アスモチ株式会社
ASMOCH

サプライチェーン取引の“信用力”を可視化する

経済産業省のSCS（サプライチェーン強化に向けたセキュリティ対策）評価制度の運用開始に備える第一歩

自社およびお取引先様の対応状況とリスクをチェックリストで可視化



SCS評価制度 三ツ星（★3）の要求事項（26項目）および対応状況チェックリスト

（2026/3/20 時点）

大分類	中分類	Index	要求事項（案）	★3 評価基準	製品/サービス対応状況 *1. Acronis Cyber Protect *2. Acronis Cyber Protect Cloud *3. 3rd Party Solution	チェック ★3 △ ー	備考
ガバナンスの整備	役割/責任/権限	1	**セキュリティ推進活動部門** セキュリティ推進活動を担当する部署、役員及び従業員を決定し、責任及び権限を割り当てること。	1.セキュリティを統括する役員(例えば、CISOを設置する会社の場合は、当該CISO)及びセキュリティ担当部署の役割・責任を定めること。 2.平時のセキュリティ推進活動に必要な役員(例えば、CISOを設置する会社の場合は、当該CISO)及びセキュリティ担当部署の連絡先リストを定めること。 3.年1回以上の頻度で上記に定めた平時の体制について点検すること。	ー		組織体制の確立は、主に文書とプロセスによって行われます。 ※直接的な製品機能の対応はありません。 ※Acronis製品の統合管理機能は、セキュリティ担当者の運用管理負担を大幅に軽減します。
		2	**守秘義務のルール** 守秘義務のルールを策定し、遵守させること。	1.役員、従業員、派遣社員及び受入出向者を対象に、自社の守秘義務のルールを定めること。 2.入社時又は社外要員の受入れ時に守秘義務のルールを説明すること。	ー		組織体制／契約上の要件となります。 ※直接的な製品機能の対応はありません。
	ポリシー	3	**セキュリティ対応方針の策定** 自社のセキュリティ対応方針(ポリシー)を策定し、周知すること。	1.自社のセキュリティ対応方針を定めること。 2.定常的に役員、従業員、派遣社員及び受入出向者がセキュリティ対応方針を参照できるようにすること。 3.セキュリティ対応方針の改正時に、当該改正内容を役員、従業員、派遣社員及び受入出向者に周知すること。	ー		組織体制／文書化の要件となります。 ※直接的な製品機能の対応はありません。
取引先管理	サイバーセキュリティサプライチェーンリスクマネジメント	4	**取引先とのビジネス又はシステム上の関係** 取引先と自社とのビジネス又はシステム上の関係を把握すること。	1.自社以外の組織(顧客・子会社・関係会社・クラウドサービス提供者を含む取引先)が管理・提供し、自社の資産が接続しているシステムを把握するための仕組みを整備すること。 2.年1回以上の頻度で上記において把握すべき情報の内容を点検すること。	ー		組織体制／文書化の要件となります。 ※直接的な製品機能の対応はありません。
		5	**機密情報の取扱い** 他社との間で、機密情報の取扱い方法を明確にすること。	1.自社の機密情報を共有する取引先との間で、業務開始前に機密情報の取扱いについて、以下の事項の取り交わすこと。 - 機密情報の定義 - 機密情報の取扱い(表示、保管方法、複製可否及び第三者への提供可否) - 機密情報の返還又は廃棄	ー		組織体制／文書化の要件となります。 ※直接的な製品機能の対応はありません。
		6	**セキュリティインシデント発生時の役割・責任** セキュリティインシデント発生時の他社との役割及び責任を明確にすること。	1.機密情報を共有する子会社又は取引先との間で、セキュリティインシデント発生時の自社と子会社又は取引先の役割及び責任について、以下の事項を定めること。 - セキュリティインシデント発生時の相手方への通知義務 - セキュリティインシデント発生時の連絡先 - 再発防止策の協議方法	ー		組織体制／文書化の要件となります。 ※直接的な製品機能の対応はありません。
リスクの特定	資産管理	7	**ハードウェア、OS及びソフトウェアの把握** ハードウェア、OS及びソフトウェアに関する情報を把握すること。	1.適用範囲内のパソコン及びシンクライアントの製造元、OS及び台数を把握するための仕組みを整備すること。 2.適用範囲内のサーバ、仮想サーバ及びハイパーバイザの製造元、OS及び台数を把握するための仕組みを整備すること。 3.情報機器、OS及びソフトウェアについて、導入、設置、ネットワーク接続及びセキュリティパッチ適用のルールを含む管理ルールを定めること。 4.年1回以上の頻度で上記に定めた管理ルールの遵守状況について点検すること。	*1, *2. ・ハードウェア、ソフトウェアインベントリ管理 ・組織内に配置されているデバイス検出 ・脆弱性診断／パッチ管理		Acronis製品のIT資産情報管理機能を利用して、定期的な棚卸に必要な、IT資産情報（ハードウェア、OS、ソフトウェア）の可視化を支援します。 また、脆弱性診断、パッチ管理機能を利用し。パッチ運用ルール策定を支援します。
		8	**ネットワークの一覧作成** ネットワークの情報に関する一覧を作成すること。	1.適用範囲内のネットワークを把握するための仕組みを整備すること。その際、把握すべき情報の中に各ネットワークの所在地及び目的に関する情報を含めること。 2.適用範囲内のネットワーク機器を把握するための仕組みを整備すること。その際、把握すべき情報の中に各機器の製造元、モデル及び保守事業者に関する情報を含めること。	*1, *2. ・脆弱性診断 ・評価		Acronis製品でネットワーク機器のインベントリは直接示されていませんが、システム全体の脆弱性評価を行います。
		9	**外部情報サービスの管理** 自社の機密情報を扱う外部情報サービスを管理すること。	1. 以下の内容を含む外部情報サービスの利用ルールを定めること。 - 外部情報サービスを利用する際のセキュリティ要件を定めること。 - 外部情報サービスの利用時にセキュリティ要件を満たしているかサービス内容を確認し、自社の役員又は従業員が承認すること。 2. 外部情報サービスの接続先と機密情報の取扱いについて取り交わすこと。	ー		組織体制／文書化の要件となります。 ※直接的な製品機能の対応はありません。
		10	**機密区分に応じた情報の管理** 機密区分に応じた情報の管理ルールを定め、それに基づく管理を行うこと。	1.自社の保有する情報を対象に、以下の内容を含む管理ルールを定めること。 - 機密の特定 - 機密区分のレベル判定及び表示 - 区分に応じた取扱方法 - 取扱エリアの区分及び制限" 2.年1回以上の頻度で上記に定めた管理ルールの内容について点検すること。 3.機密区分のうち、高い機密区分の情報並びに当該情報ごとの管理者名、部署名、保管場所、保管期限、開示先及び管理者の連絡先を把握するための仕組みを整備すること。	*2. ・DLP（データ損失防止） ・暗号化		Acronis製品のDLP機能で、機密データのカテゴリ分類、データ転送監視、通信ポート・チャネルの制御を行います。
		11	**ユーザIDの管理手続** ユーザID の発行・変更・削除の手続を定め、適切に運用すること。	1.自社の従業員、派遣社員及び受入出向者に対するユーザIDの付与・変更・削除は申請・承認制にすること。 2.ユーザIDの共有について、以下のいずれかを適用すること。 -ユーザIDを共有しない。 -やむを得ず共有IDが必要な場合(例えば、システムの仕様により、使用人数分のIDを発行することができない場合)は、共有IDを利用したユーザを特定できるようにする。" 3.ユーザIDが不要になった場合(例えば、ユーザが組織を退職した場合又はIDが一定期間使用されなかった場合)、速やかにユーザIDを削除又は無効化すること。 4.ユーザIDにおける特別なアクセス権限が不要になった場合(例えば、スタッフの役割が変わった場合)は、当該権限を速やかに削除又は無効化すること。	*3.		組織的なID管理手続きの策定が求められる要件です。 ※3rd Party Solutionのご利用についても検討。

攻撃等の防御	アイデンティティ管理とアクセス制御	12	**管理者IDの管理手続** 管理者IDの発行・変更・削除の手続を定め、適切に運用すること。	1.すべてのサーバ及びネットワーク機器について、システム管理者及び責任者を定めること。 2.管理者権限を付与する役員、従業員、派遣社員及び受入出向者を限定したうえで、管理者IDについて以下のいずれかを適用すること。 -管理者IDを共有しない。 -やむを得ず管理者IDの共有が必要な場合(例えば、システムの仕様により、使用人数分のIDを発行することができない場合)は、共有の管理者IDを利用したユーザを特定できるようにすること。" 3.各管理者IDに対して役割に応じた必要最低限の権限のみを付与すること。 4.システム開発を実施する役員、従業員、派遣社員及び受入出向者が本番環境において、管理者権限で操作できないようにすること。 5.組織内でどの役員、従業員、派遣社員及び受入出向者が管理者IDを持っているかを把握するための仕組みを整備すること。 6.管理者IDが不要になった場合(例えば、管理者が組織を退職した場合及びIDが一定期間使用されなかった場合)、速やかに管理者IDを削除又は無効化すること。 7.管理者IDの付与・変更・削除は申請・承認制にすること。 8.管理者IDの付与・変更・削除並びにサーバ及びネットワーク機器の設定内容の変更を行う権限を業務上必要な役員、従業員、派遣社員及び受入出向者に限定すること。	*3.		組織的なID管理手続きの策定が求められる要件です。 ※3rd Party Solutionのご利用についても検討。
		13	**認証の強度・実装方法の決定** システム及び情報の重要度に応じて認証の強度及び実装方法を決定すること。	1.すべてのユーザIDについて、アプリケーション及び情報機器へのアクセスを許可する前に、一意の認証情報(パスワード等)でユーザを認証すること。 2.重要な情報を取り扱うと考えられるクラウドサービスにおいて、ユーザ及び管理者がサービスにアクセスする場合は、常に多要素認証を使用すること。 3.多要素認証の使用に当たっては、以下のいずれかの要素から2種類以上を選択し、利用すること。 -知識情報(例:ID・パスワード) -所有情報(例：ワンタイムパスワード※又は証明書) -生体情報(例：指紋、顔、虹彩又は静脈) -その他の情報(例:IPアドレス) ※利用者のメールアドレス、電話番号等に対してワンタイムパスワードを送信して利用者に入力させる方法及びスマートフォンへの認証要求を利用した認証方式を含む。" 4.多要素認証の知識情報として用いるパスワードは、8文字以上とすること。	***1, *2.** 多要素認証（MFA）の使用推奨（評価基準に明記） *3.		アクロニス製品は、クラウド認証システムではありませんが、この要件の必要性を明確にしています。 ※3rd Party Solutionのご利用についても検討。
		14	**アカウントロック制御** 社内システムを構成する端末にアカウントロック制御を実装すること。	1.業務で利用するシステムを構成する端末へのログオン(パソコンへのログオン及びスマートデバイスのロック解除)にあたって、設定が可能な場合、以下のいずれかを適用すること。 -試行回数を調整し、試行が失敗するたびに試行間隔が長くなるようにする。 -試行が10回以上失敗するとアカウントをロックする。 2.上記に示す要件のいずれも設定することができない場合、下記（パスワード設定ルール）で求められるよりも強度の高いパスワードを用いる等の代替策を用いること。 3.パソコン及びスマートデバイスのロック解除を行う場合、最低でも6文字以上のパスワード又はPINを利用すること。	–		端末レベルの制御ポリシー設定が求められる要件です。 ※直接的な製品機能の対応はありません。
		15	**パスワード設定ルール** パスワード設定に関するルールを定め、周知すること。	1.パソコン、サーバ、スマートデバイス及びクラウドサービスの利用者又は管理者は、それらにおけるデフォルトパスワードを変更すること。 2.ユーザ認証にパスワードを利用する場合、推測されやすい単語の設定を禁止するよう社内ルールを定めること。 3.ユーザ認証にパスワードを利用する場合、以下のいずれかの保護対策を講じること。 -多要素認証を使用するか、又は試行が少なくとも10回失敗した場合にアカウントロックするように制限したうえで、パスワードの長さを8文字以上とする。 -上記のとおり多要素認証又は試行回数の制限を実施できない場合、パスワードの長さは、英大文字小文字、数字を含めた10文字以上とする。" 4.ユーザ認証にパスワードを利用する場合、情報機器及びサービス間でのパスワードの使い回さないこと。	–		パスワード運用管理ポリシー策定の要件です。 ※直接的な製品機能の対応はありません。
		16	**パスワード管理ルール** パスワードの管理に関するルールを定め、周知すること。	1.紙媒体への記載及び施錠保管、パスワード管理アプリの利用等により、パスワードを安全に保管することを定め、役員、従業員、派遣社員及び受入出向者を対象に周知すること。 2.設定可能な場合はパスワードの定期的な変更を強制しないこと。 3.パスワードの漏洩が判明した場合、又はその疑いがある場合に速やかにパスワードを変更するための手順を定めること。	–		パスワード管理と安全な運用の要件です。 ※直接的な製品機能の対応はありません。
		17	**アクセス権の管理ルール** アクセス権の管理ルールを定めて、運用すること。	1.業務で利用するシステム及びパソコンへのログオン時のユーザのアクセス権並びに機密上の配慮が必要な場所及び部屋への入室について、以下の内容の管理ルールを定めること。 -アクセス権の発行・変更・削除は申請・承認制であること。 -与える入室許可・アクセス権の範囲は必要な範囲に限定すること。 -入室権限及びアクセス権の棚卸について定めていること。 -与えた入室許可・アクセス権の申請書又は台帳を管理していること。	–		組織体制／管理の要件です。 ※直接的な製品機能の対応はありません。
	意識向上及びトレーニング	18	**セキュリティインシデント発生時の教育・訓練** セキュリティインシデント発生時の対応に関する教育・訓練を行うこと。	1.役員、従業員、派遣社員及び受入出向者を対象に、新規受入れ時、かつ、年1回以上の頻度で、セキュリティインシデント発生時の対応について、教育資料の配布・掲示に加え、e ラーニング又は集合教育による教育・訓練を実施すること。 2.上記で実施した教育・訓練の実施内容、実施方法、実施時期及び受講状況を記録し、保管すること。 3.年１回以上の頻度でセキュリティインシデント発生時の対応に関する教育・訓練の実施内容について点検すること。	***2.** ・アクロニスセキュリティ意識向上トレーニング（SAT）		Acronis製品のセキュリティ意識向上トレーニング（SAT）で従業員の教育および訓練を実施します。
	データセキュリティ	19	**適切なバックアップ** 適切なバックアップを行うこと。	1.取得対象、取得頻度及び保管期間を定めて自組織で取り扱うデータのバックアップを取得すること。 2.重要情報については、上記におけるバックアップに加えて、遠隔地バックアップを実施すること。 3.バックアップ対象ごとにリストア手順書を整備すること。	***1, *2.** ・イメージバックアップ ・データバックアップ ・Acronis Cloud バックアップ ・ワンクリップリカバリー		Acronis製品の柔軟なバックアップと復旧機能を利用することで、任意のOPO、RTO要件に応じたシステム復旧を支援します。また、Acronis Cloudへのバックアップでは、遠隔地バックアップを支援します。
		20	**ハードウェア、OS及びソフトウェアの安全な構成** ハードウェア、OS及びソフトウェアの安全な構成を確立し、維持すること。	1.パソコン、サーバ及びスマートデバイスで利用を許可していないソフトウェアをすべて削除又は無効化すること。 2.外部記録媒体を使用する端末について自動実行(auto-run)又は自動再生(auto-play)を無効化すること。 3.サーバ及びネットワーク機器の設定変更を申請・承認制にすること。	***1, *2.** ・ハードウェア、ソフトウェアインベントリ管理		組織体制／管理の要件です。 ※Acronis製品の資産管理機能により、資産状況の可視化を可能にし、ソフトウェア資産の有効 ／無効化判断材料を提供することで、安全な構成維持を支援します。

	プラットフォームセキュリティ	21	**セキュリティパッチ・アップデートの手続** ハードウェア・ソフトウェア等へのセキュリティパッチやアップデートの適用に係る手続等を策定し、実行すること。	1.適用範囲内のシステム、情報機器及びソフトウェアは以下の状態とすること -ライセンスが付与され、サポートされている。 -サポートが終了した場合に削除されるか、又はインターネットとの全てのトラフィックを遮断することで適用範囲から削除される。 -可能であれば、自動アップデートが有効化されている。 2.以下のいずれかに該当する場合、アップデートプログラムがリリースされてから14日以内に、アップデートすること。 -当該アップデートが、ベンダーにより「重大」(Critical)又は 「高リスク」(High Risk)と説明される脆弱性を修正するものである。 -当該アップデートが、CVSS v3 の基本スコアが7以上の脆弱性を修正するものである。 -当該アップデートが修正する脆弱性のレベルの詳細がベンダーから提供されていない。 [対象] -会社支給のパソコンの OS、ブラウザ及びOffice ソフト -サーバの OS及びミドルウェア -会社支給のスマートデバイスのOS及びアプリ -インターネットとの境界に設置されているネットワーク機器の OS及びファームウェア 3.やむを得ず上記のとおりアップデートができない場合(例えば、動作検証に一定期間を要し、期限内にアップデートが完了しない場合)は、アップデート適用までの間、以下のいずれかにより脆弱性悪用のリスクを低減する対策を実施すること。 -ベンダーよりリリースされる仮想パッチを適用すること。 -対象となる情報機器を適用範囲内のネットワークから分離すること。 -対象となる情報機器と適用範囲内のネットワークとの境界部分に、通信を監視して不正な挙動を検知する機器を導入すること。	***1, *2.** ・ハードウェア、ソフトウェアインベントリ管理 ・脆弱性診断／パッチ管理 ・セーフパッチ適用		Acronis製品の資産管理機能により、資産状況の可視化を支援します。 また、脆弱性診断でリスクを特定し、パッチ管理機能でパッチ適用を支援します。。フェイルセーフパッチ適用は、パッチ適用前の自動バックアップにより、更新失敗時のロールバックを可能にします。
		22	**マルウェア感染からの保護** システムをマルウェア感染から保護すること。	1.ネットワークに接続しているすべてのパソコン及びサーバに、マルウェア対策ソフトウェアを導入すること。 2.情報機器に応じたスキャン範囲及び頻度を規定し、スキャンを実行すること。 3.マルウェア対策ソフトウェアのパターンファイルを、ベンダーの推奨に従ってアップデートすること。	***1, *2.** ・Acronis EDR / MDR ・AV / NGAV ・高度な脅威監視 ・ランサムウェア対策（Acronis Active Protection）		Acronis製品のAIベースのアンチウイルス、ランサムウェアプロテクション、EDRをはじめとする高度な脅威監視と高度なランサムウェア対策技術（Acronis Active Protection）でシステムをリアルタイムで保護します,
	技術インフラのレジリエンス	23	**ネットワーク境界防護** 内外のネットワークを適切に分離し、境界部分を防護すること。	1.すべてのファイアウォール(又はファイアウォール機能を持つネットワーク機器)及びルータについて、デフォルトの管理パスワードを強固で一意のパスワードに変更する、又はリモート管理アクセスを完全に無効化すること。 2.ファイアウォール及びルータのパスワードを変更する手順を定めること。 3.ファイアウォール及びルータに係る認証は、パスワード設定、認定ルールに定める認証、パスワード設定等に関する基準を満たすこと。 4.全てのファイアウォール(又はファイアウォール機能を持つネットワーク機器)について、認証されていないインバウンド通信をデフォルトで遮断すること。 5.すべてのファイアウォール(又はファイアウォール機能を持つネットワーク機器)について、インバウンド通信に関するファイアウォール・ルールが、担当者によって承認され、定められていること。 6.すべてのファイアウォール(又はファイアウォール機能を持つネットワーク機器)について、不要になったファイアウォール・ルールを速やかに削除又は無効化すること。 7.ファイアウォール・ルールの変更をインターネット経由で行う場合、多要素認証を適用するか、又は信頼できるIPアドレスにアクセスを制限すること。	***2.** ・セキュアURLフィルタリング *3.		ファイアウォールの管理機能および3rd party 提供の監視、管理機能、サービスをご利用の上、要件に対応願います。 Acronis製品のセキュアURLフィルタリング機能は、境界防護策の一つとして対応を支援します。
攻撃等の検知	継続的監視	24	**ネットワーク接続・データの監視** ネットワーク上の適切な場所でネットワーク接続及びデータ転送を監視すること。	1.社内外ネットワークの境界又は端末において、インターネットから社内への通信及び社内から不正なサーバへの通信の双方について、不正アクセスをリアルタイム検知・遮断する仕組みを導入すること。 2.ネットワーク機器のログ及びアラートを分析し、セキュリティ担当部署の担当者又は管理者により不審な事象が発見された場合に、それがセキュリティインシデントに該当するかが判断されること。 3.上記で設置したネットワーク機器又はサービスについて、以下の要件を満たす異常時に通知する仕組みを導入すること。 -アラートが即時発報されること。 -関連したセキュリティ事象の速報レポートが作成され、通知されること。	***1, *2.** ・Acronis EDR /MDR ・高度な脅威監視 ・レポーティング		Acronis製品の高度な脅威監視およびEDR（Endpoint Detection and Response）やMDR（Managed Detection and Response）機能で、リアルタイムの脅威を検知し、インシデントの予兆や不正アクセスを特定する仕組みを支援します。
インシデントへの対応	インシデント管理	25	**インシデント対応手順** セキュリティインシデントへの対応手順、対応体制等を定めること。	1. セキュリティインシデントへの対応手順を定めること。 2.上記に定めたセキュリティ対応手順には以下の手順を含んでいること。 ①発見報告、 ②初動、③調査・対応、④復旧、⑤最終報告 3.セキュリティインシデントの基準並びにセキュリティインシデント発生時における社内外組織(関係当局及び所管省庁への報告又は情報共有を含む。)との連絡先及びルートを定めること。 4.セキュリティインシデント発生時におけるセキュリティを統括する役員(例えば、CISOを設置する会社の場合は、当該CISO)及びセキュリティ担当部署の役割・責任を定めること。 5.年1回以上の頻度で上記に定めたセキュリティインシデント発生時の体制について点検すること。 5.セキュリティインシデントの報告フォーマットを整備すること。 6.年１回以上及び社内外で重大なセキュリティインシデントが発生した際に、インシデント事例及びその対応策を社内部署へ共有していること。	***1, *2.** ・Acronis EDR /MDR ・フォレンジックバックアップ ・レポーティング		Acronis EDR/MDRはインシデント検知後の 初動対応を支援します。フォレンジックバックアップは、インシデント調査に必要なデジタルエビデンスをバックアップから収集することを可能にし、原因究明を支援します。
インシデントからの復旧	インシデント復旧計画の実行	26	**事業継続要件に沿った復旧準備** 事業上重要なシステムについて、事業継続の要件に沿う復旧に必要な準備を行うこと。	1.事業継続上重要なシステムについて、サイバー攻撃を念頭に、業務の目標復旧レベルを定めたうえで、当該レベルまで業務を回復するために必要な対策を、以下の例を参考として整備すること。 [復旧のための対策(例)] -システムによる業務継続(例:予備機、クラウド環境等により待機系を整備する。) -人手による業務継続(例:電話、FAX等による連絡又は業務の実施に備え、影響のある取引先の連絡先及び複数の連絡手段を整備する。)	***1, *2.** ・イメージバックアップ ・データバックアップ ・Acronis DR ・ワンクリップリカバリー		Acronis製品の柔軟なバックアップと復旧機能能を利用することで、任意のOPO、RTO要件に応じたシステム復旧を支援します。 Acronis DRでは、Acronis Cloudへの重要システムのFailoverによる、ディザスタリカバリーの導入を支援します。

【備考】

・当該チェックリストは、2025年12月31日時点の、経済産業省「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関する制度構築方針（案）」、三ツ星（★3）要求事項（26項目）に基づく対応状況セルフチェックリストです。なお、SCS評価制度の構築方針（最終版）発行に向けて、評価、認定内容、条件が更新される場合があります。

・三ツ星（★3）評価は、全てのサプライチェーン企業が最低限実装すべきセキュリティ対策として、基礎的なシステム防御策と体制整備を中心に実施する段階を示し、専門家確認付き自己評価となります。

・当該セルフチェックリストへの対応のみで、三ツ星（★3）評価およびその認定が保証されるものではありません。

問い合わせ先：

https://www.koshicon.com/contact/ TEL：06-6484-5470

アスモチ株式会社

■大阪本社　〒541-0054大阪市中央区南本町3-1-2

■東京オフィス　〒150-0002 東京都渋谷区渋谷2-3-4

Rev_001_20260319