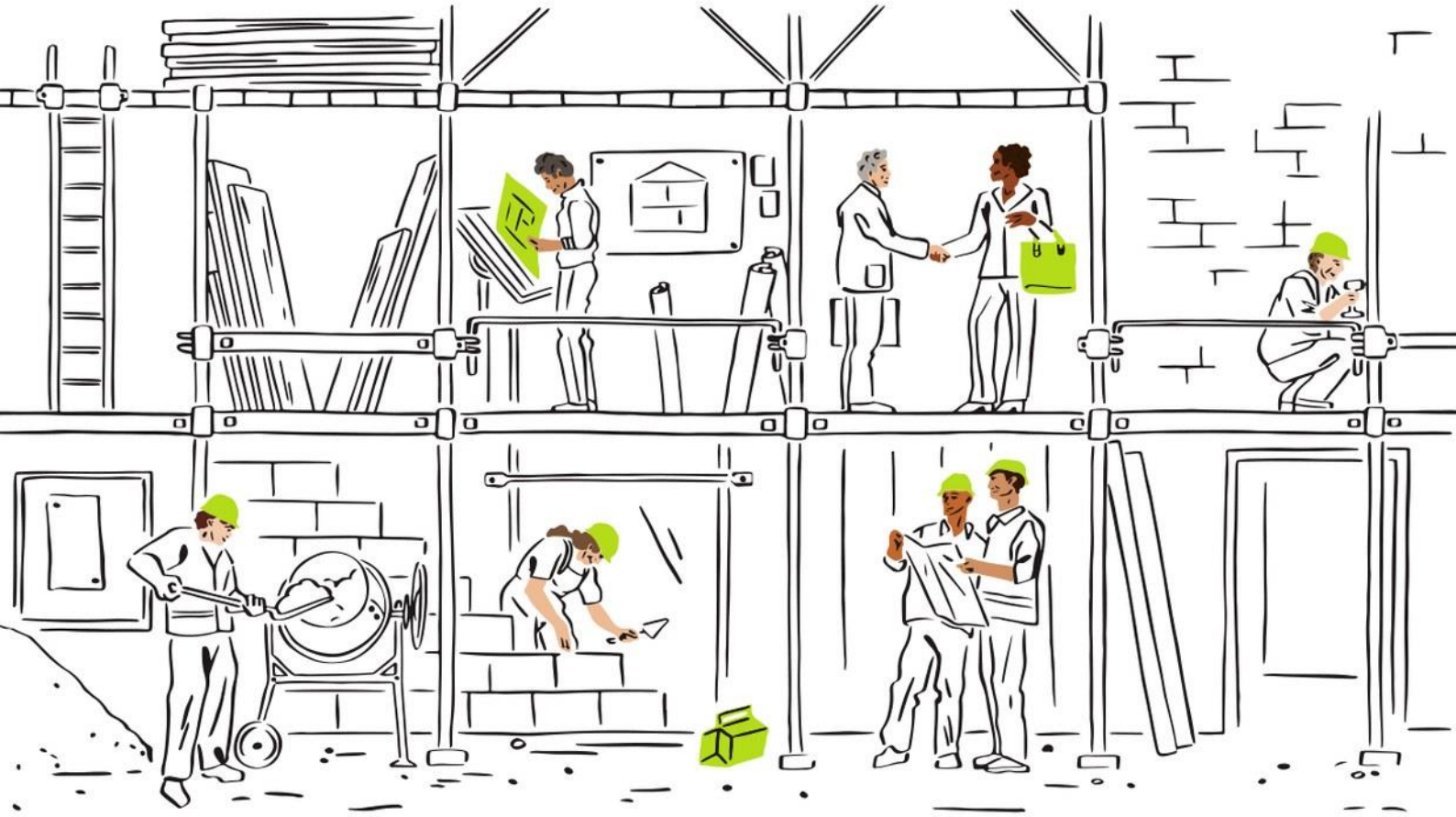


SCS評価制度実務のための ガイドブック

証跡・アクセス管理・共有ルールを整える

“証明できるセキュリティ”が取引条件になる時代へ

本ガイドブックは、SCS評価制度の理解から、評価取得・維持に必要な
証跡、アクセス管理、外部共有統制、監査、侵害からの復旧までを
実務の観点で整理したものです。

改訂履歴

版	日付	内容
v0.1	2026-05-27	添付資料にもとづく初稿
v0.2	2026-05-27	Dropbox Help 公式情報を踏まえ、Dropbox で実現できる管理・証跡・復旧・データガバナンスの記述を拡充。
v0.3	2026-05-27	保護とコントロール（Dropbox Protect）を追加。監査・インシデントレスポンス・侵害からの復旧の文脈を拡充。
v0.4	2026-05-28	Rewind を復旧手段として再追加。30 ページ相当のボリュームに戻し、制度図・Dropbox 実務図・保護とコントロール（Dropbox Protect）・Rewind・データガバナンス関連図を追加。
v1.0	2026-05-28	お客様向け FAQ を反映し、利用企業向けの実務説明に調整。
V1.6	2026-06-29	文言、エディション、ブランド名の誤りを修正
V1.7	2026-07-01	誤植を削除

本書の読み方

本書は SCS 評価制度を「制度理解」で終わらせず、評価取得・維持に必要な日常運用へ落とし込むための実務ガイドです。経営層・情シス・セキュリティ担当・購買/調達・法務/総務が共通の言葉で対応方針を議論できるよう、制度の目的、評価段階、要求事項 7 分類、証跡の考え方、Dropbox で実装できる具体機能、ロードマップ、チェックリストを一体で整理しています。

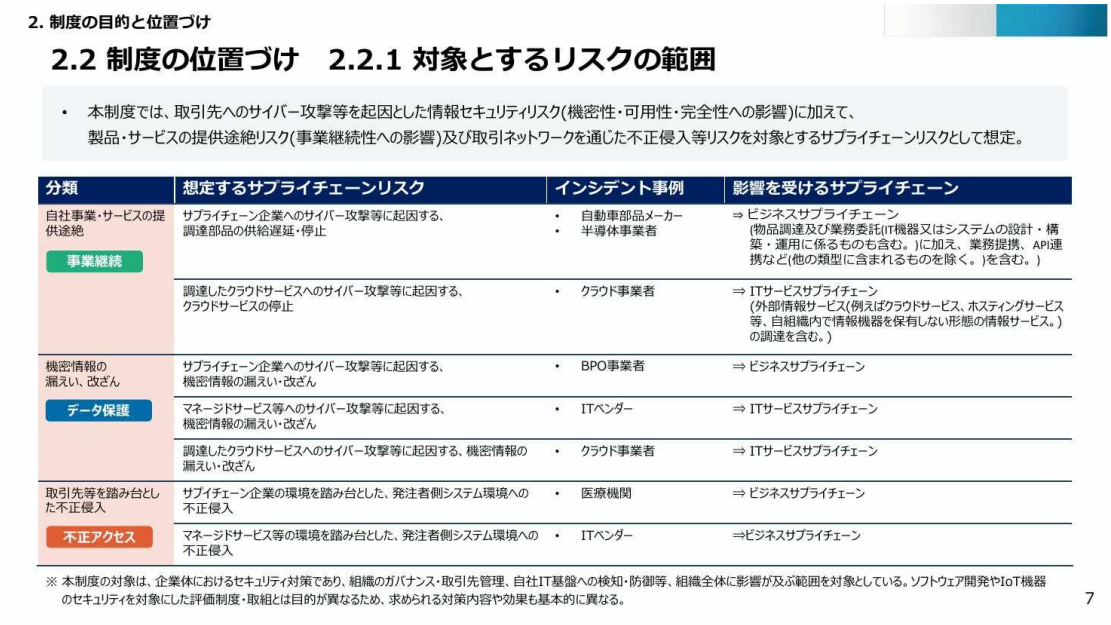
- 第 1 章から第 3 章: SCS 評価制度の背景、対象範囲、★3 および★4 の違いを理解するための章です。
- 第 4 章から第 6 章: 要求事項である 7 分類、★3 取得、★4 取得に必要な実務を整理するための章です。
- 第 7 章: Dropbox で支援できる実装を具体化した章です。
- 第 8 章以降: よくある課題、ロードマップ、FAQ、証跡チェックリストとして現場でご利用いただくための章です。

用語の定義

用語	本書での意味
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。サプライチェーン企業のセキュリティ対策状況を共通基準で可視化する任意制度です。
★3	一般的なサイバー攻撃への対処を想定した、最低限実装すべき基礎的対策。専門家確認付き自己評価が想定されます。
★4	組織ガバナンス、取引先管理、検知、対応、復旧を含む包括的対策。第三者評価および技術検証が想定されます。
証跡	対策を実施・運用した事実を第三者へ説明するための記録。ログ、設定画面、台帳、レポート、議事録、是正記録など。

目次

第 1 章 なぜ今 SCS 評価制度なのか



2. 制度の目的と位置づけ

2.2 制度の位置づけ　2.2.1 対象とするリスクの範囲

- 本制度では、取引先へのサイバー攻撃等を起因とした情報セキュリティリスク(機密性・可用性・完全性への影響)に加えて、製品・サービスの提供途絶リスク(事業継続性への影響)及び取引ネットワークを通じた不正侵入等リスクを対象とするサプライチェーンリスクとして想定。

分類	想定するサプライチェーンリスク	インシデント事例	影響を受けるサプライチェーン
自社事業・サービスの提供途絶 事業継続	サプライチェーン企業へのサイバー攻撃等に起因する、調達部品の供給遅延・停止	• 自動車部品メーカー • 半導体事業者	⇒ ビジネスサプライチェーン (物品調達及び業務委託(IT機器又はシステムの設計・構築・運用に係るものも含む。)に加え、業務提携、API連携など(他の類型に含まれるものを除く。)を含む。)
	調達したクラウドサービスへのサイバー攻撃等に起因する、クラウドサービスの停止	• クラウド事業者	⇒ ITサービスサプライチェーン (外部情報サービス(例えばクラウドサービス、ホスティングサービス等、自組織内で情報機器を保有しない形態の情報サービス。)の調達を含む。)
機密情報の漏えい、改ざん データ保護	サプライチェーン企業へのサイバー攻撃等に起因する、機密情報の漏えい・改ざん	• BPO事業者	⇒ ビジネスサプライチェーン
	マネージドサービス等へのサイバー攻撃等に起因する、機密情報の漏えい・改ざん	• ITベンダー	⇒ ITサービスサプライチェーン
	調達したクラウドサービスへのサイバー攻撃等に起因する、機密情報の漏えい・改ざん	• クラウド事業者	⇒ ITサービスサプライチェーン
取引先等を踏み台とした不正侵入 不正アクセス	サプライチェーン企業の環境を踏み台とした、発注者側システム環境への不正侵入	• 医療機関	⇒ ビジネスサプライチェーン
	マネージドサービス等の環境を踏み台とした、発注者側システム環境への不正侵入	• ITベンダー	⇒ビジネスサプライチェーン

※ 本制度の対象は、企業体におけるセキュリティ対策であり、組織のガバナンス・取引先管理、自社IT基盤への検知・防御等、組織全体に影響が及ぶ範囲を対象としている。ソフトウェア開発やIoT機器のセキュリティを対象にした評価制度・取組とは目的が異なるため、求められる対策内容や効果も基本的に異なる。

7

図 1 SCS 制度が対象とするサプライチェーンリスク（制度構築方針）

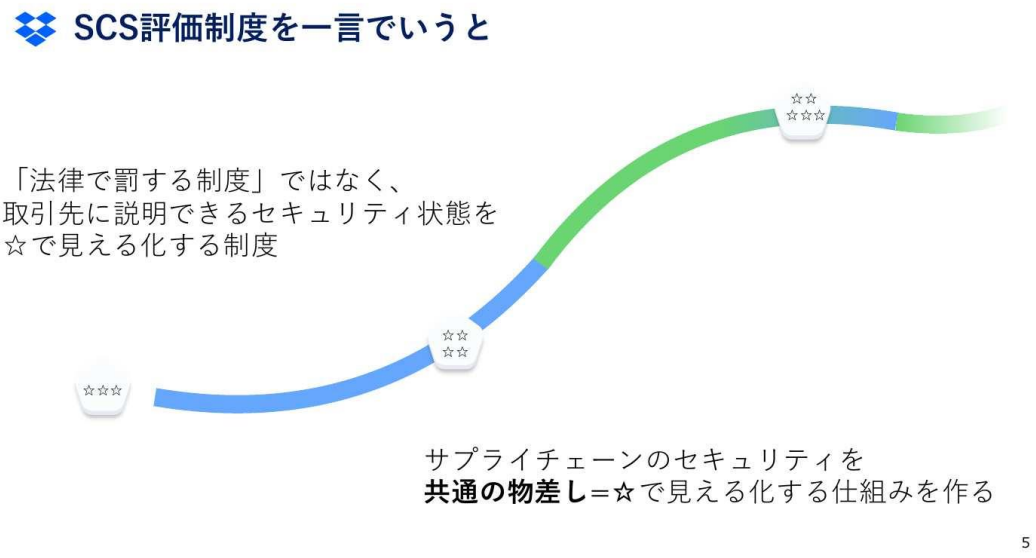


図 2 SCS 評価制度を一言で整理したスライド（Dropbox 実務資料）

1-1 サプライチェーン攻撃が経営リスクになった

従来のセキュリティ対策は自社ネットワーク、自社端末、自社システムを守る発想が中心でした。しかし現在の攻撃では、発注元企業そのものを直接攻撃するのではなく、防御が相対的に弱い取引先、委託先、協力会社、再委託先を入口にするケースが現実的な脅威になっています。発注元企業が高度な対策を実施していても、委託先のアカウント管理や外部共有、クラウド利用、ログ管理に不備があれば、そこから情報漏えい・業務停止・不正侵入が起こり得ます。

SCS 評価制度が扱うリスクは単なる情報漏えいだけではありません。制度構築方針では、サプライチェーンリスクとして事業・サービス提供途絶、機密情報の漏えい・改ざん、取引先等を踏み台とした不正侵入が整理されています。[SCS-1]

リスク分類	実務上の意味	典型例
事業・サービス提供途絶	委託先やクラウドサービスの停止が、自社の受発注、製造、顧客対応、サービス提供を止めるリスク。	部品メーカー停止、クラウド障害、委託業務停止
機密情報の漏えい・改ざん	外部委託先や共有クラウド経由で、顧客情報、設計情報、契約情報、営業資料などが漏えい・改ざんされるリスク。	BPO、IT ベンダー、共同プロジェクトでの情報共有
取引先を踏み台とした不正侵入	委託先のアカウントや接続環境を起点に、発注元のシステムへ侵入されるリスク。	VPN、リモート保守、MSP、API 連携、共有アカウント

1-2 SCS 評価制度を一言でいうと

SCS 評価制度は法律で罰する制度ではなく、取引先に説明できるセキュリティ状態を★で見える化する制度です。制度構築方針でも、事業者の対策レベルを競わせる格付け制度ではなく、求められる対策の水準と対応状況を可視化するものとして整理されています。[SCS-1]

これまで発注企業ごとに異なるチェックリストや監査項目が存在し、受注側は取引先ごとに異なる形式で回答や証跡提出を求められてきました。SCS 評価制度は、この非効率を共通基準に置き換え、発注側・受注側双方の取引コストを下げつつ、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狙います。

> 実務上の要点として SCS 対応は「★を取得すること」だけが目的ではありません。
>
> 取引先から問われたときに、自社のセキュリティ対策を証跡にもとづいて説明できる状態を作ることが本質です。

1-3 任意制度だが、取引説明責任になり得る

FAQ では★3 や★4 の取得は制度として義務付けるものではなく、任意制度であると説明されています。一方で、2 社間の取引契約等において、発注元が委託先へ適切な★段階を提示し、実施状況を確認することが想定されています。[SCS-FAQ]

したがって、未取得だから直ちに行政処分や罰金が発生するわけではありません。しかし、今後は取引先から「★3 相当の対策はありますか」「★4 を取得していますか」「外部共有やログの証跡を提示できますか」と問われる場面が増える可能性があります。セキュリティは社内統制の問題にとどまらず、取引継続・新規受注・顧客信頼に関わる説明責任になります。

1-4 本書が重視する 5 つの実務テーマ

テーマ	評価で問われること	実務で整えるもの
データー元管理	重要情報がどこにあるか説明できるか。	情報資産台帳、ファイル管理基盤、保存場所ルール
アクセス管理	誰が何にアクセスできるか説明できるか。	ID 管理、グループ設計、権限棚卸し、退職者への対応履歴
外部共有統制	社外共有がルールに基づき制御されているか。	共有リンク設定、承認ルール、有効期限、外部共有レポート
ログ・証跡	対策を行っていることを第三者へ示せるか。	アクティビティログ、監査ログ、CSV レポート、確認記録
復旧・保全	誤削除、暗号化、インシデント時に復旧できるか。	状態の巻戻し、バージョン履歴、保持ポリシー、復旧手順

第 2 章 SCS 評価制度の全体像

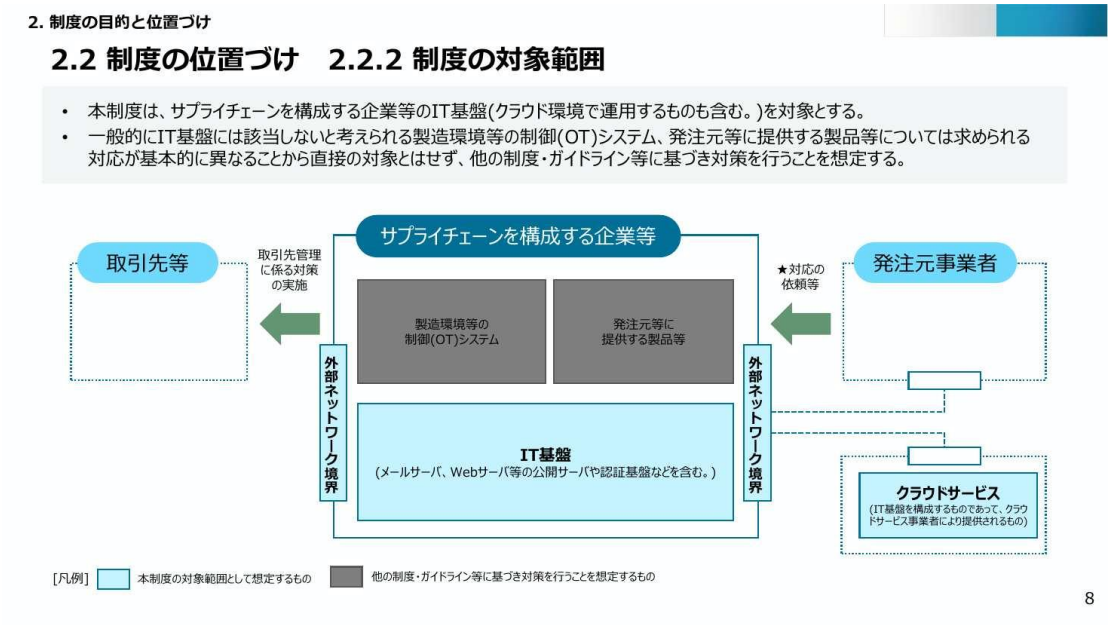


図 3 制度対象範囲: IT 基盤と外部ネットワーク境界　経済産業省のガイダンスより抜粋

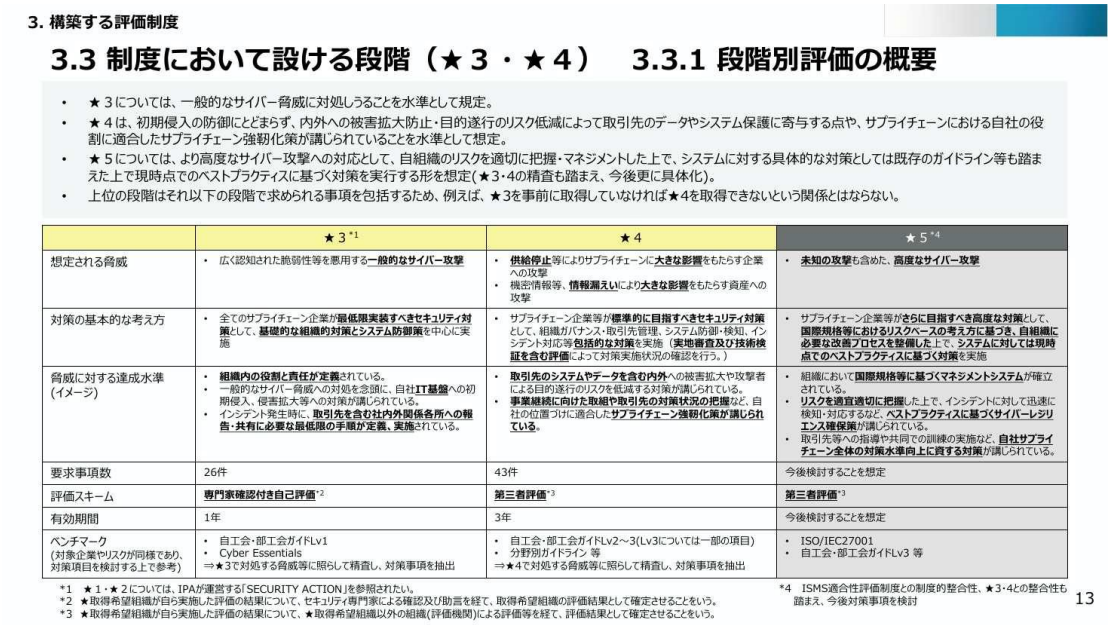


図 4 ★3・★4・★5 の段階別評価の概要　経済産業省のガイダンスより抜粋

2-1 制度の対象組織

制度構築方針では、セキュリティ対策の実施主体としてサプライチェーン企業すなわち 2 社間契約における受注者側が想定されています。ただし、サプライチェーン企業は取引関係によって発注者にもなり得るため、自社が「評価される側」であると同時に、重要な取引先の対策状況を確認する「評価を求める側」にもなります。[SCS-1]

立場	実務上の役割	必要になる準備
受注者・委託先	発注元から提示された★段階や要求事項に対して、実施状況を説明する。	自己評価、証跡整理、外部共有・アクセス管理、専門家確認または評価機関対応
発注者・委託元	取引先に求める★段階や対策水準を決め、必要に応じて確認する。	取引先重要度判定、契約条項、チェックシート、価格交渉への配慮
再委託を行う企業	自社の重要情報・事業継続に影響する再委託先を把握し、対策状況を確認する。	重要取引先台帳、再委託ルール、セキュリティ確認記録

2-2 制度対象は IT 基盤

SCS 評価制度が直接対象とするのは、サプライチェーンを構成する企業等の IT 基盤です。クラウド環境で運用するものも含まれます。一方、一般的に IT 基盤に該当しない製造環境等の制御システム、いわゆる OT システムや、発注元に提供する製品そのものは直接対象ではなく、他の制度・ガイドラインに基づく対策が想定されています。[SCS-1]

範囲	含まれる例	実務上の確認ポイント
IT 基盤	メール、ファイル共有、認証基盤、Web サーバ、クラウドサービス、端末、管理コンソール	評価対象として棚卸しし、権限・ログ・復旧・共有統制を確認する。
外部ネットワーク境界	ファイアウォール、ルータ、VPN 装置、外部接続境界	外部からの侵入・踏み台化に関わるため、設定・脆弱性・ログを確認する。
対象外になり得る領域	OT システム、提供製品そのもの	SCS の直接対象外でも、別ガイドラインや顧客要求で対策が必要になる場合がある。

2-3 ★3・★4・★5 の違い

段階	想定される水準	評価スキーム	有効期間	本書での扱い
★3	一般的なサイバー攻撃に対処するため、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対策。	専門家確認付き自己評価	1 年	実務の入口。可視化・管理・最低限の証跡整備を中心に解説。
★4	組織ガバナンス、取引先管理、検知、対応、復旧を含む包括的・標準的対策。	第三者評価および技術検証	3 年	評価機関に説明できる証跡・ログ・運用定着を中心に解説。
★5	高度な攻撃への対応、リスクベースのマネジメント、ベストプラクティスに基づく対策。	今後具体化の予定	今後に検討	本版では参考位置づけ。具体的な取得実務は対象外。

2-4 評価・登録・更新の流れ

★3 は取得希望組織が自己評価を行い、セキュリティ専門家が確認・助言し、事務局へ提出する流れが想定されています。★4 は、評価機関による第三者評価、実地審査、技術検証を経て、評価報告書をもとに登録申請を行う工程が想定されています。[SCS-1]

工程	★3	★4
1. 現状把握	要求事項に対する自己評価を実施。	自己評価を行ったうえで評価機関に依頼する前提整理を実施。
2. 確認・評価	セキュリティ専門家が自己評価の内容を確認・助言。	評価機関が文書確認、ヒアリング、証跡確認、必要に応じ技術検証を実施。
3. 是正	不足があれば修正し、専門家の了承を得る。	不適合事項について一定期間内に是正報告を行う。
4. 登録	事務局に評価結果を提出し、登録・公開。	評価報告書をもとに登録申請し、登録・公開。
5. 更新	1 年ごとに専門家確認付き自己評価を更新。	年次自己評価を評価機関へ提出し、3 年に 1 回第三者評価。

2-5 制度開始時期と留意点

FAQ では申請受付開始時期は令和 8 年度末頃、すなわち 1 月から 3 月頃が予定されていると説明されています。評価機関、提出様式、詳細な評価方法、ガイダンス資料等は、制度具体化の過程で IPA から公表される予定です。[SCS-FAQ]

> 現時点での実務判断では制度詳細が確定する前でも、情報資産の棚卸し、アクセス権整理、外部共有統制、ログ取得、復旧手順、取引先管理台帳の整備は先行して進められます。制度開始後に慌てて証跡を集めるのではなく、今から日常運用として残る仕組みに変えることが重要です。

第 3 章 SCS 評価制度で本当に見られるポイント

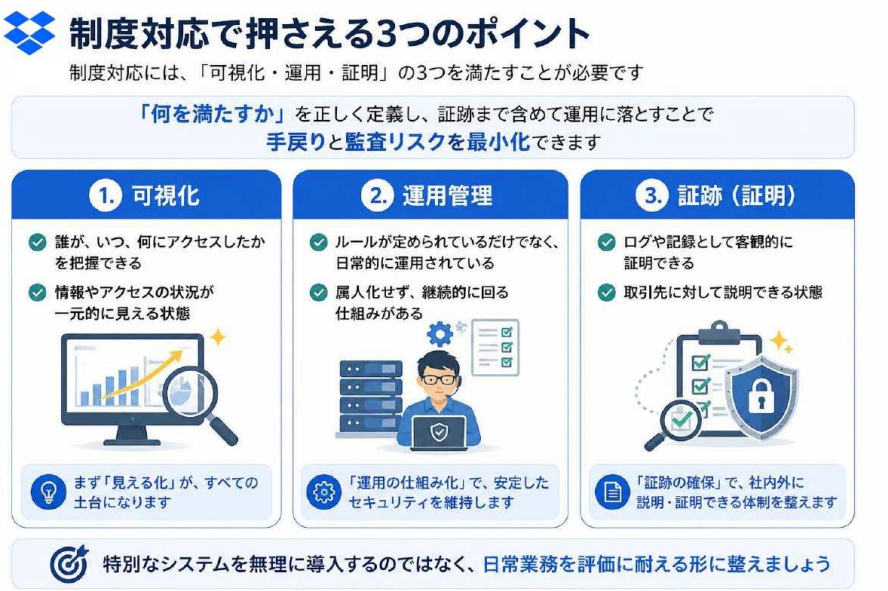


図 5 制度対応で押さえる 3 つのポイント: 可視化・運用管理・証跡

3-1 「製品導入」ではなく「運用証明」が見られる

SCS 評価制度で問われるのは、特定のセキュリティ製品を入れているかどうかではありません。FAQ でも、EDR や資産管理システムなど特定製品の導入を制度として求めるものではないとされています。[SCS-FAQ]

評価で重要になるのは、ルール、設定、運用、証跡の一貫性です。規程だけが存在しても、実際の設定やログが伴わなければ説明できません。反対に、システム機能は存在していても、設定が無効であったり、担当者がログを出せなかったりすれば、評価上の説明は弱くなります。

状態	評価上の見え方	改善の方向性
製品だけ導入済み	機能はあるが運用証跡がないため、実効性を説明しづらい。	設定値、権限一覧、ログ、運用記録を紐づける。
規程だけ整備済み	ルールはあるが、実際に守られているか不明。	ルールとシステム設定、棚卸し記録を一致させる。
ログはあるが未整理	必要なときに説明できず、監査対応が属人的になる。	検索条件、出力手順、保存場所、確認頻度を決める。
運用と証跡が連動	第三者に説明しやすく、★取得後の維持にもつながる。	継続運用として定例化する。

3-2 可視化: まず「見える状態」にする

可視化とは、情報資産、ユーザー、アクセス権、外部共有、ログ、復旧状態が把握できることです。多くの企業では、ファイルが NAS、個人 PC、メール添付、個人クラウド、部門別 SaaS に散在し、全体像が見えなくなっています。この状態では、評価取得以前に、インシデント時の影響範囲特定も困難になります。

- どの重要ファイルが、どの保管場所にあるか。
- 誰が所有者で、誰が閲覧・編集できるか。
- 外部ユーザーや共有リンクにより、社外からアクセスできるか。
- 不要な権限、退職者、期限切れプロジェクトの共有が残っていないか。
- 操作ログ、共有レポート、復旧履歴を出力できるか。

3-3 運用管理: ルールを日常業務に埋め込む

運用管理とは、規程や手順が現場で実際に使われている状態です。SCS 対応では、入社・異動・退職、プロジェクト開始・終了、外部共有開始・終了、インシデント発生時など、業務イベントごとに何をするかを決める必要があります。

業務イベント	必要な管理	残すべき証跡
入社・新規参加	必要最小限の権限付与、MFA/SSO 設定、利用ルール周知	アカウント発行記録、権限付与記録、教育受講記録
異動・役割変更	旧権限の削除、新権限の付与、共有フォルダ見直し	権限変更申請、承認記録、変更ログ
退職・契約終了	アカウント停止、端末データ削除、共有権限削除	停止記録、リモートワイプ記録、退職者チェックリスト
外部共有開始	共有範囲、期限、パスワード、ダウンロード可否を設定	共有申請、共有リンク設定、外部共有レポート
プロジェクト終了	外部ユーザー削除、共有リンク停止、成果物保管	棚卸し記録、リンク削除記録、保管先記録
インシデント発生	影響範囲確認、ログ保全、共有停止、復旧	対応記録、ログ、復旧記録、再発防止策

3-4 証跡: 「やっている」を「証明できる」に変える

証跡は、評価のためだけでなく、取引先説明、内部監査、インシデント対応、経営報告にも使う共通基盤です。実務では、証跡を評価直前に集めるのではなく、日常の運用ログ、定例点検、申請・承認、台帳更新として自然に蓄積される形にします。

証跡のカテゴリ	例	確認したい観点
規程・方針	情報セキュリティ方針、アクセス管理規程、外部共有規程	責任者、対象範囲、ルール、改定日が明確か。
台帳・一覧	情報資産台帳、SaaS 一覧、取引先台帳、アカウント一覧	最新性、所有者、重要度、更新手順があるか。
設定証跡	MFA 設定、共有リンク設定、パスワードポリシー、保持ポリシー	規程と実際の設定が一致しているか。
ログ・レポート	監査ログ、アクティビティログ、外部共有 CSV、アラート履歴	検索・出力・保管・確認の手順があるか。
運用記録	権限棚卸し、復旧テスト、インシデント訓練、是正記録	定期的に実施され、責任者が確認しているか。

第 4 章 要求事項 7 分類を実務に落とし込む

図 6 SCS 評価制度の要求事項 7 分類　経済産業省のガイダンスを抜粋

制度構築方針では、NIST Cyber Security Framework の機能に対応した 6 分類に、取引先管理を加えた 7 分類で要求事項が整理されています。本章では、各分類について「制度上の狙い」「実務でやること」「必要証跡」「Dropbox が支援しやすい領域」を整理します。[SCS-1]

4-1 ガバナンスの整備

組織としてセキュリティを推進する責任・権限・方針・報告体制を明確にする領域です。情報システム担当者の努力だけではなく、経営層の関与、責任者の任命、年次点検、改善サイクルが重要です。

実務項目	やること	証跡例
責任者・担当部署	CISO 相当、情報システム責任者、セキュリティ担当部署を明確化する。	体制図、責任者一覧、職務分掌
方針・規程	情報セキュリティ方針、外部共有規程、アクセス管理規程を定める。	方針文書、規程、改定履歴
経営報告	重大リスク、外部共有状況、インシデント、是正状況を経営層に報告する。	会議資料、議事録、承認記録
改善管理	点検結果や評価指摘に対して是正計画を作る。	点検記録、是正管理表

Dropbox で支援できる領域: Dropbox の直接機能だけでは完結しません。ただし、管理コンソールの設定・ログ・レポートを経営報告資料に組み込み、外部共有やアクセス権の実態を数値で示すことで、ガバナンスの実効性を支援できます。

4-2 取引先管理

サプライチェーン制度の中核です。自社が委託先として評価されるだけでなく自社から見た重要取引先の対策状況を把握し、必要な役割・責任を明確にします。

実務項目	やること	証跡例
重要取引先の特定	機密情報共有、事業継続影響、システム接続の観点で重要取引先を特定する。	取引先台帳、重要度判定表
情報共有範囲	取引先ごとに共有する情報、共有方法、共有期間を定める。	契約書、共有申請、共有フォルダー一覧
対策状況確認	必要に応じて★取得状況やチェックシートを確認する。	回答票、確認メール、訪問記録
再委託管理	再委託先が重要情報を扱う場合の確認方法を定める。	再委託申請、承認記録

Dropbox で支援できる領域: Dropbox では、社外共有先、共有リンク、外部ユーザー、共有ファイルのレポートを取得し、どの取引先と何を共有しているかを確認できます。取引先管理台帳と外部共有レポートを突合する運用が有効です。

4-3 リスクの特定

自社の IT 基盤、情報資産、外部サービス、外部公開システム、クラウド利用を把握し、重要情報とリスクの所在を明確にします。

実務項目	やること	証跡例
情報資産棚卸し	重要情報、保存場所、所有者、機密区分を一覧化する。	情報資産台帳
IT 基盤把握	利用中の SaaS、認証基盤、端末、ネットワークを整理する。	SaaS 一覧、構成図
外部サービス管理	外部情報サービスの利用可否、責任共有、セキュリティ確認を	クラウド利用台帳、契約・設定資料

実務項目	やること	証跡例
	行う。	
機密区分	契約書、設計情報、個人情報などの重要度を分類する。	分類基準、ラベル、保管ルール

Dropbox で支援できる領域 Dropbox に業務ファイルを集約し、チームフォルダ、所有者、共有先、アクティビティを確認できる状態にすると、情報資産の所在把握と棚卸しが容易になります。

4-4 攻撃等の防御

不正アクセス、認証の突破、マルウェア、情報漏えい、過剰共有を防ぐ領域です。ID 管理、認証強化、外部共有制御、暗号化、端末・ソフトウェア管理が中心です。

実務項目	やること	証跡例
ID やアカウントの管理	入社・異動・退職に合わせてアカウントを管理する。	ID 台帳、停止記録
認証の強化	MFA、SSO、パスワード強度、Web セッションを管理する。	設定画面、ポリシー、ログ
権限の管理	必要最小限の権限付与と定期棚卸しを行う。	権限一覧、棚卸し記録
外部共有の制御	共有リンク、期限、パスワード、DL 可否を制御する。	外部共有レポート、設定画面
データ保護	重要データの暗号化、保全、復旧を整備する。	暗号化仕様、保持ポリシー

Dropbox で支援できる領域: Dropbox では、SSO、2FA、パスワード制御、外部共有設定、共有リンクのパスワード・有効期限・ダウンロード制限、チームフォルダ権限、リモートワイプなどにより、防御策の一部を実装できます。

4-5 攻撃等の検知

攻撃や不審な操作に早く気づくための領域です。ログ取得、アラート、外部共有の監視、大量削除、移動の検知が重要です。

実務項目	やること	証跡例
ログの取得	ログイン、ファイル操作、共有、管理者操作を記録する。	アクティビティログ、監査ログ
外部共有の監視	社外共有中のファイル、フォルダ、リンクを定期確認する。	外部共有 CSV、確認記録
異常検知	大量削除、ランサムウェア、マルウェア共有、リスクのある地域からのログインを検知する。	アラート履歴、対応記録
定期レビュー	ログを確認する担当者、頻度、観点を定める。	ログレビュー記録

Dropbox で支援できる領域: Dropbox のセキュリティアラート、アクティビティログ、外部共有レポートは、異常操作や共有状態の検知・確認に活用できます。

4-6 インシデントへの対応

事故発生時に、誰が、何を、どの順番で行うかを明確にする領域です。初動、影響範囲確認、取引先連絡、証跡保全、是正が重要です。

実務項目	やること	証跡例
初動対応	検知後の連絡先、判断者、停止手順を決める。	インシデント対応手順、連絡網
影響範囲調査	操作ログ、共有先、対象ファイルを確認する。	ログ抽出結果、調査記録
外部連絡	取引先・顧客・関係部署への報告要否を判断する。	報告書、連絡記録
再発防止	原因、是正、予防策を記録し、経営層へ報告する。	再発防止策、是正記録

Dropbox で支援できる領域 Dropbox では、問題がある共有リンクの停止、外部ユーザー削除、対象ファイルの復元、アラートステータス管理、ユーザー停止などを初動・封じ込めに活用できます。

4-7 インシデントからの復旧

誤削除、ランサムウェア、改ざん、アカウント不正利用などが発生した後、業務を再開できるようにする領域です。

実務項目	やること	証跡例
復旧方針	どのデータを、どの時点まで、どの時間内に戻すかを決める。	RPO/RTO、復旧方針
復旧手順	削除ファイル復元、バージョン戻し、フォルダ復旧の手順を定める。	復旧手順書
復旧テスト	定期的に復旧できることを確認する。	復旧テスト記録
データ保全	法的・規制上必要なデータを保持する。	保持ポリシー、リーガルホールド

Dropbox で支援できる領域 Dropbox のリウインド、削除ファイル復元、バージョン履歴、データ保持、リーガルホールドは復旧・保全の実務に活用できます。

第 5 章 ★3 取得実務

図 7 ★3 における最低限の可視化・管理

5-1 ★3 のゴール

★3 のゴールは一般的なサイバー攻撃に対して最低限の組織的対策とシステム防御策を整え、取引先へ説明できる状態を作ることです。制度構築方針では、★3 について、組織内の役割と責任、初期侵入・侵害拡大への基礎的対策、インシデント時の報告・共有手順などが達成水準のイメージとして整理されています。[SCS-1] ★3 は「完璧なセキュリティ」ではなく、最低限の可視化・管理・証跡を整える段階です。実務では、まず情報資産、アクセス権、外部共有、認証、ログ、復旧の 6 領域を優先して整えます。

優先領域	★3 での到達イメージ	最低限の成果物
情報資産	重要情報と保存場所を把握している。	情報資産台帳、保存場所一覧
アクセス権	ユーザーと権限を把握し、不要権限を削除できる。	アカウント一覧、権限一覧、棚卸し記録
外部共有	外部共有のルールがあり、現状を確認できる。	外部共有規程、外部共有一覧
認証	MFA、パスワード、退職者停止など基本対策がある。	認証設定、ID 管理手順
ログ	主要な操作ログを取得し、確認できる。	アクティビティログ、ログ取得手順
復旧	削除・改ざん時に戻せる手順がある。	復旧手順、テスト記録

5-2 ★3 取得プロジェクトの進め方

ステップ	実施内容	主担当	成果物
1. 適用範囲の定義	対象となる法人、部門、IT 基盤、クラウド、共有環境を定義する。	情シス/セキュリティ	適用範囲定義書
2. 現状の棚卸し	情報資産、ID、外部共有、取引先、ログ、復旧を棚卸しする。	情シス/各部門	棚卸し台帳
3. ギャップ分析	要求事項と現状の差分を整理する。	セキュリティ担当	ギャップ一覧
4. ルールの整備	最低限の規程・手順を作成または改定する。	情シス/法務/総務	規程・手順書
5. 技術要素の設定	MFA、共有制御、ログ取得、復旧設定を整える。	情シス	設定証跡
6. 証跡の整理	評価で示す証跡をフォルダ構成化し、最新版を保管する。	事務局/情シス	証跡フォルダ
7. 専門家への確認	セキュリティ専門家に自己評価と証跡を確認してもらう。	プロジェクト責任者	確認結果、是正記録

5-3 ★3 の証跡フォルダ構成例

証跡は評価直前に散在したファイルを探すのではなく、最初から評価分類に沿って保管することを推奨します。以下は、Dropbox 等のファイル管理基盤上で管理する場合のフォルダ構成例です。

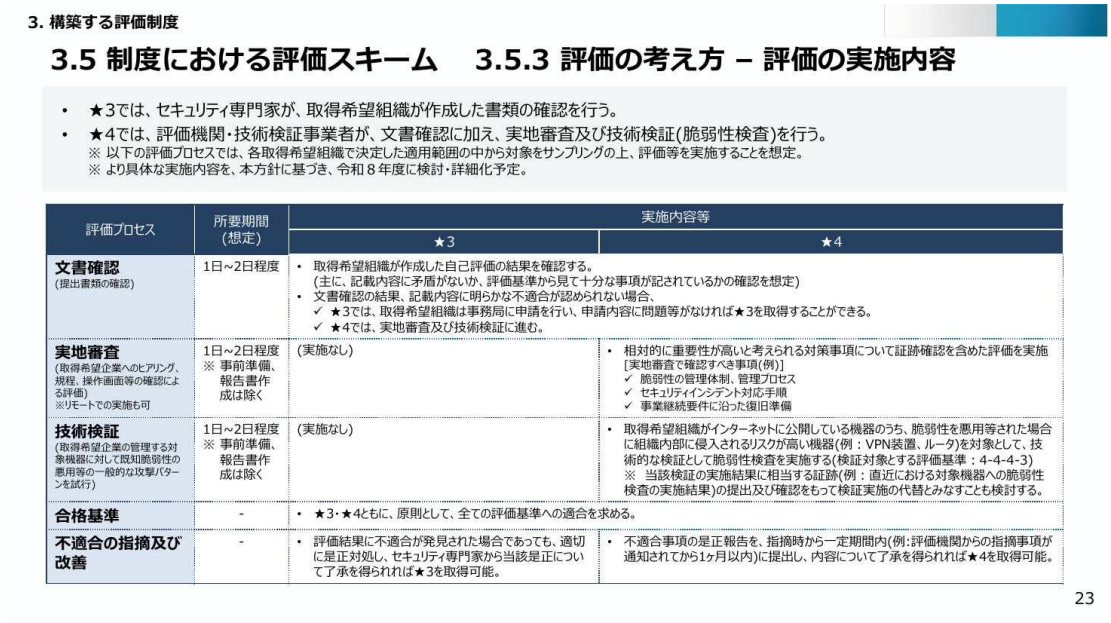
フォルダ	格納する証跡の例
01_方針・体制	情報セキュリティ方針、体制図、責任者一覧、経営報告資料
02_情報資産・IT 基盤	情報資産台帳、SaaS 一覧、ネットワーク構成、適用範囲定義
03_ID・アクセス管理	ID 台帳、権限一覧、MFA 設定、SSO 設定、退職者停止記録
04_外部共有管理	外部共有規程、共有リンク一覧、外部共有レポート、棚卸し記録
05_ログ・検知	アクティビティログ、監査ログ、アラート履歴、ログ確認記録
06_インシデント対応	対応手順、連絡網、訓練記録、対応記録、再発防止策
07_復旧・保全	復旧手順、バージョン履歴確認、削除ファイル復元手順、復旧テスト記録
08_取引先管理	重要取引先台帳、契約条項、セキュリティ確認票、是正依頼
09_自己評価・専門家確認	自己評価表、専門家コメント、是正完了記録、申請資料

5-4 専門家確認で説明しやすい状態

専門家確認では、自己評価の記載内容と実際の証跡に矛盾がないことが重要です。たとえば「外部共有は有効期限を設定している」と記載する場合、規程、管理コンソール設定、外部共有レポート、例外管理の記録が一致している必要があります。

自己評価で書きがちな表現	不足しがちな点	補強すべき証跡
MFA を利用している	全員必須なのか、一部は任意なのかが、不明になっている	MFA 必須設定、対象者一覧、例外承認、回避策
外部共有を管理している	共有リンクの棚卸し頻度や責任者が不明になっている	外部共有レポート、棚卸し記録、削除記録
ログを取得している	どのログを誰が確認するか不明。	ログ取得設定、ログ確認手順、確認記録
復旧できる	実際に復旧した記録がない。	復旧テスト記録、復旧手順、対象範囲
取引先を管理している	重要取引先の定義が曖昧。	重要度判定基準、取引先台帳、確認票

第 6 章 ★4 取得実務



3. 構築する評価制度

3.5 制度における評価スキーム　3.5.3 評価の考え方 – 評価の実施内容

- ★3では、セキュリティ専門家が、取得希望組織が作成した書類の確認を行う。
- ★4では、評価機関・技術検証事業者が、文書確認に加え、実地審査及び技術検証(脆弱性検査)を行う。
  ※ 以下の評価プロセスでは、各取得希望組織で決定した適用範囲の中から対象をサンプリングの上、評価等を実施することを想定。
  ※ より具体な実施内容を、本方針に基づき、令和８年度に検討・詳細化予定。

評価プロセス	所要期間(想定)	実施内容等 ★3	実施内容等 ★4
文書確認 (提出書類の確認)	1日~2日程度	• 取得希望組織が作成した自己評価の結果を確認する。 (主に、記載内容に矛盾がないか、評価基準から見て十分な事項が記されているかの確認を想定) • 文書確認の結果、記載内容に明らかな不適合が認められない場合、 ✓ ★3では、取得希望組織は事務局に申請を行い、申請内容に問題等がなければ★3を取得することができる。 ✓ ★4では、実地審査及び技術検証に進む。	
実地審査 (取得希望企業へのヒアリング、規程、操作画面等の確認による評価) ※リモートでの実施も可	1日~2日程度 ※ 事前準備、報告書作成は除く	(実施なし)	• 相対的に重要性が高いと考えられる対策事項について証跡確認を含めた評価を実施 [実地審査で確認すべき事項(例)] ✓ 脆弱性の管理体制、管理プロセス ✓ セキュリティインシデント対応手順 ✓ 事業継続要件に沿った復旧準備
技術検証 (取得希望企業の管理する対象機器に対して既知脆弱性の悪用等の一般的な攻撃パターンを試行)	1日~2日程度 ※ 事前準備、報告書作成は除く	(実施なし)	• 取得希望組織がインターネットに公開している機器のうち、脆弱性を悪用等された場合に組織内部に侵入されるリスクが高い機器(例：VPN装置、ルータ)を対象として、技術的な検証として脆弱性検査を実施する(検証対象とする評価基準：4-4-4-3) ※ 当該検証の実施結果に相当する証跡(例：直近における対象機器への脆弱性検査の実施結果)の提出及び確認をもって検証実施の代替とみなすことも検討する。
合格基準	-	• ★3・★4ともに、原則として、全ての評価基準への適合を求める。	
不適合の指摘及び改善	-	• 評価結果に不適合が発見された場合であっても、適切に是正対処し、セキュリティ専門家から当該是正について了承を得られれば★3を取得可能。	• 不適合事項の是正報告を、指摘時から一定期間内(例:評価機関からの指摘事項が通知されてから1ヶ月以内)に提出し、内容について了承を得られれば★4を取得可能。

23

図 8 ★3/★4 の評価実施内容　経済産業省のガイダンスより抜粋

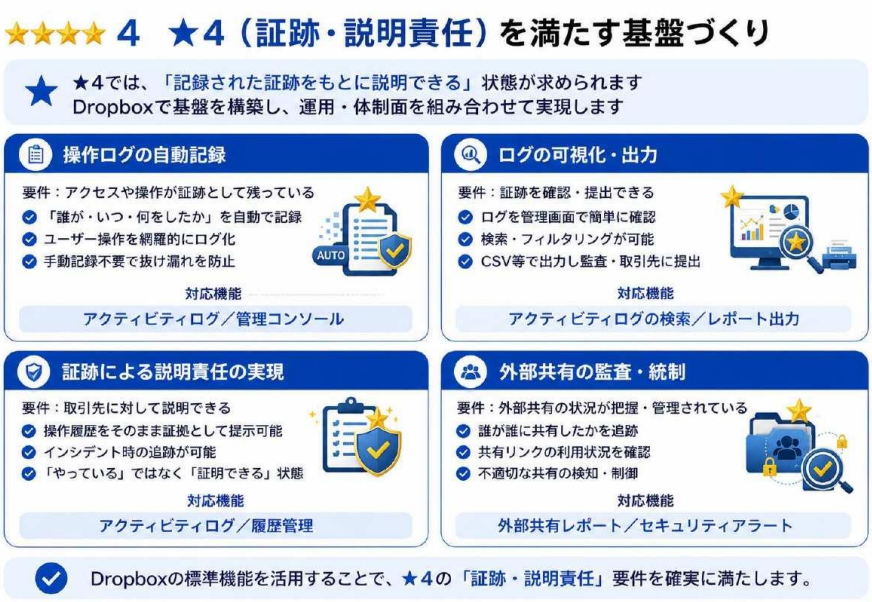


図 9 ★4 における証跡・説明責任の基盤（Dropbox にデータを集積した場合）

6-1 ★4 のゴール

★4 は、★3 の基礎的な可視化・管理に加え、組織ガバナンス、取引先管理、システム防御・検知、インシデント対応、復旧を包括的に実装する段階です。制度構築方針では、★4 について、実地審査および技術検証を含む評価によって対策実施状況を確認することが想定されています。[SCS-1]

★4 で重視されるのは、評価機関に対して「運用の実態」を説明できることです。文書確認に加え、ヒアリング、画面確認、設定確認、ログ確認、証跡確認が行われる可能性があります。

6-2 ★4 で★3 から強化すべき点

領域	★3 での状態	★4 で求めたい状態
ガバナンス	担当者・方針がある。	経営層への定期報告、不備の是正、改善サイクルがある。
取引先の管理	重要な共有先を把握している。	重要取引先の対策状況を年次等で確認し、役割・責任を明確化している。
リスク特定	情報資産と IT 基盤を把握している。	脆弱性や外部サービスの状況を継続的に反映している。
防御	MFA、アクセス権、外部共有制御がある。	多層防御、ログ収集、社内外通信、重要データ暗号化・保全まで説明できる。
検知	ログを取得している。	異常検知、アラート対応、ログ分析の記録がある。
対応	手順書がある。	訓練、実績、取引先連絡、証跡保全まで含む運用がある。
復旧	復旧手段がある。	復旧ポイント・復旧時間を踏まえた手順とテスト記録がある。

6-3 実地審査への備え

★4 では、文書だけでなく実地審査が想定されます。実地審査では、規程に書かれた内容が実際の設定・運用と一致しているかが問われます。次の観点で事前リハーサルを行うと効果的です。

審査観点	確認される可能性	準備方法
体制	責任者は誰か。経営層への報告はあるか。	体制図、議事録、報告資料をすぐ提示できるようにする。
アクセス権	特定フォルダに誰がアクセスできるか。退職者権限は削除済みか。	権限一覧、棚卸し記録、管理画面の表示手順を準備する。
外部共有	どのファイルが外部共有されているか。期限やパスワードは設定されているか。	外部共有レポート、リンク設定、例外承認を準備する。
ログ	誰がいつ何を操作したか追跡できるか。	検索条件、サンプルログ、CSV 出力手順を準備する。
インシデント	不審操作があった場合に誰が対応するか。	手順書、訓練記録、過去の対応記録を準備する。
復旧	削除・暗号化時にどこまで戻せるか。	削除ファイル復元、バージョン履歴、復旧テスト記録を準備する。

6-4 不適合への対応

制度構築方針では、★4 評価で不適合が発見された場合でも、一定期間内に是正報告を提出し、内容について了承を得られれば★4 取得が可能とされています。[SCS-1] 実務では、指摘事項を「設定変更で直せるもの」「規程改定が必要なもの」「運用定着が必要なもの」に分けると対応しやすくなります。

不適合タイプ	例	是正方針	証跡
設定の不足	共有リンクに有効期限がない、MFA が任意になっている。	管理コンソール設定を変更し、対象範囲を確認する。	変更前後の設定画面、変更ログ
文書の不足	外部共有ルールや復旧手順が文書化されていない。	規程・手順書を作成し、関係者へ周知する。	文書、承認記録、周知記録
運用手順の未実施	権限棚卸しやログ確認を実施していない。	定例運用として実施し、次回以降の予定を設定する。	棚卸し記録、ログ確認記録、運用カレンダー
取引先への確認不足	重要取引先の対策状況を把握していない。	重要取引先を特定し、確認票を回収する。	重要度判定表、確認票、回答記録

第 7 章 Dropbox で実現する SCS 対応

図 10 Dropbox を活用した SCS 準備ロードマップ

本章の位置づけ: 本章は Dropbox を導入すれば SCS 評価制度の全項目を自動的に満たせるという趣旨ではありません。Dropbox は、SCS 対応のうち、情報資産管理、アクセス管理、外部共有統制、ログ・証跡、検知、復旧、データ保全を支援する基盤です。外部共有統制・監査証跡・権限是正にはアクティビティログや Dropbox Protect（保護とコントロール）で扱います。組織体制、規程、取引先の管理、教育、経営層への報告などは別途整備が必要です。

7-1 Dropbox が支援できる領域の全体像

SCS 実務領域	Dropbox で使う主な機能	評価で提示しやすい証跡（何で裏付けられるか）
情報資産の管理	チームフォルダ、共有フォルダ、グループ、所有者管理	フォルダ構成、権限一覧、情報資産台帳との対応表
認証や ID の管理	SSO、2FA、パスワード制御、Web セッション制御、メンバー停止	管理コンソール設定、対象者一覧、停止・削除記録
端末・離任への対応	メンバー停止、リモートワイプ	リモートワイプ履歴、退職者チェックリスト
外部共有の統制	外部共有設定、承認済みリスト、共有リンク設定、パスワード、有効期限、ダウンロード制限	外部共有レポート、共有リンク設定、例外承認記録
横断的な可視化と是正	保護とコントロール、レポート、フィルタ、CSV 出力、リンク/共同編集者の是正、ポリシー	共有状態 CSV、アクション履歴、是正前後比較、ポリシー設定
ログ・証跡	アクティビティページ、外部共有レポート、ファイルアクティビティ	CSV レポート、ログレビュー記録、調査記録
検知・アラート	セキュリティアラート、ランサムウェア検知、大量削除・移動検知	アラート履歴、対応ステータス、是正記録
復旧・証跡保全	ファイルの巻戻し、削除ファイル復元、バージョン履歴、データ保持、リーガルホールド	復旧手順、復旧テスト記録、保持ポリシー、ホールド記録

7-2 データー元管理: チームフォルダとグループ設計

Dropbox のチームフォルダは、Dropbox チームアカウントで利用できる共有基盤です。チームフォルダはグループ単位で共有でき、グループには編集者または閲覧のみのロールを割り当てられます。管理者が外部共有を許可している場合、チームフォルダ内のコンテンツを社外ユーザーに共有できます。[DBX-TEAM]

SCS 対応では、ファイルサーバや NAS の代替案として単にファイルを移行するだけでなく、部門、プロジェクト、機密区分、取引先共有の観点でフォルダ設計を行います。特に、上位階層の権限が意図せず下位へ広がること、個人単位の例外権限が増えること、終了プロジェクトの外部共有が残ることを避ける設計が重要です。

設計項目	推奨する考え方	SCS 証跡
フォルダ階層	部門フォルダ、プロジェクトフォルダ、取引先共有フォルダ、アーカイブを分ける。	フォルダ設計書、情報資産台帳
権限付与	個人ではなくグループを基本にする。編集者と閲覧のみを分ける。	グループ一覧、権限一覧
外部共有	社外共有専用フォルダを定義し、期限・パスワード・承認ルールを付ける。	外部共有規程、共有レポート
機密区分	重要情報はアクセス範囲を限定し、共有リンクを原則禁止または制限する。	機密区分表、設定証跡
棚卸し	四半期または半期ごとに権限と外部共有を棚卸しする。	棚卸し記録、削除記録

実装時の注意: チームフォルダ内の一部フォルダにアクセス制限をかける運用は可能ですが、設計が複雑になりすぎると管理負荷が上がります。SCS 対応では、実装と説明責任のバランスを取る必要があります。評価イベントで説明しやすい単純な権限モデルを検討することも可能です。

7-3 認証・ID 管理: SSO、多要素認証、パスワード、Web セッション

Dropbox では、Advanced、Enterprise ライセンス等のチーム管理者が SSO を有効化することが可能です。SSO を必須にし、チームメンバーは Dropbox パスワードではなく、中央の ID プロバイダで認証することが可能です。ただし、管理者アカウントなど一部の扱いや、多要素認証の管理主体は ID プロバイダになる場合があるため、IdP 側の証跡も併せて管理します。[DBX-SSO]

多要素認証については、管理者が全員または一部メンバーに複数の要素の認可を要求できます。SSO を利用している場合は、Dropbox 管理コンソールまたは ID プロバイダ側のいずれで統制するかを明確にします。[DBX-2FA] また、Dropbox のパスワード制御では、チームメンバーに強力なパスワードを要求でき、強度設定を変更すると新しいパスワード作成が求められ、Web セッションからログアウトされます。[DBX-PWD]

管理項目	Dropbox での実装	SCS 観点の証跡	留意点
SSO	オプションまたは必須として設定。「必須」では Dropbox パスワードではなく IdP 認証を利用。	SSO 設定画面、IdP 設定、対象者一覧	IdP 側の MFA・ログも証跡対象にする。
2FA	全員または一部メンバーに要求。テキストメッセージまたは認証アプリ等で認証。	多要素認証の要求設定、対象者、例外承認やケースの提出	SSO 利用時は IdP 側で管理する場合がある。
パスワード強度	パスワード強度を設定。	パスワード制御の設定、変更履歴	パスワードの運用規程と一致させる。
Web セッション	特定の期間またはアイドル時間に基づき dropbox.com のセッションを期限切れにする。	セッション制御の設定	–

7-4 入退社・異動対応: メンバー停止とリモートワイプ

退職者や契約終了者のアクセス権が残ることは、SCS 対応で避けるべき典型的な不備です。Dropbox では、特定の管理者がメンバーを一時停止でき、一時停止されたメンバーはチームアカウント、ファイル、フォルダ、ペーパーへのアクセスを失い、すべてのデバイスからログアウトされます。[DBX-SUSPEND]

また、Dropbox のリモートワイプは、メンバーが退職した場合やデバイス紛失・盗難時に、管理者がそのメンバーのチームアカウントに属する Dropbox ファイルをデバイスから削除するための機能です。Dropbox はリモートワイプは取り消せないこと、個人用アカウント等には影響しないことも説明しています。[DBX-WIPE]

イベント	Dropbox 操作	残す証跡	SCS 実務メモ
退職	メンバー停止、必要に応じてファイル移管、リモートワイプ。	退職者チェックリスト、停止ログ、ワイプステータス	人事情報と連動し、当日中の停止を標準化する。
異動	所属グループ変更、旧フォルダ権限削除、新権限付与。	権限変更申請、承認、変更ログ	旧権限の削除漏れが最も起こりやすい。
紛失・盗難	対象デバイスにリモートワイプを実施。	ワイプ指示、完了状況、インシデント記録	端末管理ツールの記録と合わせて保管する。

7-5 外部共有統制: 管理者設定、承認済みリスト、リンク制御

図 11 Dropbox による外部共有・ログ・復旧の実務対応例

Dropbox は管理者がチーム外との共有を許可または制限できること、外部共有の承認済みリストをメールアドレスまたはドメインで設定できること、共有リンクの既定アクセス権限や編集/閲覧権限、パスワード、有効期限を管理できることが説明しています。[DBX-EXT]

共有リンクの個別設定では、パスワード、有効期限、ダウンロード無効化、リンクアクセス範囲の制限が利用できます。なお、共有リンクの設定はリンク経由でアクセスするユーザーに影響し、ファイルやフォルダに直接共有されたユーザーの権限は残る点も説明されています。この違いは評価説明時の重要な注意点です。[DBX-LINK]

統制項目	具体設定	評価での説明	証跡
外部共有の可否	チーム外へのファイル・フォルダ共有を許可/制限。	どの情報を社外共有可能にしているか。	外部共有の設定画面、規程
承認済みリスト	許可するメールアドレスまたはドメインを設定。	取引先・委託先をリスト化し、例外を管理しているか。	承認済みリスト、例外承認
リンク既定アクセス	全て、招待者のみ、チームメンバーのみ等を選択。	原則として最小範囲を既定にしているか。	共有リンク設定
パスワード	共有リンクにパスワードを設定。	機密情報や社外共有で追加認証を要求して	リンク設定、運用手順

統制項目	具体設定	評価での説明	証跡
		いるか。	
有効期限	共有リンクの期限を設定。	期限切れリンクが放置されない運用か。	リンクレポート、期限設定
ダウンロード制限	必要に応じてダウンロードを無効化。	閲覧のみで十分な共有に対して DL を制限しているか。	リンク設定、共有申請

外部共有の評価でよくある落とし穴: 共有リンクを制限していても、ファイルやフォルダに直接追加された外部ユーザーのアクセスは別管理です。SCS 対応では「共有リンク一覧」と「直接追加された外部ユーザー一覧」の両方を棚卸しします。

7-6 外部共有の監視と CSV レポート

Dropbox では、管理者が管理コンソールのアクティビティページや外部共有レポートを使ってデータがチーム内外でどのように共有されているかを追跡できると説明されています。外部共有レポートは CSV として Dropbox Business Reports フォルダに保存され、アイテムの種類、名前、共有者、共有先、アクセス権、共有先ドメイン、共有方法、アクセス有無、有効期限、パスワード、ダウンロード設定などの項目を含みます。[DBX-MONITOR]

SCS 評価では、この CSV レポートを「外部共有棚卸し」の証跡として利用できます。単に出力するだけでなく、レポートを確認した日、確認者、是正対象、削除・期限変更・権限変更の結果を残すことが重要です。

レポート項目	見るべきリスク	是正例
共有先のドメイン	未承認ドメインや個人メールに共有されていないか。	承認済みリストにない共有を停止、例外承認を取得
アクセス権	編集権限が過剰に付いていないか。	閲覧のみへ変更、共有相手を限定
有効期限	期限なしリンクが残っていないか。	期限設定、リンク削除
パスワード	機密情報の共有リンクにパスワードがないか。	パスワード設定、共有方法変更
ダウンロード設定	閲覧のみでよい資料が DL 可能になっていないか。	ダウンロード制限を設定
未更新アクセス	古い共有が放置されていないか。	共有停止、アーカイブ化

7-7 Dropbox Protect（保護とコントロール）: 横断的な共有・権限の可視化とアクション

図 12 Dropbox Protect（保護とコントロール）による横断的な共有の可視化とアクション

保護とコントロール（Dropbox Protect）は、Dropbox の管理者向けデータ保護・共有統制機能として、本書では外部共有統制、権限棚卸し、証跡化、監査対応に関係する領域として扱います。本書では Dropbox Protect（保護とコントロール）が SCS 評価制度で求められる外部共有統制、権限棚卸し、証跡化、監査対応に直接的に関係するためその対象に含めます。Dropbox では、Dropbox Protect（保護とコントロール）は Dropbox、Microsoft 365（OneDrive/SharePoint）、Google ドライブといった接続済みアプリを横断して、ファイルへのアクセス状況を表示・制御・監視し、権限変更の記録を残す機能として位置付けています。[DBX-PAC-ADMIN]

観点	保護とコントロール（Dropbox Protect）で確認できること	SCS 実務へのつながり
所有者・所在	アイテム名、アプリ、所有者、所有者のメールアドレス、識別子、更新日、作成/アップロード時期など。	情報資産の所在把握、責任者確認、監査時の説明資料。
共有先	内部ユーザー、外部ドメイン、個人メールアカウント、リンク種別、権限レベルを一覧化。	外部共有棚卸し、過剰権限の発見、取引先共有の確認。
リンクの種別	制限付き、社内、公開、社外、ゲスト、対象、外部などのリンク分類。	公開リンク、全社リンク、外部共有リンクのリスク評価。
フィルタ	更新日、ファイル種別、アプリ、共有状態などで絞り込み。	重要領域に絞った点検、評価対象証跡の作成。
レポート	概要や放置されたアクセスなど、幅広い長期間放置された共有	棚卸し計画、古い共有リンクの整理、監査準備。

観点	保護とコントロール(Dropbox Protect)で確認できること	SCS 実務へのつながり
	を把握。	
是正アクション	コラボレーター追加/削除、リンク追加/削除、共有停止、削除など。	インシデント初動、権限是正、是正記録の作成。
CSV 出力	フィルタ済みの選択結果や一覧を CSV に出力可能。	監査、分析、報告、取引先説明用の証跡化。

運用上の注意: Dropbox Protect(保護とコントロール)の CSV には、ファイル名、所有者、共同編集者、リンク種別、権限レベルなど機微なメタデータが含まれ得ます。評価・監査用に出力する場合は、対象をフィルタで絞り込み、保存場所、アクセス権、保存期間、持ち出し可否を定めてください。[DBX-PAC-CSV]

7-8 監査・インシデントレスポンス・侵害からの復旧での活用

SCS 評価制度の実務では、平時の監査証跡と、有事のインシデント対応証跡を同じ基盤で管理できることが重要です。Dropbox は平時にはアクセス権・外部共有・古い共有の棚卸し、有事にはアラート確認、影響範囲調査、共有停止、アカウント停止、復元、証跡保全に活用できます。特に、取引先への説明では「いつ、誰が、何にアクセスし、どの共有があり、どの是正をしたか」を一連の記録として提示できることが重要です。

局面	Dropbox で有用な機能	実務での使い方	残すべき証跡
監査・評価	Dropbox Protect(保護とコントロール)、CSV 出力、アクティビティログ、外部共有レポート、保持ポリシー	共有状態、古いアクセス、個人メール共有、Public リンク、権限変更を定期点検する。	CSV、点検記録、是正前後の比較、承認記録
検知	セキュリティアラート、ランサムウェア検知、大量削除/大量移動、マルウェア共有、リスク国ログイン	疑わしい操作を早期把握し、担当者に通知する。	アラート詳細、発生日、対象者、対象ファイル、影響範囲
封じ込め	メンバー停止、Web セッション管理、リモートワイプ、リンク削除、共有停止、コラボレーター削除	侵害された可能性のあるアカウントや共有経路を止める。	停止記録、ワイプステータス、共有停止記録
調査	ファイルアクティビティ、アクティビティログ、Dropbox Protect(保護とコントロール)、アイテムの詳細、アクション履歴	誰が、いつ、何を変更・削除・共有したかを調査する。	ログ抽出、時系列、対象アイテム一覧
復旧	巻戻し、削除ファイル復元、バージョン履歴、アクティビティページからの復元導線	削除・改ざんされたファイルを安全な版へ戻す。	復元対象、復元時点、復元者、復元後確認
証跡の保全	データガバナンス、リーガルホールド、CSV サマリー、保持ポリシー	紛争・内部不正・取引先説明に備えて証拠を保全する。	ホールド記録、保持設定、エクスポート CSV

侵害からの復旧の考え方: 侵害後の復旧は「戻す」だけではなく、1) 侵害アカウント・端末・共有経路の封じ込め、2) ログと共有状態からの影響範囲特定、3) 改ざん・削除データの復元、4) 証跡保全、5) 再発防止設定の確認、6) 取引先・評価機関へ説明できる記録化、の順で進めます。Dropbox はこのうち、ファイル共有領域の可視化・封じ込め・復元・証跡化を支援します。

7-9 ログ・証跡: アクティビティ、ファイル履歴、調査記録

Dropbox のファイルアクティビティでは、ファイルやフォルダに対する追加、編集、移動、名前変更、バージョン履歴による復元などの活動を確認できます。アクティビティタブでは、誰がいつ操作したかを確認でき、共有操作も表示されます。ただし、Dropbox 外にダウンロードして編集した内容などは記録されない場合があるため、ログの限界も評価説明に含めるべきです。[DBX-ACTIVITY]

ログおよび UI の用途	Dropbox で確認するもの	証跡化の方法
外部共有の調査	外部共有レポート、Dropbox Protect(保護とコントロール) CSV	CSV 出力し、調査記録とセットで保管。
不正操作の調査	ファイルアクティビティ、ログイン履歴、管理者操作	対象期間・対象者・対象ファイルを絞って抽出。
変更された権限の確認	共有フォルダやリンクの作成・変更・削除イベント、アクション履歴	権限変更申請とログを突合。
復旧の確認作業	バージョン履歴、削除ファイル復元	復旧操作記録、復旧後確認結果を残す。
定例レビュー	月次/四半期の外部共有、アラート、メンバー停止	レビュー議事録、是正管理表を作成。

7-10 検知・アラート: ランサムウェア、マルウェア、大量操作

Dropbox では、セキュリティアラートにより、不審な挙動、リスクの高いアクティビティ、潜在的なデータ漏えいが検出された場合に通知されます。トリガーには、ランサムウェア検知、大量削除、大量移動、機密コンテンツの外部共有、チーム外からのマルウェア共有、チーム内マルウェア共有、頻繁なログイン試行、リスクの高い国からのログインなどが含まれます。[DBX-ALERT]

アラートでは、誰が、何を、いつ行ったか、影響を受けるファイル・フォルダ・ユーザーを確認し、メンバーへの連絡、一時停止、ステータス変更などの対応を取れます。SCS 対応では、アラートを「出す」だけでなく、確認・判断・対応・完了の記録を残す必要があります。

アラート種別	想定される SCS リスク	初動対応	証跡
ランサムウェア検知	データ暗号化、業務停止、機密情報毀損	対象範囲確認、端末隔離、復旧ポイント選定	アラート履歴、復旧記録
大量削除・移動	誤操作、不正削除、持ち出し準備	ユーザー確認、操作停止、復旧要否判断	アクティビティログ、対応記録
機密情報の外部共有	情報漏えい、契約違反	共有停止、共有先確認、上長/法務報告	外部共有レポート、是正記録
マルウェアの共有	感染拡大、取引先被害	共有停止、対象ユーザー確認、通知	アラート、調査記録
高リスクのログイン	アカウント侵害、不正アクセス	パスワードリセット、メンバー停止、ログ確認	ログイン履歴、停止記録

7-11 復旧・侵害からの復旧: 巻戻し、削除ファイル復元、バージョン履歴、証跡保全

図 13 侵害からの復旧までの流れ

Dropbox Rewind は多数の変更を一度に取り消すための機能であり、ウイルス感染など重大なデータ損失が発生した場合に特に有用です。Rewind は、ファイル編集、名称変更、追加、削除、共有フォルダ内の操作、編集権限を持つチームフォルダ内の操作などを取り消すことができます。一方で、アカウントのバージョン履歴より前の変更、完全削除されたファイル、他チーム所有のファイルやフォルダ、メンバーシップ変更などは取り消せない点に注意が必要です。[DBX-REWIND]

SCS 評価制度の侵害からの復旧においてこれらは「大量変更を安全な時点へ戻す」ための手段です。ただし、復旧の前に、侵害アカウントの停止、外部共有リンクの停止、対象範囲のログ抽出、証跡保全を実施し、復旧後に業務影響と共有状態を確認する手順を定めておく必要があります。Dropbox では削除されたファイルやフォルダを復元できること、Dropbox は削除ファイルを 30 日またはチームプランではより長い期間保存すること可能です。旧バージョンに戻す場合は、バージョン履歴を利用します。[DBX-RECOVER]

バージョン履歴では、ファイルの変更、コメント、編集、名前変更、新規アップロード、削除・移動などの履歴を確認でき、プランに応じて履歴期間が異なります。Dropbox では Advanced、Enterprise では 365 日、Standard 等では 180 日などの履歴期間が示されています。[DBX-VERSION]

侵害からの復旧では、単にファイルを戻すだけでなく、侵害されたアカウントや共有経路を封じ込め、影響範囲を調査し、改ざん・削除されたファイルを安全な時点へ戻し、再発防止策を記録する必要があります。Dropbox では、巻戻し、削除ファイル復元、バージョン履歴、セキュリティアラート、メンバー停止、リモートワイプ、外部共有の停止、データガバナンスによる保持・リーガルホールドを組み合わせることで、復旧と証跡保全を同時に進められます。

復旧・保全手段	使う場面	証跡化する内容	注意点
削除ファイル復元	誤削除、退職者操作、フォルダ削除	復元対象、復元日時、確認者	保存期間はプランに依存。
バージョン履歴	上書き、改ざん、誤編集	戻した版、理由、承認者	履歴期間はプランに依存し、延長は遡及しない。
共有停止・権限削除	外部漏えい、アカウント侵害、誤共有	停止対象、実行者、実行日時、是正後状態	復旧と同時に漏えい経路を封じ込める。
リーガルホールド	内部不正、紛争、監査、事故調査	対象メンバー、対象期間、エクスポート CSV	復旧前に証跡保全が必要な場合がある。
復旧テスト	年次/半期の確認	テストシナリオ、所要時間、結果	評価用に 1 件以上サンプルを用意する。

7-12 データガバナンス: 保持、処理、リーガルホールド

図 14 データガバナンスによる削除防止・長期保管・法的リスク低減

Dropbox のデータガバナンス アドオンでは、管理者がコンプライアンスや規制要件のためにデータ保持ポリシーまたは処理ポリシーを作成できます。保持ポリシーでは、チームメンバーがコンテンツを削除または完全削除しても、ポリシー終了までコンテンツが保持されます。処理ポリシーでは、ポリシー終了時にコンテンツが自動削除され、削除から 31 日後に完全削除されます。アクティブなポリシーは最大 100 件まで設定できます。[DBX-RETENTION]

リーガルホールドでは、管理者がホールド対象メンバーの作成または変更したコンテンツを表示・エクスポートできます。対象メンバーには通知されず、通常の権限で引き続き利用します。エクスポート時にはファイルと CSV サマリーを出力できます。[DBX-LEGAL]

機能	SCS での活用	対象データ例	証跡
保持ポリシー	重要データの意図的/偶発的削除からの保護。	契約書、議事録、監査資料、研究データ	保持ポリシー、対象フォルダ、設定履歴
処理ポリシー	保存期間満了後の自動削除と過剰保管リスク低減。	一時プロジェクト資料、期限付き共有データ	処理ポリシー、削除予定、完了記録
リーガルホールド	紛争・調査・監査時の証拠保全。	訴訟関連資料、不正調査対象者の資料	ホールド一覧、エクスポート CSV、承認記録
長期バージョン履歴	法的・監査対応のための履歴保全。	契約・決裁・重要成果物	履歴設定、復元テスト記録

7-13 Dropbox セキュリティ基盤と説明時の注意点

Dropbox では、保存時のファイルが AES-256 で暗号化され、Dropbox アプリとサーバ間の通信は SSL/TLS で保護され、アプリケーションとインフラが脆弱性テストを受けるなど多層的な保護を実現しています。[DBX-SECURITY] また、第三者監査人による広く認められたセキュリティ標準・規制に対するテストやトラストセンターでの認証・コンプライアンス情報の確認も案内されています。[DBX-COMPLIANCE]

ただし、SCS 評価で求められるのは、Dropbox のサービスとしてのセキュリティだけではありません。利用企業側の責任として、適用範囲定義、権限設計、共有設定、アカウント管理、ログ確認、復旧訓練、取引先管理を実施する必要があります。クラウドサービス利用では責任共有モデルの観点で、サービス提供者の対策状況と利用者側設定の両方を説明します。

説明できること	Dropbox 側の情報	利用企業側で必要な証跡
基盤の暗号化・通信保護	AES-256、SSL/TLS の規格/トラストセンターの情報	機密情報の保存場所、アクセス権、共有制御
第三者認証・監査	コンプライアンスページ、トラストセンター、ISMAP 等の公開情報	自社のクラウド利用評価、契約・利用範囲
アクセス制御	SSO、2FA、パスワード制御等の機能	自社の設定画面、対象者、例外管理
ログ・証跡	アクション履歴、外部共有レポート、保護とコントロール（Dropbox Protect）、ファイルアクティビティ	ログレビュー記録、調査記録、是正記録
復旧・保持	巻戻し、削除ファイル復元、バージョン履歴、保持、リーガルホールド	復旧手順、復旧テスト、保持ポリシー

7-14 なぜ Dropbox が SCS 評価制度に有効か: 代表的な他社製品との違い

SCS観点でのDropboxと代表的な他社製品の違い

SCS観点	Dropboxで説明しやすい点	代表的な他社製品で起こりやすい課題
アクセス権	ファイルサーバー/NASに近いグループ・フォルダ設計	上位権限の継承が強く、現場運用と乖離しやすい
操作性	日常業務に近い操作感で全社利用を定着させやすい	ブラウザ中心や同期制約により利用が分散しやすい
外部共有	パスワード、有効期限、DL制限、承認済みドメイン	例外運用や無期限リンクが残りやすい
証跡	監査ログ、外部共有レポート、Dropbox Protect (保護とコントロール)のCSV、アクション履歴	ログ種類・保存期間・横断可視化に制約が出やすい
復旧	巻戻し、削除ファイル復元、バージョン履歴、保持	復旧粒度や証跡化が運用依存になりやすい

図 15 SCS 観点での Dropbox と代表的な他社製品の違い

SCS 評価制度の対象は、メール、クラウドストレージ、ファイル共有、認証、アクセス管理、ログ管理といった企業の IT 基盤です。Dropbox はこの領域を間接的ないし直接的にサポートしており、★3 で求められる可視化・管理と★4 で求められる証跡・説明責任の双方を、日常業務の中で同時に整えやすい点が特徴です。以下は Dropbox と代表的なクラウドストレージ製品の比較観点を、SCS 評価制度の文脈に読み替えたものです。[SCS-DBX]

本節の読み方 ここでいう「代表的な他社製品」は、添付資料中のクラウドストレージ比較を一般化した表現です。実際の機能差は契約プラン、オプション、管理者設定、利用地域、製品アップデートにより変わるため、利用検討時には最新仕様で確認してください。

SCS 観点	Dropbox で説明しやすいポイント	代表的な他社製品で起こりやすい課題	SCS 実務への意味
アクセス権設計	ファイルサーバー/NAS に近い感覚で、チームフォルダ、グループ、サブフォルダ単位の権限設計を組み合わせやすい。現場の部門・案件・取引先単位の共有構造を制度対応に落とし込みやすい。	上位階層の権限が下位へ強く継承されるウォーターフォール型の設計では、現場の「このフォルダだけ見せない/見せる」という運用と乖離しやすい。	★3 の「誰が何にアクセスできるか」の説明がしやすく、★4 の権限棚卸し・証跡確認にもつなげやすい。
操作性・定着	エクスプローラー/Finder に近い操作感で、IT リテラシーに依存せず全社利用を進めやすい。同期・オフライン利用を含め、日常業務の中に統制を埋め込みやすい。	ブラウザ前提の運用や同期・アップロード制約が利用定着の妨げになると、ファイルがローカル、メール添付、個人クラウドに分散しやすい。	統制基盤にデータが集まらないと、情報資産台帳、外部共有棚卸し、ログ証跡が成立しにくい。
外部共有制御	共有リンクのパスワード、有効期限、ダウンロード制限、承認済みドメインなどを組み合わせて、社外共有ルールを実装しやすい。	同様のリンク機能があっても、権限設計や現場定着が弱いと、例外運用、無期限リンク、個人メール共有が残りやすい。	★3 では最低限の共有制御、★4 では共有状態の棚卸しと是正記録が重要になる。
監査ログ・証跡	添付資料では、Dropbox の監査ログは多種類のイベントを扱い、契約期間中保存されると整理されている。外部共有レポート、アクティビティ、保護とコントロール（Dropbox Protect）CSV と組み合わせて説明資料を作りやすい。[SCS-DBX]	ログの種類や保存期間が限定的な場合、過去の操作追跡、評価機関への説明、取引先への報告に必要な粒度が不足することがある。	★4 の「証跡・説明責任」では、ログの有無だけでなく、検索・出力・保管・是正との紐づけが評価上の差になる。
履歴・復元	標準のバージョン履歴、削除ファイル復元、データガバナンスによる長期保管を組み合わせ、誤削除・改ざん・事故調査に備えられる。	世代数や保存期間が短い場合、改ざん・削除に気づくまでの時間が長いケースで復旧や説明が難しくなる。	インシデントレスポンスでは、復旧可能性に加え、いつの版に戻したか、誰が確認したかの証跡が重要になる。
ランサムウェア・不審な操作	セキュリティアラートにより、ランサムウェア、大量削除、大量移動、マルウェア共有、リスクの高いログイン等の検知・対応記録を残しやすい。[DBX-ALERT]	検知や復元が追加オプションの場合、対応品質にばらつきが出る。	★4 では検知後の確認、封じ込め、復旧、再発防止の一連の記録が重要になる。

7-15 Dropbox Protect（保護とコントロール）がオーバーシェアリング対策で有効な理由

SCS 対応で最大の実務リスクの一つが、オーバーシェアリング、すなわち本来の意図を超えた範囲への共有です。Dropbox Protect（保護とコントロール）は、Dropbox 内のコンテンツだけでなく、接続済みの Microsoft 365（OneDrive/SharePoint）や Google ドライブを横断して、所有者、共有先、リンク種別、権限、更新日、個人メール共有、外部ドメイン共有などを確認できます。[DBX-PAC-ADMIN][DBX-PAC-ITEM]

代表的な他社製品の管理機能が自製品内の共有・権限管理に閉じがちな場合、実際の業務で複数クラウドを併用している企業では、「Dropbox は管理されているが、他のクラウドに残る公開リンクや個人メール共有が見えない」という空白が生じます。Dropbox Protect（保護とコントロール）は、この空白を横断的に可視化し、不要なリンク削除、共同編集者削除、共有停止、ポリシーによる自動是正、アクション履歴による是正記録までつなげられる点が、SCS の★4 で求められる説明責任に直結します。[DBX-PAC-RISK][DBX-PAC-LINKS][DBX-PAC-POLICY]

保護とコントロール（Dropbox Protect）の機能	具体的にできること	SCS 上の価値
横断可視化	Dropbox、Microsoft 365、Google ドライブの接続済みアプリを横断して、ファイル、所有者、共有先、リンク、権限を確認する。	自社 IT 基盤の実態把握、外部共有棚卸し、取引先説明に使える。
リスク抽出	公開リンク、社内リンク、外部共有、個人アカウント、古いアクセスなどをレポートやフィルタで抽出する。	過剰共有、個人メール共有、長期放置共有のリスクを可視化する。
是正	リンク削除、共有停止、共同編集者削除、リンク種別変更などを個別または一括で実施する。	インシデント初動と定期棚卸しの是正を証跡化できる。
CSV 出力	フィルタ済み結果を CSV として出力し、監査、分析、報告、共有に使える。	評価機関、取引先、経営層への説明資料として活用できる。
アクション履歴	誰が、いつ、どの是正を行い、成功・失敗したかを記録する。	★4 で重要な「是正した事実」の証明につながる。
ポリシー	公開リンクや外部共有などを検知し、アラートや自動修復に展開する。	継続的改善と運用定着を示せる。

7-16 Dropbox 導入だけでは埋まらない領域

領域	Dropbox で支援できる部分	別途必要な実務
経営ガバナンス	必要に応じてログやレポートを報告資料に使える。	責任者任命、経営会議、リスク受容、投資判断。
取引先管理	共有先・外部ユーザー・共有ファイルを把握できる。	重要取引先判定、契約条項、セキュリティ確認票。
端末管理	リモートワイプを一部支援する	MDM/EDR、OS 更新、端末暗号化、持ち出し管理。
ネットワーク境界	Dropbox 単体では FW/VPN/ルータ管理は対象外。	外部公開機器、VPN、脆弱性診断、技術検証。
教育・訓練	共有ルールやアラートを教材にできる。	セキュリティ教育、標的型訓練、インシデント訓練。

第 8 章 制度対応でよくある課題

8-1 何をすればよいかわからない

最初から全要求事項を完璧に満たそうとすると進みません。まず、情報資産、アクセス権、外部共有、ログ、復旧の 5 項目を棚卸しします。これらは★3・★4 のいずれでも土台になります。

8-2 証跡が残っていない

「実施している」が「証明できない」状態です。評価対応では、操作ログ、棚卸し記録、設定画面、承認記録、是正記録を紐づけます。証跡は評価直前に作るのではなく、日常運用で自動的に残るように設計します。

8-3 アクセス権が個人単位で複雑化している

個別権限が増えると、誰が何にアクセスできるか説明できなくなります。Dropbox ではグループ単位のチームフォルダ設計を基本にし、例外権限は期限・理由・承認者を記録します。

8-4 外部共有が野放しになっている

共有リンクが無期限、パスワードなし、個人メール宛、ダウンロード可能な状態で放置されるケースです。外部共有レポートを定期出力し、未承認ドメイン、期限なしリンク、過剰権限を是正します。

8-5 ログはあるが説明できない

ログを出せる人が一部担当者に限られると、評価・監査・インシデント対応が属人化します。ログ検索手順、出力条件、保存先、確認頻度を文書化し、定例レビューを行います。

8-6 復旧できるはずだが試したことがない

復旧機能が存在しても、実際に戻せるか、どのくらい時間がかかるか、誰が操作するかが不明では説明できません。削除ファイル復元、バージョン履歴による復元テストを実施し、記録を残します。

8-7 課題別の即効アクション

課題	今週やること	30 日以内にやること	90 日以内にやること
データの散在	主要保存場所を列挙する。	重要情報を Dropbox 等の管理基盤へ集約する方針を決める。	部門別移行と保存ルールを完了する。
権限が不明	管理者が権限一覧を出す。	不要ユーザー・退職者・外部ユーザーを削除する。	グループ単位の権限設計へ移行する。
外部共有が不明	外部共有レポートを出す。	未承認共有、期限なしリンクを是正する。	外部共有の定例棚卸しを運用化する。
ログが未活用	取得可能なログを確認する。	月次ログレビュー手順を作る。	異常検知・アラート対応を記録化する。
復旧未確認	復旧機能の対象範囲を確認する。	削除ファイル復元・Rewind の対象範囲を確認する。	Rewind・削除ファイル復元・バージョン履歴を含む復旧訓練を実施する。

第 9 章 実践ロードマップ

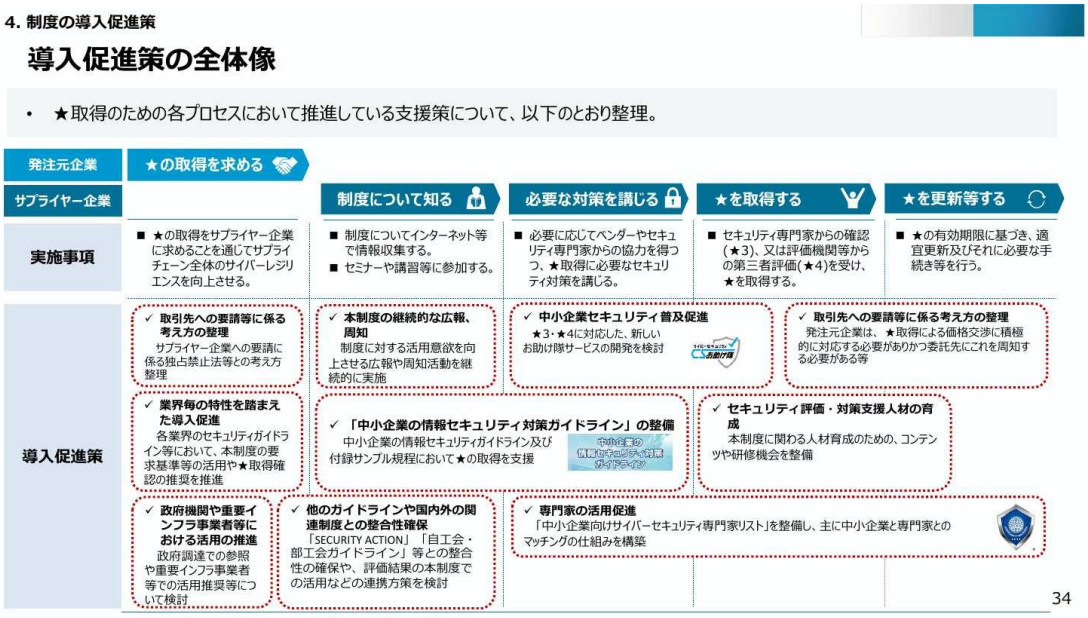


図 17 制度導入促進策の全体像 – 経済産業省のガイダンスより抜粋

SCS 対応は、制度開始を待ってから一括で行うより、現状把握、基盤整備、証跡運用、評価準備に分けて段階的に進める方が現実的です。以下は、Dropbox を業務ファイル基盤として活用する場合の 180 日のロードマップ例です。

期間	フェーズ	実施内容	成果物
0–30 日	現状把握	IT 基盤、ファイル保存場所、アクセス権、外部共有、ログ、復旧手段を棚卸し。	現状診断シート、リスク一覧
31–60 日	基盤設計	Dropbox のフォルダ構成、グループ、共有ルール、SSO/MFA、ログ取得方針を設計。	設計書、運用ルール案
61–90 日	設定・移行	チームフォルダ、グループ、外部共有設定、共有リンク既定値、アラート、レポート出力を設定。	設定証跡、移行計画
91–120 日	証跡運用	権限棚卸し、外部共有棚卸し、ログレビュー、復旧テストを実施。	棚卸し記録、ログレビュー記録、復旧テスト記録
121–150 日	自己評価	★3/★4 要求事項に対して自己評価し、不足項目を是正。	自己評価表、ギャップ一覧、是正計画
151–180 日	評価準備	専門家確認または評価機関相談に向け、証跡フォルダと説明資料を整備。	証跡パッケージ、説明資料、申請準備

9–1 役割分担モデル

役割	責任	主なタスク
経営層	リスク受容、投資判断、方針承認	方針承認、報告受領、是正優先度判断
SCS 対応責任者	全体進行、評価対応、証跡統括	ロードマップ管理、自己評価、専門家/評価機関連携
情報システム	技術設定、ログ、アカウント、復旧	SSO/MFA、権限設計、ログ出力、復旧テスト
セキュリティ担当	要求事項解釈、リスク評価、点検	ギャップ分析、インシデント手順、教育
法務・総務	規程、契約、取引先管理	外部共有規程、契約条項、取引先確認票
各部門	実運用、情報資産管理	情報資産棚卸し、外部共有申請、権限確認

第 10 章 よくある質問

Q1. SCS 評価制度は義務ですか。

制度としては任意制度です。ただし、2 社間の取引契約で発注元が委託先へ特定の★段階や要求事項への対応を求めることは想定されます。[SCS-FAQ]

Q2. ★を取得しないと取引停止になりますか。

制度が直ちに取引停止を求めるものではありません。契約上の扱いは当事者間で合意すべきものです。ただし、取引先説明のための共通基準として使われる可能性があります。[SCS-FAQ]

Q3. 中小企業だけが対象ですか。

中小企業だけでなく、業種・規模を問わずサプライチェーンを構成する幅広い事業者が対象になり得ます。[SCS-FAQ]

Q4. ISMS を取得していれば SCS 対応は不要ですか。

不要とは限りません。ISMS はマネジメントシステムの構築・運用を評価する制度であり、SCS の★3・★4 は代表的な脅威を前提に具体的対策をベースライン化する制度です。相互補完的に位置づけられます。[SCS-1]

Q5. 特定のセキュリティ製品が必要ですか。

特定製品の導入が制度上求められているわけではありません。評価基準を満たす実装方法は、組織規模や構成に応じて異なります。[SCS-FAQ]

Q6. Dropbox を入れれば★3/★4 を取得できますか。

Dropbox は情報資産管理、アクセス管理、外部共有統制、ログ、復旧、データ保全を支援できますが、組織体制、規程、取引先管理、教育、経営報告、ネットワーク/端末対策などは別途必要です。

Q7. どのログを残せばよいですか。

最低限、ログイン、ファイル操作、外部共有、リンク作成、管理者操作、アラート、復旧操作を確認できるようにします。評価では、ログ取得だけでなく、検索・出力・確認・是正の記録が重要です。

Q8. 外部共有は全面禁止すべきですか。

全面禁止は現実的ではありません。重要なのは、共有可能な情報、承認、共有先、期限、パスワード、ダウンロード可否、棚卸しのルールを明確にすることです。

Q9. ★3 の専門家確認は社内情シスだけでよいですか。

単に社内情報システム担当者であればよいわけではありません。FAQ では、所定の資格や研修要件を満たすセキュリティ専門家が想定されています。本文章は Dropbox 社内の資格所有者が執筆したものです。[SCS-FAQ]

Q10. いつから申請できますか。

FAQ では、申請受付開始時期は令和 8 年度末頃、1 月から 3 月頃が予定されています。詳細は IPA から公表される予定です。[SCS-FAQ]

10-2 お客様向け FAQ（制度理解と Dropbox 活用）

以下は、添付の「SCS 評価制度 × Dropbox 質問・回答集」のうち、お客様向けに利用できる制度理解、Dropbox 活用、監査、外部共有、復旧、導入運用の論点を再整理したものです。利用企業が自社対応を検討する際の実務 FAQ として記載します。[SCS-DBX-FAQ]

制度理解に関する FAQ

質問	回答の要旨	示唆
SCS 評価制度とは何ですか。	サプライチェーン全体のセキュリティ対策状況を共通基準で見える化し、★3・★4・★5 などの段階で説明しやすくする制度です。	単なるチェックリストではなく、取引先へ自社の対策水準を説明するための共通言語として捉えます。
罰則制度ですか。	未取得だから直ちに罰金や行政処分を受ける制度ではなく、企業の優劣をランキングする制度でもありません。	任意制度であっても、取引先確認の材料になるため、証跡を準備しておくことが重要です。
なぜ今対応が必要ですか。	攻撃対象が大企業本体から取引先・委託先・協力会社へ広がっているためです。	セキュリティは IT 部門だけでなく、取引条件や企業信頼性に関わる経営課題になります。
対象は中小企業だけですか。	中小企業だけではなく、発注元から評価を求められる企業、取引先を管理する企業、外部委託先を多く抱える企業が対象になり得ます。	自社が受注者として評価される立場か、発注者として確認する立場かを整理します。
対象範囲はどこですか。	中心はメール、クラウドストレージ、ファイル共有、認証、アクセス管理、ログ管理、外部共有管理などの IT 基盤です。	OT システムや提供製品そのものとは切り分け、IT 基盤の適用範囲を先に定義します。

★3・★4 に関する FAQ

質問	回答の要旨	Dropbox で支援できる例
★3 では何が求められますか。	最低限の可視化・管理です。誰がどの情報にアクセスできるか、重要ファイルがどこにあるか、外部共有が管理されているかを説明できる状態が必要です。	ファイル一元管理、チームフォルダ、権限設定、MFA/SSO、共有リンク制御、退職者対応。
★4 では何が求められますか。	対策しているだけでなく、証跡をもとに説明できる状態です。誰が、いつ、何にアクセスし、何を共有したかをログとして確認できることが重要です。	アクティビティログ、管理コンソール、レポート出力、外部共有レポート、セキュリティアラート、データ保護。
Dropbox だけで★3・★4 を取得できますか。	Dropbox は技術的な土台を支援しますが、社内ルール、管理体制、教育、インシデント対応手順などの組織的取り組みも必要です。	Dropbox は IT 基盤・証跡管理・外部共有統制の土台として位置づけます。
まず★3 か★4 か。	多くの企業では、まず★3 相当の可視化・管理を整え、その後★4 相当の証跡・説明責任へ進むのが現実的です。	ファイル・ユーザー・権限の棚卸しから始め、ログ取得・外部共有ルール、監査証跡へ進みます。

Dropbox 機能に関する FAQ

質問	回答の要旨	SCS 上の価値
Dropbox は何に役立ちますか。	可視化、運用管理、証跡、外部共有統制、復旧・保全の 5 つを支援します。	日常業務のファイル共有を、評価に耐える管理基盤へ近づけます。
「誰が、いつ、何をしたか」を確認できますか。	アクティビティログや管理コンソールで、閲覧、編集、共有、削除、移動などの操作履歴を確認できます。	★4 で重要な証跡をもとにした説明に直結します。
外部共有の管理はできますか。	共有リンクのパスワード、有効期限、ダウンロード制限、共有状況の確認が可能です。	部門ごとにばらつきやすい外部共有ルールを標準化できます。
認証強化に対応していますか。	MFA、SSO 連携、パスワードポリシー等に対応します。	不正アクセスリスクを低減し、ユーザー認証を組織全体で統制できます。
退職者や異動者のアクセス停止に対応できますか。	管理コンソールでユーザー停止、権限変更、必要に応じたリモートワイプ等を実施できます。	退職者アカウントの残存や旧部署データへのアクセス継続を防ぎます。

証跡・監査対応に関する FAQ

質問	回答の要旨	運用ポイント
証跡とは何ですか。	セキュリティ対策が実際に運用されていることを客観的に示す記録です。アクセスログ、操作ログ、共有履歴、権限変更履歴、認証ログなどが該当します。	「対策しています」ではなく、ログや記録で説明できる状態を作ります。
Dropbox のログは監査や取引先説明に使えますか。	アクティビティログや管理コンソールから操作履歴を確認・検索・出力できます。	監査時や取引先確認時に、証跡として提示しやすくなります。
ログがあれば★4 対応は十分ですか。	ログ取得だけでは不十分です。定期確認し、不審な共有やアクセスがあれば是正する運用が必要です。	取得、確認、是正の 3 点をセットで運用します。
監査準備で最初にすべきことは何ですか。	重要ファイルがどこにあるか、誰がアクセスできるか、どのように外部共有されているかを整理します。	データ集約、権限設計、共有ルール、ログ取得、レポート出力を順に整備します。

外部共有・オーバーシェアリングに関する FAQ

質問	回答の要旨	SCS 上の価値
オーバーシェアリングとは何ですか。	本来共有すべき範囲を超えてファイルやフォルダが広く共有されてしまう状態です。無期限リンク、全社共有、個人メール共有、退職者アクセス残存などが例です。	情報漏えい、コンプライアンス違反、説明不能リスクにつながります。
なぜ重要ですか。	SCS 評価制度では、外部共有やアクセス権限が適切に管理されているかが重要です。放置すると「誰がどの情報にアクセスできるか」を説明できません。	★3 の可視化・管理、★4 の証跡・説明責任の両方に関係します。
Dropbox で防げますか。	共有リンク制御、パスワード、有効期限、ダウンロード制限、共有状況の確認に加え、保護とコントロール（Dropbox Protect）で不要な共有の是正を支援できます。	外部共有棚卸しと是正記録を作りやすくなります。
他クラウドの共有も確認できますか。	Dropbox Protect（保護とコントロール）は、接続済みの Dropbox、Microsoft 365（OneDrive/SharePoint）、Google ドライブを横断して共有状態を可視化・統制できます。	複数クラウド併用時の見えない共有を減らし、★4 の説明責任を補強します。

データガバナンス・侵害からの復旧に関する FAQ

質問	回答の要旨	SCS 上の価値
データガバナンスは何に役立ちますか。	重要データの長期保管、削除防止、バージョン履歴、リーガルホールドに役立ちます。	重要データを「残す・戻す・示す」状態に整えるデータ保護基盤として活用できます。
ランサムウェア対策に役立ちますか。	ランサムウェア検知や復元関連機能、バージョン履歴、巻戻しにより、被害発生前の状態へ戻す対応を支援します。	侵入を防ぐだけでなく、被害後に復旧できる体制の説明に使えます。

質問	回答の要旨	SCS 上の価値
バージョン履歴や巻戻しはなぜ重要ですか。	誤削除、上書き、ランサムウェアによる暗号化などの際、過去の状態へ戻せるためです。	業務停止リスクの低減と、侵害からの復旧体制の強化につながります。
どの部門に向いていますか。	人事、総務、法務、経理、研究開発など、長期保管や改ざん防止が必要な文書を扱う部門です。	誓約書、議事録、契約書、監査資料、研究データなどに有効です。

導入・運用に関する FAQ

質問	回答の要旨	進め方
最初に何をすべきですか。	現状把握から始めます。重要データの所在、アクセス権限、外部共有、認証、ログ、証跡の有無を確認します。	棚卸し結果をもとに、Dropbox で一元管理できる対象と優先順位を決めます。
導入後に必要な運用は何ですか。	権限見直し、外部共有確認、ログ確認、共有ルール更新、証跡管理を定期的に行います。	一度設定して終わりではなく、継続的に回せる仕組みを作ります。
ファイルサーバーや NAS から移行するメリットは何ですか。	データ、権限、共有、ログを一元管理しやすくなります。	どこに何があり、誰がアクセスでき、どう共有され、どのログが残るかを説明しやすくなります。
OneDrive や SharePoint を使っている場合でも活用できますか。	用途に応じた使い分けが可能です。Dropbox は大容量ファイル共有、外部共有、ファイルサーバー代替、証跡管理の基盤として活用しやすい領域があります。	既存環境を置き換えるだけでなく、SCS 上の不足領域を補完する観点で検討します。
運用負荷は増えませんか。	日常業務の中でファイルを保存・共有・編集するだけで、アクセスログや操作履歴を蓄積しやすい点が特徴です。	新しい記録作業を増やすのではなく、普段の業務を評価に耐える形へ整えます。

10-3 お客様向けまとめ

上記 FAQ を踏まえると、Dropbox の活用価値は、SCS 評価制度の取得を保証することではなく、日常業務で使うファイル共有・アクセス管理・外部共有・ログ・復旧・保全の仕組みを、取引先や評価機関へ説明できる形に整える点にあります。評価対応を特別な作業として追加するのではなく、普段の業務を評価に耐える形へ変えることが重要です。

付録 A Dropbox 設定・証跡チェックリスト

領域	設定・確認項目	証跡	頻度
チームフォルダ	部門/プロジェクト別フォルダとグループ権限が定義されている。	フォルダ構成、グループ一覧	半期
SSO	SSO が必要に応じて必須／オプションで設定されている。	SSO 設定画面、IdP 設定	年次/変更時
多要素認証	全員または対象者に多要素認証が要求されている。	多要素認証の設定、例外一覧	四半期
パスワード	Dropbox または IdP で強力なパスワードが要求されている。	ポリシー設定	年次
Web セッション	dropbox.com のセッション期限が設定されている。	セッション設定	年次
メンバー停止	退職者・契約終了者が停止されている。	停止ログ、退職者リスト	都度/月次
リモートワイプ	紛失・退職時のワイプ手順がある。	ワイプステータス、手順書	都度
外部共有設定	社外共有可否、承認済みリスト、リンク既定値が設定されている。	共有設定画面	四半期
共有リンク	パスワード、有効期限、DL 制限のルールが適用されている。	リンク設定、共有レポート	月次
外部共有レポート	CSV を出力し、未承認共有を是正している。	CSV、是正記録	月次/四半期
アクティビティログ	ファイル操作や共有操作を調査できる。	ログ抽出、確認記録	月次/都度
セキュリティアラート	ランサムウェア、大量削除、マルウェア共有等のアラートを確認している。	アラート履歴、対応記録	都度/月次
削除ファイル復元	削除時の復元手順がある。	復元テスト記録	半期
バージョン履歴	履歴期間と復元手順を把握している。	履歴設定、復元記録	半期
巻戻し	大量変更・ランサムウェア時の一括復旧手順を把握している。	巻戻し手順、復旧時点選定記録、復旧後の確認履歴	半期/年次
復旧テスト	削除・改ざん時の復旧手順を確認している。	削除ファイル復元手順、バージョン履歴、テスト記録	年次
データ保持	重要データに保持ポリシーを適用している。	ポリシー設定、対象フォルダ	年次
リーガルホールド	調査・紛争時のホールド手順がある。	ホールド記録、CSV エクスポート	都度

付録 B 規程テンプレート骨子

B-1 外部共有管理規程

	方針	規程（リンク）、証跡
目的・適用範囲		
共有可能な情報区分		
共有承認者		
共有リンク設定要件		
パスワード・有効期限・ID 制限		
外部共有棚卸し頻度		
違反時の対応		

B-2 アクセス管理規程

	方針	規程（リンク）、証跡
アカウント発行		
権限付与の原則		
グループ管理		
異動・退職時の変更		
管理者権限		
権限棚卸し		
例外管理		

B-3 ログ管理規程

	方針	規程（リンク）、証跡
取得対象ログ		
保存期間		
確認頻度		
確認者		
アラート対応		
ログ出力手順		
インシデント時の保全		

B-4 復旧手順書

	方針	規程（リンク）、証跡
対象データ		
復旧手段		

削除ファイル復元		
バージョン履歴		
復旧テスト		
復旧後の確認		
証跡保全		

B-5 取引先管理規程

	方針	規程(リンク)、証跡
重要取引先の定義		
情報共有範囲		
委託/再委託管理		
セキュリティ覚書		
契約条項		
是正依頼		
年次見直し		

.参考資料

ID	資料名・URL
SCS-1	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(令和 8 年 3 月、添付資料)
SCS-FAQ	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)に関するよくあるお問い合わせ(FAQ)(最終更新日: 令和 8 年 3 月 27 日、添付資料)
SCS-DBX	SCS 評価制度を回すための実務 – 証跡・アクセス管理・共有ルールを整える(添付資料)
DBX-TEAM	Dropbox Help: Team folders: an overview – https://help.dropbox.com/organize/team-folders
DBX-SSO	Dropbox Help: How to enable single sign-on for your team – https://help.dropbox.com/security/sso-admin
DBX-2FA	Dropbox Help: How to require two-factor authentication for Dropbox teams – https://help.dropbox.com/security/2-factor-authentication
DBX-PWD	Dropbox Help: Password control for Dropbox teams – https://help.dropbox.com/security/password-control
DBX-SESSION	Dropbox Help: Web session control – https://help.dropbox.com/security/web-session-control
DBX-SUSPEND	Dropbox Help: Suspend or unsuspend a team member – https://help.dropbox.com/security/suspend-member
DBX-WIPE	Dropbox Help: Remote wipe Dropbox files from a computer – https://help.dropbox.com/delete-restore/remote-wipe
DBX-EXT	Dropbox Help: Manage external sharing in your team – https://help.dropbox.com/share/manage-team-sharing
DBX-LINK	Dropbox Help: How to set or change shared link permissions – https://help.dropbox.com/share/set-link-permissions
DBX-MONITOR	Dropbox Help: How to monitor Dropbox team sharing activity – https://help.dropbox.com/share/monitor-sharing-activity
DBX-ACTIVITY	Dropbox Help: File activity – https://help.dropbox.com/organize/file-activity
DBX-ALERT	Dropbox Help: Security alerts – https://help.dropbox.com/security/security-alerts
DBX-REWIND	Dropbox Help: How to use Dropbox Rewind – https://help.dropbox.com/delete-restore/rewind
DBX-RECOVER	Dropbox Help: Recover deleted files and folders – https://help.dropbox.com/delete-restore/recover-deleted-files-folders
DBX-VERSION	Dropbox Help: Version history overview – https://help.dropbox.com/delete-restore/version-history-overview
DBX-PAC-REPORTS	Dropbox Help: View 保護とコントロール(Dropbox Protect) reports – https://help.dropbox.com/security/view-protect-control-reports-dash
DBX-PAC-ADMIN	Dropbox Help: How to manage 保護とコントロール(Dropbox Protect) – https://help.dropbox.com/security/dash-保護とコントロール(Dropbox Protect)-admin
DBX-PAC-CSV	Dropbox Help: How to export to CSV in 保護とコントロール(Dropbox Protect) – https://help.dropbox.com/security/export-csv-protect-control
DBX-PAC-POLICY	Dropbox Help: How admins can enforce policies with 保護とコントロール(Dropbox Protect) – https://help.dropbox.com/onboarding/dropbox-dash-policy-enforcement-guide
DBX-PAC-RISK	Dropbox Help: How to fix security risks in 保護とコントロール(Dropbox Protect) – https://help.dropbox.com/security/fix-security-risks
DBX-PAC-LINKS	Dropbox Help: How to manage shared links in the 保護とコントロール(Dropbox Protect) dashboard – https://help.dropbox.com/share/managing-links-protect-control

ID	資料名・URL
DBX-PAC-ITEM	Dropbox Help: How to view and understand item details in 保護とコントロール（Dropbox Protect） dashboard – https://help.dropbox.com/security/protect-control-item-list
DBX-RETENTION	Dropbox Help: Data retention – https://help.dropbox.com/security/data-retention
DBX-LEGAL	Dropbox Help: Legal holds – https://help.dropbox.com/security/legal-hold
DBX-SECURITY	Dropbox Help: How Dropbox keeps your files secure – https://help.dropbox.com/security/how-security-works
DBX-COMPLIANCE	Dropbox Help: The standards and regulations we comply with – https://help.dropbox.com/security/standards-regulations
SCS-DBX-FAQ	SCS 評価制度×Dropbox 質問・回答集（添付資料、お客様向け FAQ として本書に反映）

メモ：本書は制度詳細公表前の実務ガイド案です。提出様式、評価ガイド、評価機関、技術検証手順、★5 の具体内容は、IPA 等の今後の公表内容に合わせて更新してください。Dropbox の各機能についても、プラン、アドオン、管理者権限、最新仕様を確認したうえで実装してください。