランサムウェア、アカウント侵害など一般的な攻撃による業務影響の低減
- 自己評価と専門家確認に向けた実務的なエビデンス整備

SCS ★3サイバーセキュリティの柱

SCS ★3では、方針策定から実運用、そして実施状況を可視化するために、要求事項を実務的な領域ごとに整理しています。

ガバナンスの整備	取引先管理	リスクの特定	攻撃等の防御	攻撃等の検知	インシデントへの対応	インシデントからの復旧
セキュリティ方針や役割、責任を明確化し、組織的に統制・管理する	取引先との関係性や情報共有範囲を整理し、サプライチェーンの安全性を確保する	守るべき情報資産や脅威を洗い出し、事業上のリスクを可視化する	認証強化やセキュリティ対策を実装し、サイバー攻撃を未然に防止する	不正アクセスや異常な挙動を早期に検知できる監視体制を確立する	事故発生時に迅速かつ適切に対応できる手順と体制を整備する	被害後も業務を早期に復旧し、事業継続性を確保する体制を構築する

注意： 経済産業省は、SCS評価制度について、任意の制度であり、個別の商取引を規制するものではなく、特定のセキュリティ製品の導入を求めるものでもないと明示しています。最終的な評価判断にあたっては、必ず経済産業省およびIPAの公式資料をご確認ください。

Acronis Cyber Protect CloudとSCS ★3 対応領域の関係

SCS ★3は、製品機能の有無を確認するためのチェックリストではありません。企業ごとに自社環境に必要な施策を行い、その実施状況を示すことが求められます。アクロニスは、ネイティブ統合型のサイバープロテクションプラットフォームで、SCS ★3の評価要件で求められる、管理、セキュリティ、検知と対応、バックアップと復旧をはじめとする領域での実運用を支援します。

資産管理

アクロニスの資産管理・監視機能は、エンドポイントや主要なワークロードにおける資産の把握、状態監視、ポリシー状況の可視化を支援します。これにより、管理上の抜け漏れを把握しやすくなり、実施状況を説明するための材料整備にも役立ちます。

保護・防御

アクロニスのセキュリティ機能は、エンドポイントを中心に、メール、コラボレーション環境、機密データに対する脅威の予防と封じ込めを支援します。継続的な防御運用を通じて、基本的な管理策の実装と維持を支援します。

更新管理

アクロニスのパッチ管理機能は、OS やサードパーティ製アプリケーションを最新の状態に維持する運用を支援します。集中管理されたスケジュール設定とレポートにより、継続的かつ一貫したパッチ適用を進めやすくします。

バックアップと復旧

アクロニスのバックアップ機能は、エンドポイント、サーバー、Microsoft 365 などのデータ保護を支援し、ランサムウェア被害、誤削除、障害発生時の復旧性向上に役立ちます。高速かつ粒度の細かい復元により、事業継続に向けた備えを支援します。

検知・対応

アクロニスの検知・対応機能は、アラートのトリアージや封じ込めの迅速化を支援します。また、何が起き、どのように対応したかを把握しやすくする運用フローやレポートを通じて、実施状況の可視化にも役立ちます。

SCS ★3に向けたサイバーレジリエンス強化

多くの組織が課題を抱えるのは、セキュリティ製品が不足しているからではありません。より大きな課題は、対策を継続的かつ一貫して運用すること、設定のばらつきを防ぐこと、パッチ適用を維持すること、そして実際に何が実装されているかを説明できることにあります。

Acronis Cyber Protect Cloudは、保護、監視、パッチ管理、バックアップ、復旧、レポートを1つの統合プラットフォームに集約することで、SCS ★3対応を単なる要件対応にとどめず、実運用に結び付ける取り組みを支援します。

AI 支援による堅牢なセキュリティ

ランサムウェアや高度化するサイバー攻撃に対し、AI を活用した保護機能により、日常的な防御運用を支援します。

プロアクティブな運用管理

継続的な監視、パッチ管理、自動化により、問題が業務へ影響する前の予防的な運用を支援します。

レジリエンスの可視化

検証可能なバックアップと復旧プロセスにより、誤削除、障害、ランサムウェア被害からの迅速な業務復旧を支援します。

運用効率の最大化

ネイティブ統合されたプラットフォームで、複雑性を排除し、リスクの低減と俊敏な対応を実現します。

次のステップ

SCS ★ 3 への対応は、書類対応だけで終わるものではありません。まずは現状把握を行い、現在の状況を確認したうえで、優先度の高いギャップを特定し、必要な施策を実施、検証していくことが重要です。あわせて、専門家による確認に向けたエビデンスを整備し、実施状況を説明できる状態を整えることが求められます。

出典：2026 年 4 月 27 日時点で公開されている経済産業省 / IPA の SCS 評価制度に関する公開資料、およびアクロニスの公開製品情報に基づいて作成しています。本資料は一般的な対応検討の参考を目的としたものであり、法的助言、公式な認証判断、または SCS ★ 3 取得を保証するものではありません。

Acronis

詳細はこちらをご覧ください
acronis.com