SCS評価制度対応支援パッケージ

「ファスト・セキュリティ・パス®」

ご紹介



2026年10月

株式会社 iSecure

SCS評価制度

近年、サプライチェーンを通じたセキュリティインシデントが頻発しています。委託先等、サプライチェーン全体のセキュリティ対策が求められる中、以下の課題が表面化しつつあります。

委託元企業：委託先におけるセキュリティ対策が可視化しづらく、要求事項（チェックリスト等）の適正性の担保も難しい
委託先企業：複雑なサプライチェーン下で様々な委託元から様々な要求事項を求められ、過度な負担につながっている

本制度に基づくマークの取得を通じて、ビジネス・ITサービスサプライチェーンにおける、委託先へのサイバー攻撃等を起因とした自社事業・サービスの提供途絶／機密情報の漏えい、改ざんや委託先等を踏み台とした不正侵入等のリスクに対する適切なセキュリティ対策の実施を促し、サプライチェーン全体でのセキュリティ対策水準の向上を図ることを目的としています。
具体的には、2社間の取引契約等において、委託元が、委託先に適切な段階（★）を提示し、示された対策を促すとともに実施状況を確認することを想定しています。

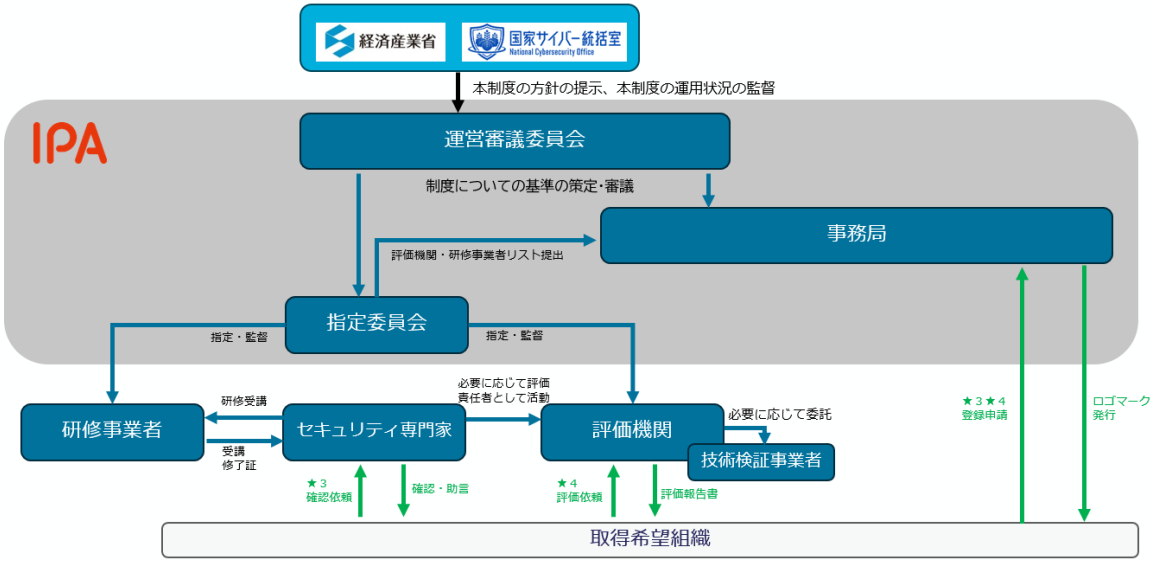
目指す効果として、サプライチェーンにおけるリスクを対象にした上で、その中での立ち位置に応じて必要な対策を提示することで、企業の対策決定を容易・適切なものにします。全てのサプライチェーン企業が対象となりますが、特にサプライチェーンを構成する中小企業は、セキュリティ対策におけるリソースが限られていること、また自社のリスクを踏まえてセキュリティ対策を行うことはハードルが高いことから、活用による効果が大きいと想定しています。

（独）情報処理推進機構（IPA） SCS評価制度紹介ページより

2026 iSecure Co., Ltd. All Rights Reserved.

SCS評価制度

経済産業省および内閣官房国家サイバー統括室の監督のもと、独立行政法人情報処理推進機構（IPA）が運営



構築する評価制度

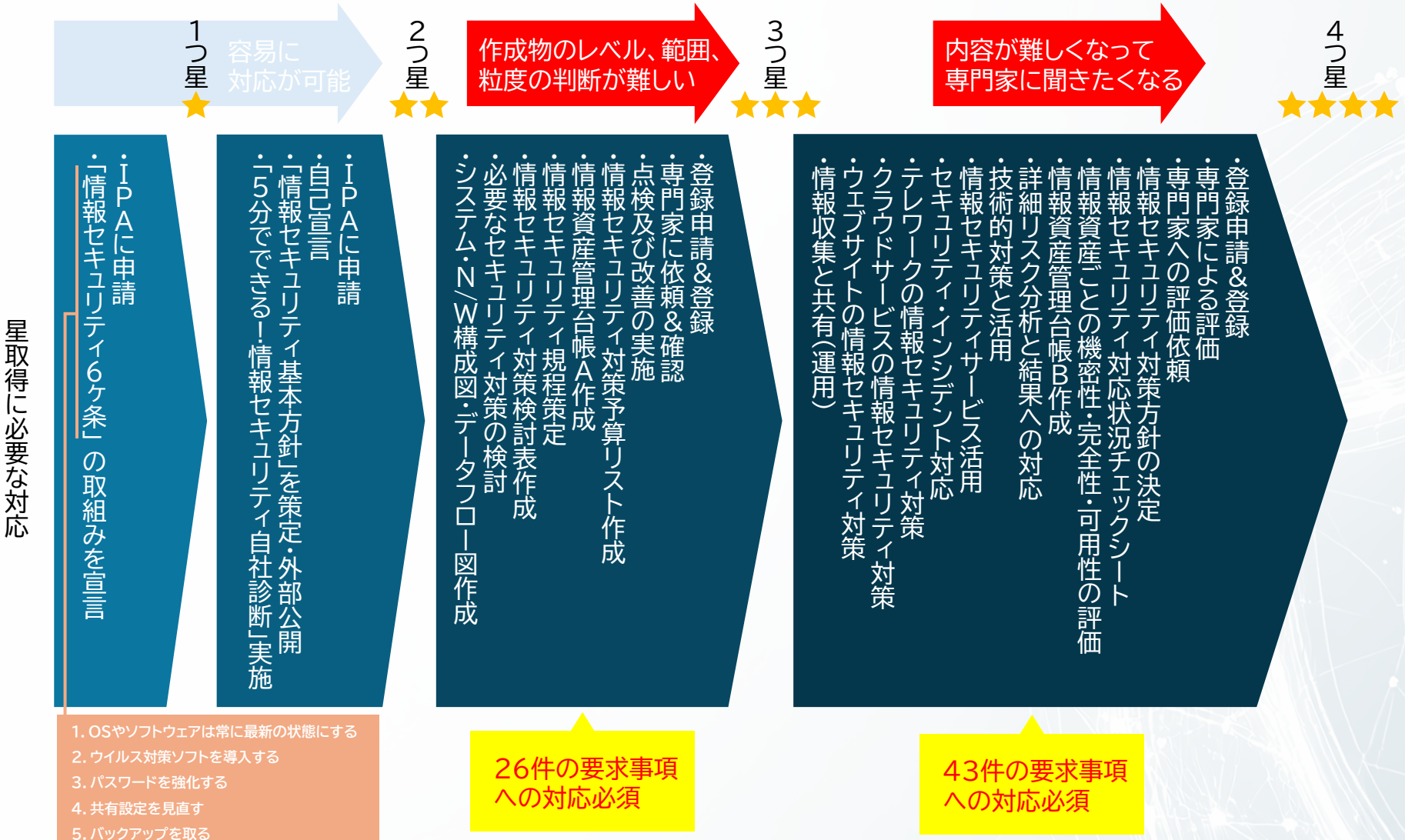
	★3		★4		★5 [検討中※5]
想定される脅威	• 広く認知された脆弱性等を悪用する一般的なサイバー攻撃		• 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃		• 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全てのサプライチェーン企業が**最低限実装すべき**セキュリティ対策： • 基礎的な組織的対策とシステム防御策を中心に実施		サプライチェーン企業等が**標準的に目指すべき**セキュリティ対策： • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施		サプライチェーン企業等がさらに目指すべき高度な対策： • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善工程を整備、システムに対しては現時点でのベストプラクティスの対策を実施
要求事項 / 有効期間	26件	1年	43件	3年（毎年自己評価を実施し結果を評価機関へ提出）	（今後検討）
評価スキーム	**専門家確認付き自己評価** ※4		**第三者評価**		第三者評価

［※4］専門家：登録セキスペ、CISSP等の資格を有し、かつ制度が定める研修を受講したセキュリティ専門家　［※5］ISMS適合性評価制度、★3・4との整合性も踏まえ、対策事項を今後検討

経済産業省およびIPAの SCS評価制度紹介ページより

2026 iSecure Co., Ltd. All Rights Reserved.

SCS評価制度対応の概要



2026 iSecure Co., Ltd. All Rights Reserved.

ファスト・セキュリティ・パス（FSP）

SCS評価制度への対応は必要だけど、**知識も時間も無いのに**、ガイドラインとサンプル的なテンプレートだけでは正直なかなか難しい・・・



ファスト・セキュリティ・パスの特徴

POINT 1

『公式の評価』をご提供
- 対応する有資格の専門家が完成物を評価し、評価報告書を作成
- あとはお客様からIPAに登録申請を行うだけで★～★★★★を取得することが可能

POINT 2

『ガイドブック』
- 「何故」「何を」「どこまで」を明確に解説
- 対応作業のスケジュールも管理

POINT 3

『作業マニュアル』
- 「作業詳細」「作業ポイント」を明確に解説
- 1つ1つの細かな作業ごとの説明で、“何をすれば良いか”で迷わなくなる

POINT 4

『完全テンプレート』
- 作成を要求されるすべての「規定」「チェックシート」「管理表」などをフルセットでご用意
- ガイドブックの指示で選択したテンプレートにマニュアルの説明通りに自社の情報を記載するだけ

POINT 5

『専門家によるサポート』
- それでも分からないときは専門家がメール回答

2026 iSecure Co., Ltd. All Rights Reserved.

FSP：星3つ「確認」及び星4つ「評価報告書」

SCS評価制度で星3つを取得するには、IPAに認定された専門家による助言に基づいて対応した内容を修正し、専門家からの確認を貰うことが必要になります。また、星4つを取得するには、IPAに認定された専門家に評価を依頼し、専門家が対応として合格していると認めた評価報告書を受領することが必要となります。

FSPでは、お客様を担当するIPA公認の専門家によって星3つの確認および星4つの評価報告書をご提供することで、お客様が対応作業の終了とともに資格を取得することをサポートします。



2026 iSecure Co., Ltd. All Rights Reserved.

FSP:ガイドブック例



2026 iSecure Co., Ltd. All Rights Reserved.

FSP:作業マニュアル例

全作業の共通作業No.
*全行程中の進捗を把握

全作業の作業フェーズ

作業フェーズのステップ
*フェーズ中の進捗を把握

個別作業のスケジュール
*予定の目安に対する遅れを把握

作業の内容
*作業を明確に指示

作業のポイントを解説
*単なる作業ではなく意義、意図、目的などを詳細に学びながら進めることができる

作業実施日管理
*対応完了日を記録

作業進捗
*個別作業の進み具合を記録

タスクNo.	フェーズ	Step	作業予定日	作業内容	作業のポイント	内容理解・実施日	進捗率
142	ブルー	4	Week 6 / Day 4	プロセス８. [テンプレート19. 情報セキュリティ規程] を策定する。	●情報セキュリティ対策について、[テンプレート19. 情報セキュリティ規程]を策定します。 ●"情報セキュリティ規定"とは、会社の情報セキュリティに関する法律のようなものであり、基本的に全ての従業員、情報システム環境はこの規定を満たしていることが求められます。		
143	ブルー	4	Week 6 / Day 4	"1.組織的対策"を作成する。	●組織的対策について[テンプレート19. 情報セキュリティ規程-1.組織的対策]を確認し、必要に応じて適切な内容に修正して規定を作成します。 ●会社の情報セキュリティ対策の一元的な主管部門として、"情報セキュリティ委員会"を設置します。		
144	ブルー	4			●情報セキュリティ委員会のメンバーは、[テンプレート1. 情報管理体制表]で定義した各メンバーをそのまま記載します。 ●[テンプレート1. 情報管理体制表]では定義していない、委員会として必要な新たな役割となる、"インシデント対応責任		
145	ブルー	4			●情報セキュリティの取組みの監査・点検/点検は年に１度実施するのが一般的です。		
146	ブルー	4	Week 6 / Day 4	"2.人的対策"を作成する。	●人的対策について[テンプレート19. 情報セキュリティ規程-2.人的対策]を確認し、必要に応じて適切な内容に修正します。		

2026 iSecure Co., Ltd. All Rights Reserved.

FSP:テンプレート例

【テンプレート 19-1】

株式会社XXXXXXX　情報セキュリティ規程 1

1　組織的対策（適用範囲：全社・全従業員）

1　情報セキュリティのための組織

・情報セキュリティ対策を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

[情報セキュリティ委員会]

① 情報セキュリティ責任者：（部署）（役職）氏名
情報セキュリティに関する責任者。情報セキュリティ対策などの決定権限を有するとともに、全責任を負う

② 情報セキュリティ部門責任者：（部署）（役職）氏名
各部門における情報セキュリティの運用管理責任者。各部門における情報セキュリティ対策の実施などの責任を負う

③ システム管理者：（部署）（役職）氏名
社内の情報システムに必要な情報セキュリティ対策の検討・導入を行う

④ 教育責任者：（部署）（役職）氏名
情報セキュリティ対策を推進するために従業員への教育を企画・実施する

⑤ インシデント対応責任者：（部署）（役職）氏名
事故の影響を判断し、対応について意思決定する

⑥　個人情報苦情相談対応：（部署）（役職）氏名
インシデント対応責任者の管理下で、個人情報の取扱いに関して本人からの苦情・相談に対応する

⑦ 個人情報保護管理者：（部署）（役職）氏名
個人情報の取扱いについて関連法令を遵守する責任を負う

⑧ 監査・点検/点検責任者：（部署）（役職）氏名
情報セキュリティ対策が適切に実施されているか情報セキュリティ関連規程を基準として検証または評価し、助言を行う

作成する必要のあるすべての規程、管理表、チェックシートなどのテンプレートを提供。
*基本的にユーザーは赤字部分を自社に合わせて記載するだけで作る必要のあるドキュメントが完成する。

2026 iSecure Co., Ltd. All Rights Reserved.

FSP:専門家によるサポート

FSPをご利用いただくことで基本的にお客様ご自身でSCS評価制度の対応準備(申請まで)が可能です。が、例外的な対応を必要とする場面ではご自身の判断に迷う、あるいは対応の仕方が分からないこともあるか、と思います。そんなときのために、FSPでは認定資格を有する専門家のサポートをご用意しております。原則として、お問い合せの翌日にはご返答をお戻しすることで対応作業を遅滞なく進めていただくことが可能です。



2026 iSecure Co., Ltd. All Rights Reserved.



2026 iSecure Co., Ltd. All Rights Reserved.