Hitachi Solutions Create

HITACHI

サプライチェーンセキュリティ（SCS）評価制度対応コンサルティングサービスの紹介

2026年6月

株式会社 日立ソリューションズ・クリエイト

目次

1. はじめに

1-1.当社コンサルティングサービスの特徴

当社は、情報セキュリティコンサルティングの専門家として、お客さまのリスク管理から認証取得まで、一貫したサポートを提供します。
現場の実態に即した実践的なアプローチで、お客さまのセキュリティ強化を推進します。

審査員視点の取得支援 × 現場に寄り添う実装力 × 幅広いコンサルティング支援
＝ お客さまに最適なセキュリティ対応を実現

審査員視点で早期の取得を実現

SCS評価制度の評価基準の主体はISO27001であり、ISO27001審査員の視点からコンサルティングを実施できるため、早期の評価ランク取得ステップを踏むことが可能です。

現場実態を考慮した寄り添い型コンサル

情報セキュリティの対策は統制観点も重要な観点となります。現場の実態を考慮した実装をするなど、お客さまに寄り添ったコンサルティングを提供します。

幅広い領域を貫くコンサルティングサービス

情報セキュリティ領域において、セキュリティポリシーの整備やリスク分析・内部監査・脆弱性診断など幅広い課題にも対応可能です。

HITACHI

1-2. 日立ソリューションズ・クリエイトの強み

ISO27001認証取得支援で培った実績と日立グループの信頼を背景に、他社にはない4つの強みを提供します。

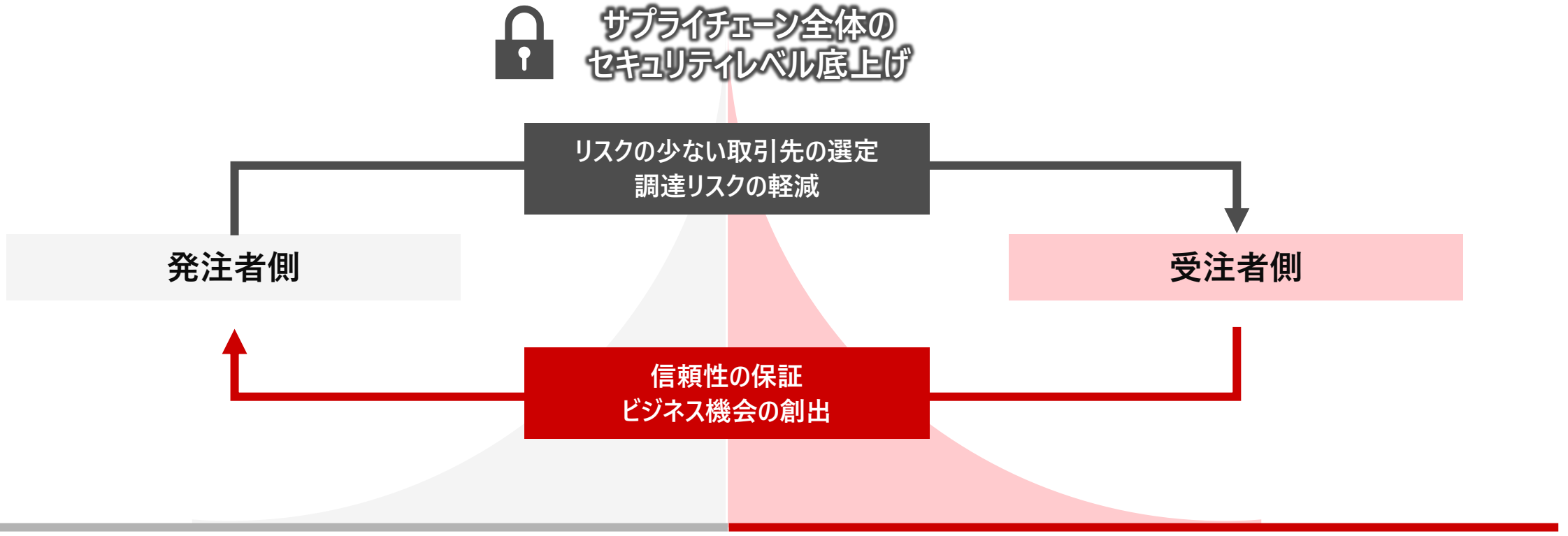
ISO27001の実績 × ワンストップの対応力 × 日立グループの安心感
＝着実・円滑に、★3「自己評価対応」・★4「第三者評価対応」の取得を実現

① ISO27001認証取得支援の豊富な実績	② 組織的・技術的対策のワンストップ対応	③ 日立グループの豊富な実績による安心感	④ 経済産業省制度への迅速なキャッチアップ
SCS評価制度の要求事項の多くがISO27001と重複しており、ISO27001認証支援で蓄積した知見やノウハウを活用可能。 お客さま内の準備工数を大幅に削減できます。	★3「自己評価対応」・★4「第三者評価対応」についてワンストップ対応が可能。 組織的・技術的対策における複数ベンダーとの調整コストが不要です。	日立グループの一員として、セキュリティ専門家チームが在籍。 継続更新を見据えた長期的なセキュリティ対策の伴走パートナーです。	2024年より経済産業省の動向を継続して確認。 制度変更・最新情報を即時反映したサポートを実現します。

2. SCS評価制度概要

2-1.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の目的

サプライチェーンを構成する企業のセキュリティ対策水準を統一の評価基準に基づいて可視化し、取引を通じて波及するサイバー攻撃リスクの低減を図る制度です。サプライチェーン全体としての信頼性・レジリエンスを高めることを目的としています。



2-2. 制度検討の背景と主旨

近年のサプライチェーン攻撃による被害の増加を受け、2024年より経済産業省により検討が開始された制度。
2026年度中の運用開始をめざす、企業のセキュリティ対策レベルを段階的（★3～5）に評価・可視化する仕組み。

① サプライチェーン攻撃による被害の増加

・サプライチェーン攻撃被害の増加による取引企業の対策水準を把握しようとするニーズの高まり

② 企業間取引における対策水準の不透明性

・受注企業側：取引先ごとに異なる対策水準への対応負担
・発注企業側：対策水準を判断する指針の不足

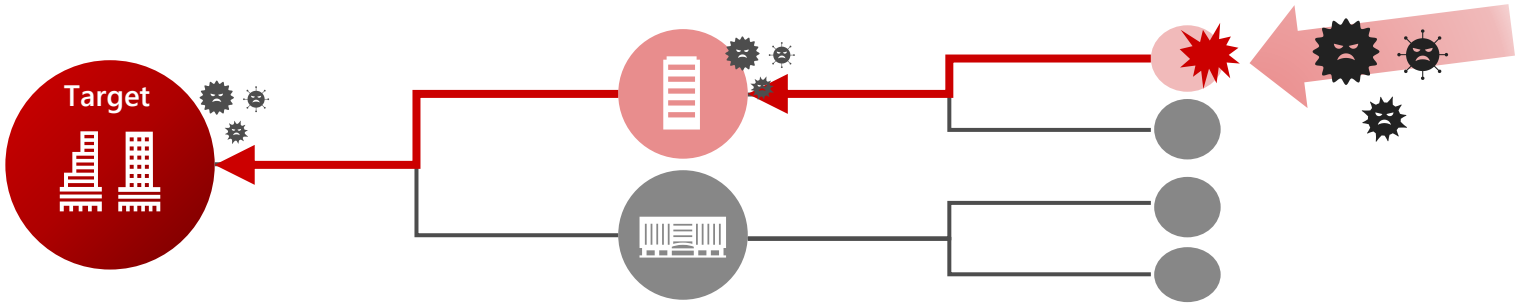
サプライチェーン強化に向けたセキュリティ対策評価制度

・サプライチェーンを構成する企業のセキュリティ対策水準を★3～★5で格付けし、可視化
・2026年3月に制度構築方針が公表され、2026年4Qに★3・★4の運用開始をめざし整備が進む
・情報セキュリティの幅広い範囲をカバー
・早ければ2027年度から取引要件に含まれる可能性があり、
対応の遅れは既存取引の縮小・見直し、競争力低下につながる恐れがある

HITACHI

2-3. 発注者側からみたサプライチェーン攻撃に対する課題

近年、サプライチェーン上の取引先や業務委託先を経由した攻撃が増加しており、認証管理や運用体制の不備が侵入経路となるケースが報告されています。
こうした攻撃は自社のみならず、取引先全体の業務継続や信頼に影響を及ぼす可能性があります。



参考：サプライチェーン攻撃のイメージ図

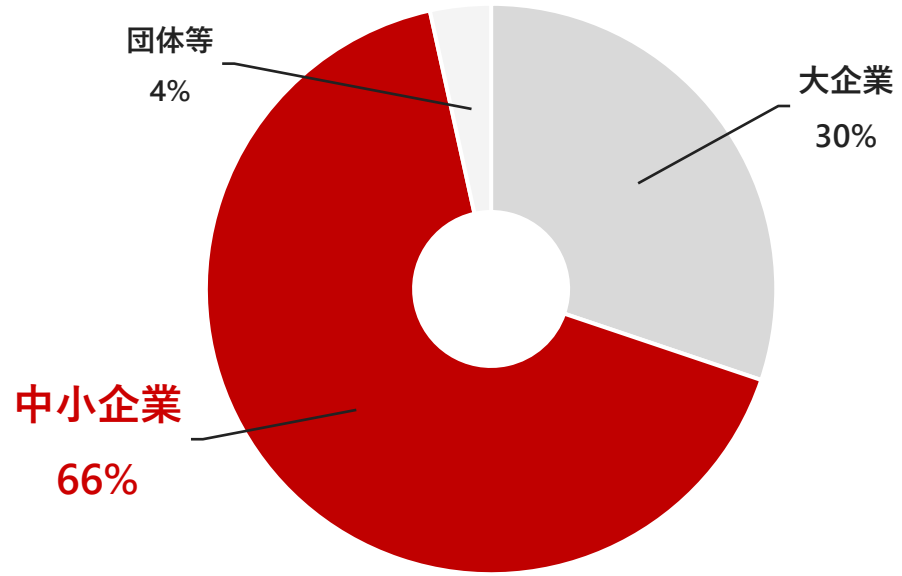
HITACHI

2-4. 受注者側からみたサプライチェーン攻撃に対する課題

ランサムウェア被害の大半は中堅中小企業となっていますが、これはサプライチェーン攻撃の第一のターゲットとされるケースが多いことが原因の一部と考えられます。また、被害にあった企業の多くには、補償費用などの負担や取引への影響が生じています。

ランサムウェア攻撃のターゲット

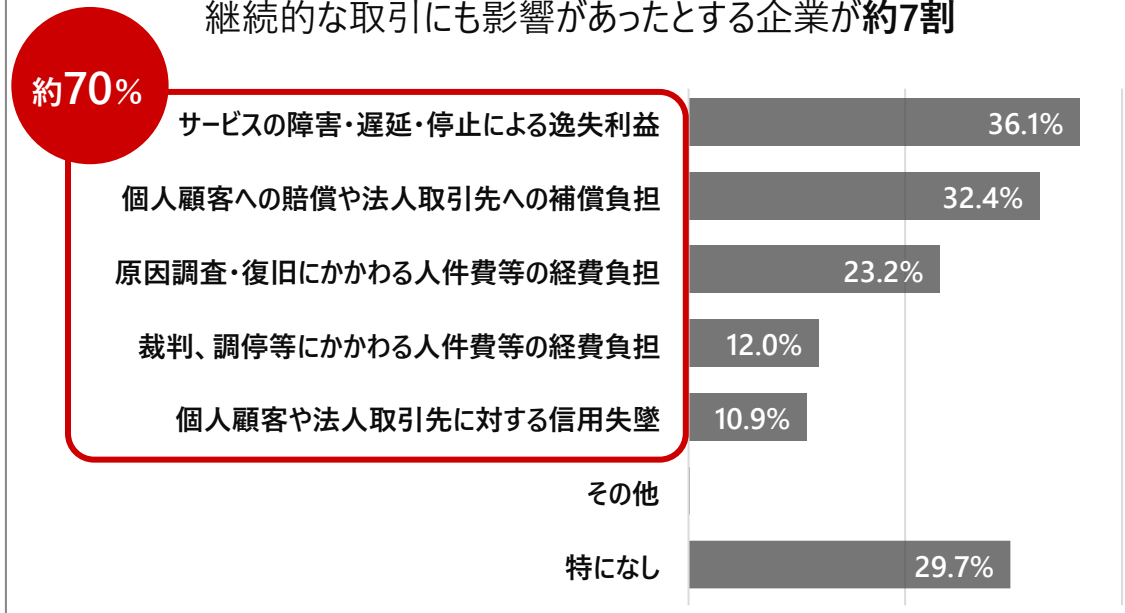
ランサムウェアの被害件数は、中堅中小の企業が66％と最多となっており、
攻撃者のターゲットとなっていることがうかがえる



参考：警察庁広報資料「令和7年度上半期におけるサイバー空間をめぐる脅威の情報等について」

約7割が取引先に影響と回答

攻撃を受けた企業の内、感染拡大による補償や経費の負担のみならず、
継続的な取引にも影響があったとする企業が**約7割**

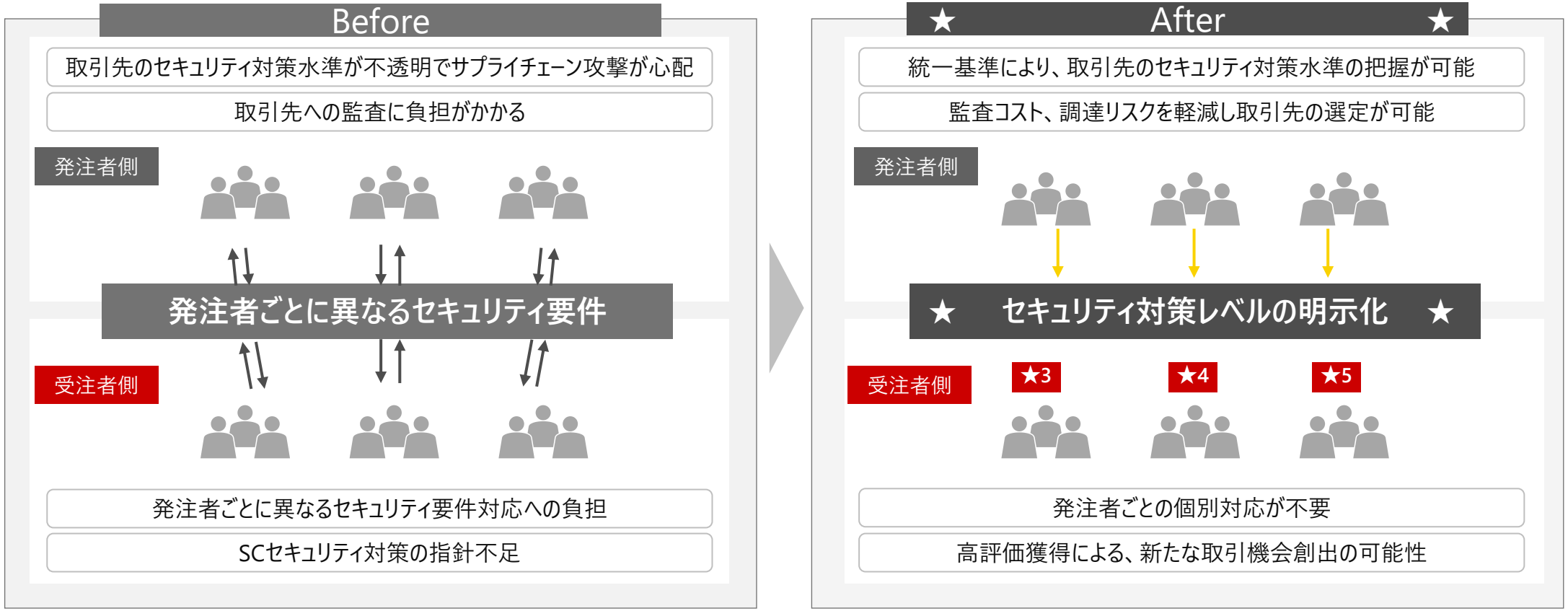


出典：IPA　2024年度中小企業等実態調査結果

HITACHI

2-5. 制度施行により予測される「企業間取引の変化」

制度施行後、発注者側の取引先選定条件の1つとして本制度の活用が期待されています。
受注者側企業は事前に自社への影響を分析し、対策を考慮する必要があります。



HITACHI

2-6. 制度の対象となる企業と、評価ランクの考え方

	★3	★4	★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	• 供給停止など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 • 機密情報など、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などが標準的にめざ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、インシデント対応など包括的な対策を実施	**サプライチェーン企業などが到達点としてめざすべき対策** • 国際規格などにおけるリスクベースの考え方に基づき、自社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
評価スキーム	専門家確認付き自己評価 ※1	第三者評価 ※2	第三者評価　※2
有効期間	1年	3年	今後検討

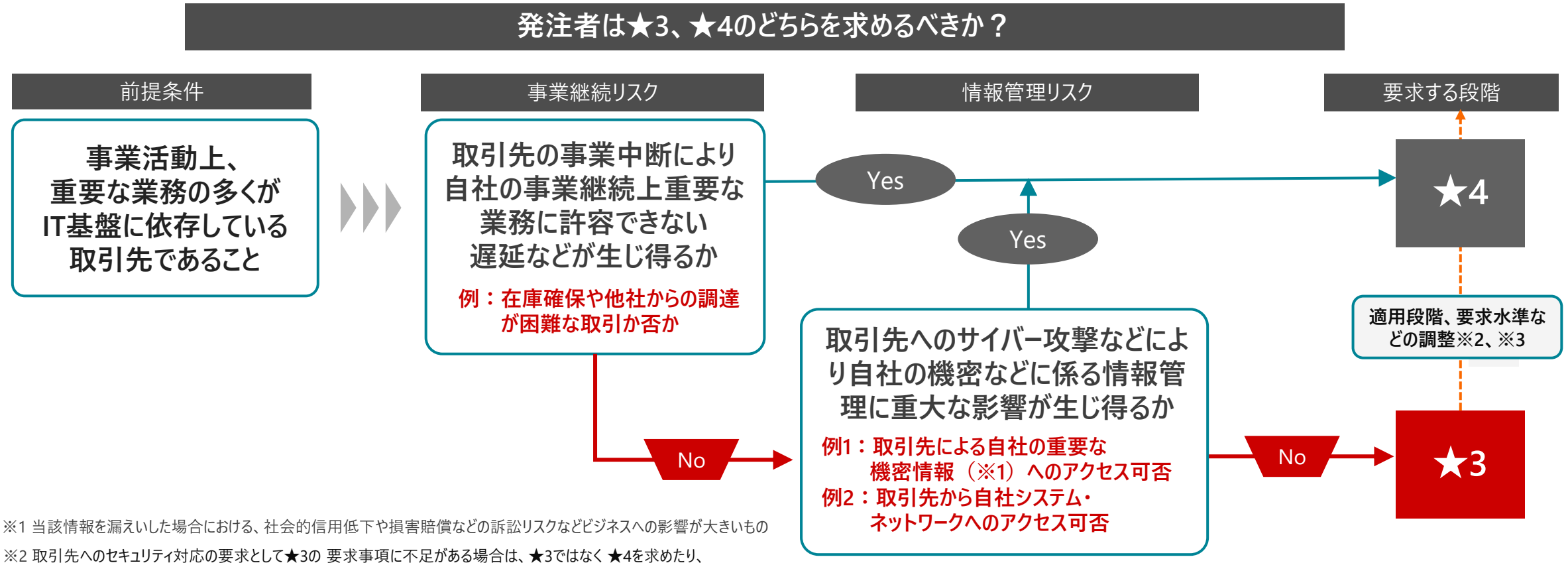
※1 ★取得希望組織が自ら実施した評価の結果について、セキュリティ専門家による確認および助言を経て、取得希望組織の評価結果として確定させることをいう。

※2 ★取得希望組織が自ら実施した評価の結果について、★取得希望組織以外の組織（評価機関）による評価などを経て、評価結果として確定させることをいう。

参考：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を基に作成

HITACHI

2-7. ＜参考＞【発注者側】が受注者側に要求する段階（★3、★4）の考え方の例



※1 当該情報を漏えいした場合における、社会的信用低下や損害賠償などの訴訟リスクなどビジネスへの影響が大きいもの

※2 取引先へのセキュリティ対応の要求として★3の 要求事項に不足がある場合は、★3ではなく ★4を求めたり、
それぞれの要求事項へ必要な対策を上乗せしたりすることも想定される。

※3 調整するための追加要素（例）
・直近で当該取引先または同業他社など でインシデントが観測されるなど、リスク増大が懸念されるか
・再委託先に自社にとって重要な事業者 が含まれるか

参考：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を基に作成

HITACHI

2-8. ＜参考＞【受注者側】が準備するべき段階（★3、★4）の考え方の例

受注者は★3、★4のどちらを取得するべきか？

前提条件	発注者側と取引は主にIT基盤（受発注システムなど）で行われているか
事業継続リスク	自社の事業中断が原因となり、発注者側の業務に許容できない遅延が生じるか
情報管理リスク	自社の環境から、発注者側の内部システムへアクセスができるか

★3	いずれにも該当しない（※）
★4	1つ以上該当する

参考：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を基に作成

HITACHI

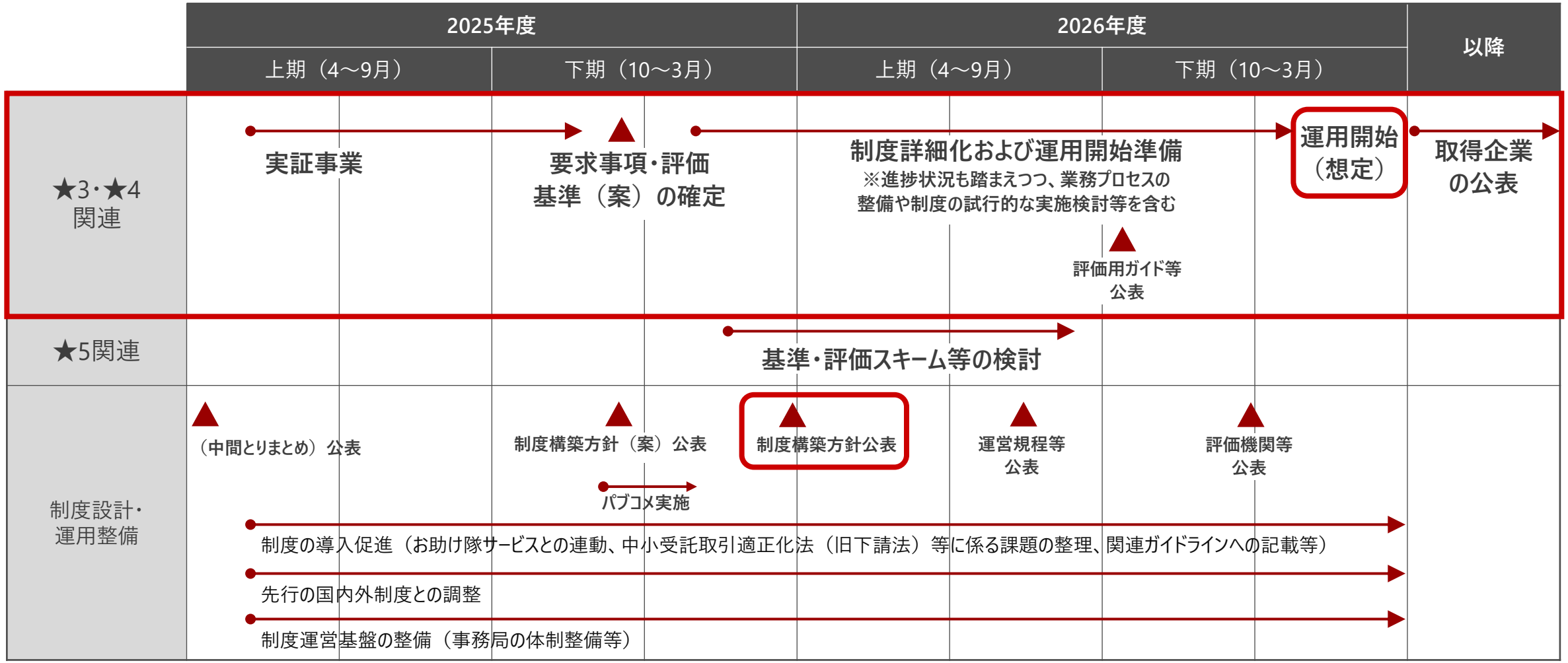
2-9. 評価ランクの概要

	★3	★4	★5
評価実施主体	自己評価 適合性評価の対象となる組織自身	第三者評価 指定委員会から指定を受けた評価機関	構築中
有効期間	1年	3年	
必要な手続き	・有効期限を更新するため、要求事項の遵守状況について、年次でセキュリティ専門家の確認・助言を経た自己評価の更新版を事務局へ提出する	・有効期間内は、1年ごとに自己評価を実施し、結果を評価機関に提出する 1年ごとに提出する自己評価結果について、前回取得時に設定した適用範囲の変更又は要求事項・評価基準の達成に顕著な影響を及ぼす変更がある場合は、再度評価機関の評価を受ける。 ・有効期限を更新する際（3年に1回）は第三者評価を受ける	
合格基準	・原則として、全ての評価基準への適合を求める		
★の取り消し等	内部通報等により、取得組織において虚偽報告、情報隠蔽等の不正行為が確認された場合、評価機関または事務局から★の一時停止または取り消しを行う場合がある		

参考：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を基に作成

HITACHI

2-10. 制度開始に向けたスケジュール



参考：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を基に作成

3. 制度における評価スキーム

HITACHI

3-1. 要求事項の概要

★3、★4ともに、要求事項（評価基準）の多くが、既存の国内外のセキュリティガイドラインや認証規格を「**参考文献**」として採用しています。**評価ランク取得には、★3および★4それぞれの要求事項全てに対応する必要があります。**

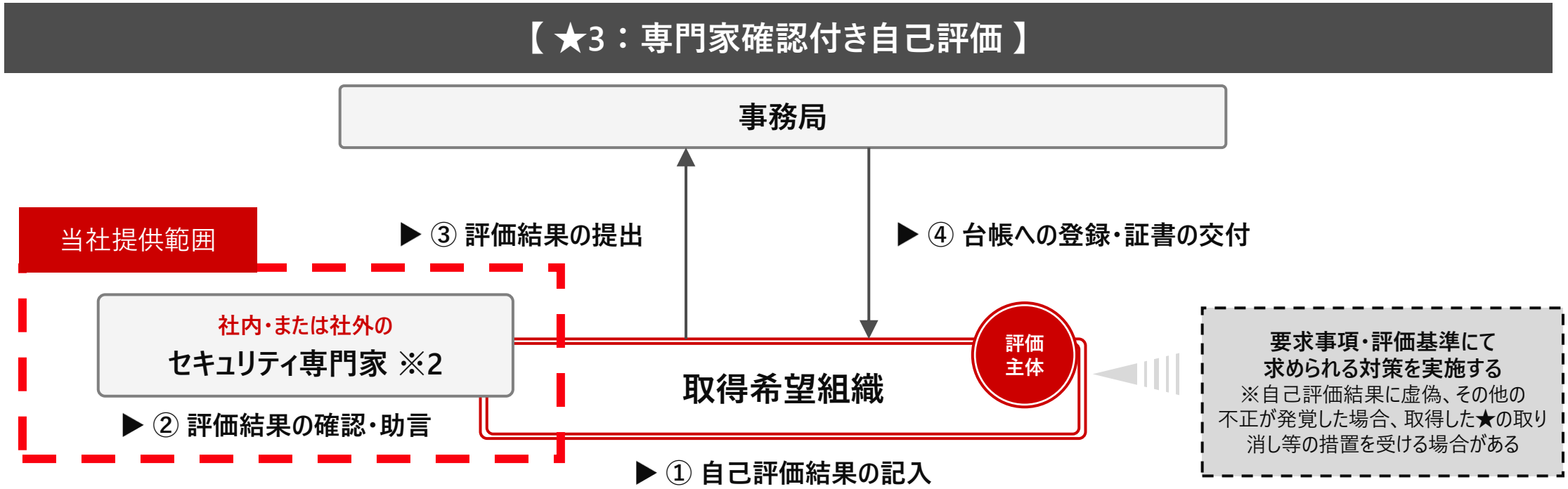
▶ 各要求事項のサマリ

大分類	中分類	★3評価基準	ISO27001	中分類	★4評価基準	ISO27001
① ガバナンスの整備	2	8	8	4	19	19
② 取引先管理	1	4	2	1	7	4
③ リスクの特定	1	11	11	2	29	27
④ 攻撃等の防御	5	48	48	5	82	81
⑤ 攻撃等の検知	1	3	3	2	8	8
⑥ インシデントへの対応	1	6	6	1	6	6
⑦ インシデントからの復旧	1	1	1	1	2	2
	12	81	79 （97.5%）	16	153	147 （96.0%）

参考：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構築に向けた中間取りまとめを基に当社にて集計し作成

HITACHI

3-2. 評価スキーム★3：セキュリティ専門家による確認を経た取得希望組織による自己評価

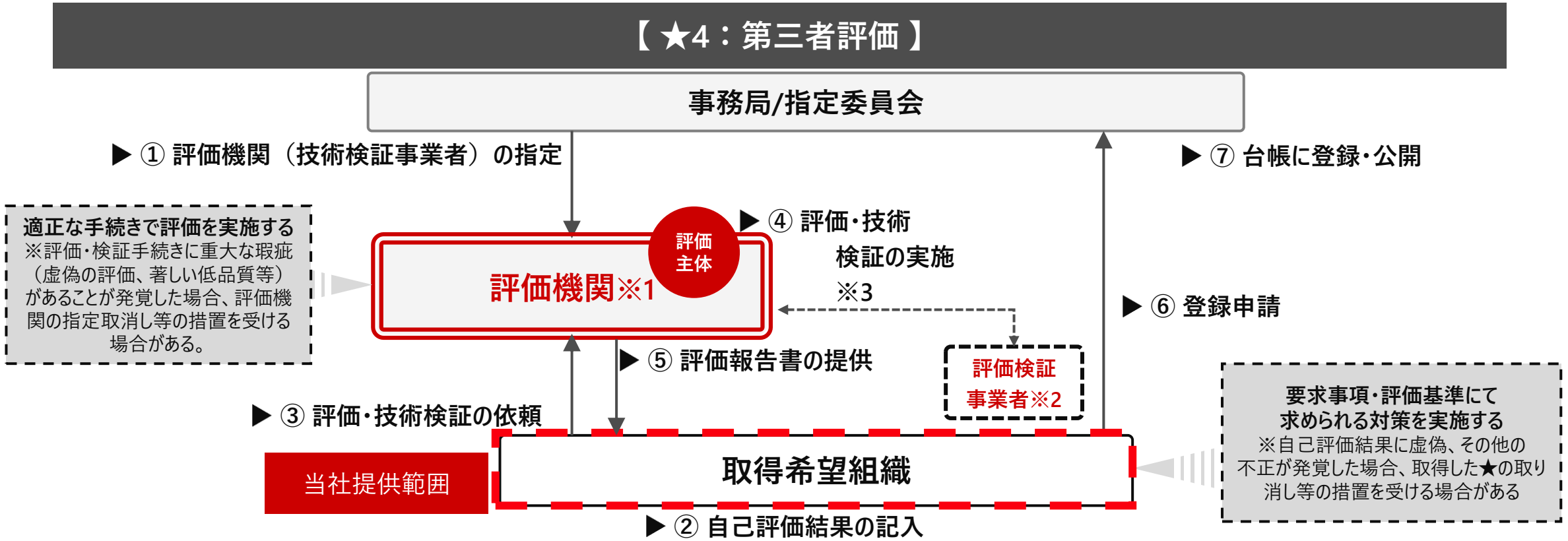


※1 経営層による自己適合宣言を経た取得希望組織として実施する評価のことを指し、組織内のセキュリティを担当する担当者や部門が独自に実施する評価は含まれない。
※2 取得希望組織が実施した自己評価結果に対してその内容の確認・助言を実施する者であって、**一定のセキュリティ関連資格を有し、かつ、制度側で指定した研修を受講したもの**をいう。確認・助言に係る作業については、制度側で指定した研修を受講した作業従事者に実施させることができる。

参考：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を基に作成

HITACHI

3-3. 評価スキーム★4：「第三者評価」および「技術検証の実施」



※1 指定委員会による指定を受けた組織であって、取得希望組織外の立場で★4取得希望組織に対する第三者評価を実施するものをいう。
※2 指定委員会による指定を受けた組織であって、取得希望組織外の立場で★4取得希望組織のIT基盤などに対して制度側が指定した方法による技術的な検証を実施するものをいう。
※3 技術検証については評価機関内部で実施する場合と評価機関が外部事業者に委託して実施する場合が想定される。

参考：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を基に作成

4. サービス内容（★3取得支援）

HITACHI

4-1. 取得支援サービス（範囲）

お客さまご自身で作成された「自己評価」に対する内容確認・修正を含めた助言を行うサービス（A）および自組織での作成が困難である場合「自己評価」の記入から支援するサービス（B）の2種類のサービスを提供します。

今回の説明対象

お客さま担当項目　当社担当項目

※1　別途オプションにて規定類の作成・修正が可能です。また、各種セキュリティソリューションの提案も可能です。

【★3】A. 自己評価支援サービス

Step 1	★3要求事項に基づき自己評価を記入	
Step 2	評価内容の確認、必要に応じた評価結果の修正を含む助言	
Step 3	助言に基づき、修正や対策実施	※1
Step 4	事務局へ提出する内容に関して確認し、了承した場合に署名を実施	
Step 5	事務局へ提出	

【★3】B. 自己評価シート作成支援サービス

Step 1	★3要求事項への記入支援（評価結果の修正など助言を含む）	
Step 2	助言に基づき、修正や対策実施	※1
Step 3	事務局へ提出する内容に関して確認し・了承した場合に署名を実施	
Step 4	事務局へ提出	

4-2. A.自己評価支援サービス（タスク）

①自己評価の実施

SCS評価制度★3の要求事項に対して、お客さまご自身が対応状況を確認し、自己評価結果を作成します。

②自己評価結果の全体確認

お客さまが作成された自己評価結果を確認し、SCS評価制度が求める観点やどの程度準拠できているかを客観的に確認します。

③自己評価結果に対する妥当性の確認

お客さまの情報セキュリティ規定類や運用結果エビデンス（ログ・アクセス権など）を確認し、自己評価結果の妥当性を客観的に確認します。必要に応じて、管理者へのヒアリングも実施します。

④アセスメント結果報告

自己評価結果に対する妥当性の確認結果として、各観点への準拠性や改善課題※一覧をまとめ、お客さまへ報告します。

⑤改善課題への対応※

アセスメントで特定した改善課題に基づき、セキュリティ対策を実施します。

⑥申請準備・署名

お客さまにて対策した内容を反映した申請書を作成します。当社にて、内容を確認し、問題なければ署名します。

⑦事務局へ提出

申請書と必要なエビデンス一式をそろえて、事務局へ提出します。

※アセスメントで特定した改善課題に基づき、制度取得に必要な"セキュリティ規定類の整備"を別途オプションとして支援することも可能です。
また、必要に応じて各種セキュリティソリューションのご提案も可能です。

4-2. A.自己評価支援サービス（作業内容）

A.自己評価支援サービスの作業内容は以下の通り。

#	タスク	当社作業	お客さま作業	アウトプット
1	自己評価の実施	– ・自己評価結果の受領	・自己評価記入シートへ結果の記入 ・自己評価結果の提供	・自己評価結果 （記入済み自己評価記入シート）
2	自己評価結果の全体確認	・自己評価結果の確認 ・妥当性確認に向けてのセキュリティ規定類や運用エビデンスの提供一覧作成・提出依頼	・自己評価結果の概要説明 ・セキュリティ規定類や運用エビデンスなどの提供	・自己評価結果の確認結果（ドラフト） ・セキュリティルールや運用エビデンスの提供一覧
3	自己評価結果に対する妥当性の確認	・自己評価結果に対する妥当性の確認 （ルールの観点、運用結果の観点など） ・上記不明点や妥当性確認に向けた管理者ヒアリング ・妥当性・ヒアリング結果を踏まえた改善課題一覧作成	– ・ヒアリングへの対応 ・改善課題一覧の確認	・自己評価結果の確認結果 ・改善課題一覧
4	アセスメント結果報告	・アセスメント結果報告書の作成 ・アセスメント結果の報告会実施	– ・アセスメント結果報告会への参加	・アセスメント結果報告書
5	改善課題への対応※	・改善課題への対応確認	・改善課題への対応実施	・改善課題一覧（対策完了版）
6	申請準備・署名	– ・申請関連資料の受領 ・申請関連資料の確認と署名 ・署名済み申請関連資料の返却	・申請書類の記載、必要な資料の整理 ・申請関連資料の提供 – ・署名済み申請関連資料の受領	・署名済み申請関連資料
7	事務局へ提出	– –	・申請書類、必要な資料の整理 ・事務局への申請	・認定証書 ・★3認定取得台帳

※アセスメントで特定した改善課題に基づき、制度取得に必要な“セキュリティ規定類の整備”を別途オプションとして支援することも可能です。
また、必要に応じて各種セキュリティソリューションのご提案も可能です。

HITACHI

4-3. A.自己評価支援サービスのスケジュール（案）

※ スケジュールは、担当コンサルタントとお客さまとの打ち合わせにより、確定します。
※ タスク1～4でのサービス提供も可能です。

作業タスク		プロセス	202X年度 1カ月	2カ月	3カ月	4カ月＋αカ月
打ち合わせ			▼ ▼	▼ ▼ ▼	▼ ▼	▼ ▼
1	自己評価の実施	自己評価結果の提供	■			
2	自己評価結果の全体確認	自己評価結果の確認	■■■			
		規定類や運用エビデンスの提供一覧作成	■			
3	自己評価結果に対する妥当性の確認	自己評価結果に対する妥当性の確認		■■■		
		管理者へのヒアリング		■		
		改善課題一覧作成		■		
4	アセスメント結果報告	アセスメント結果報告書の作成			■	
		アセスメント結果報告の実施			■	
5	改善課題への対応	改善課題への対応実施				■ 署名
6	申請準備・署名	申請書類の記載・資料の準備 資料内容の確認・署名				■
7	事務局へ提出	事務局への申請実施				■

Point アセスメントで特定した改善課題に基づき、制度取得に必要な"セキュリティ規定類の整備"を別途オプションとして支援することも可能です。
また、必要に応じて各種セキュリティソリューションのご提案も可能です。

5. サービス内容（★4取得支援）

HITACHI

5-1.【★4】取得支援サービス

ISO27001に関連した複数サービスの長年にわたる提供で得た知見を生かし、「ISO27001認証取得支援サービス」をベースとした★4取得支援サービスを提供します。

取得支援プロセスイメージ

※ 構築フェーズ以降のスケジュールについては、アセスメントの結果により、変動します。

計画フェーズ → 構築フェーズ → 確認・検証フェーズ

アセスメント
「改善課題の明確化」

提供内容
- 自己評価記入シートの確認
- ヒアリングによる妥当性確認
- 改善課題の抽出

成果物
- 確認結果、課題一覧

想定期間
- 2～3カ月

対応計画確定
「取得計画の策定」

提供内容
- 確認結果報告
- 対応範囲、スケジュール確定
- 役割分担定義（お客さま/当社）

成果物
- 取得計画、役割分担表

想定期間
- 1～1.5カ月

改善・支援
「改善課題への対応」

提供内容　※1
- 規定類の策定・修正
- 改善課題への対策
- セキュリティ運用の実施

成果物
- 自己評価結果（対策結果記入）

想定期間
※確認結果の内容により変動

確認・検証対応
「★4取得の実現」

提供内容
- 事前評価計画
- 事前文書審査
- 現地審査シミュレーション

成果物
- 事前評価実施計画書
- 事前評価結果報告書

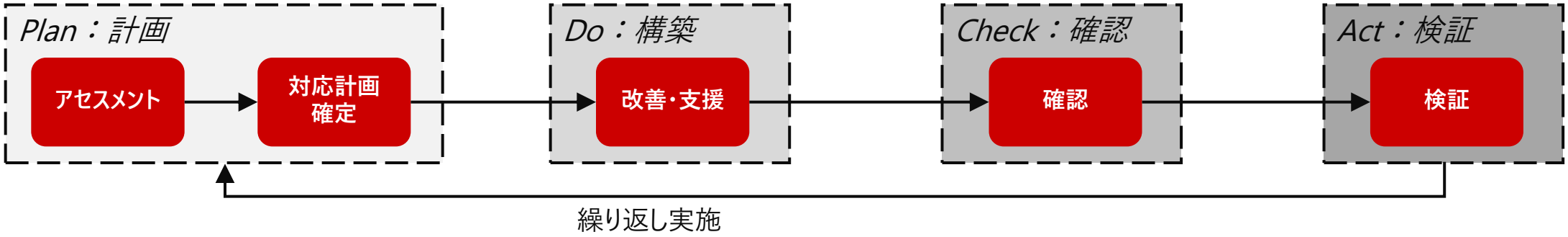
想定期間
- 1～1.5カ月

※1　別途オプションでの支援可能

HITACHI

5-2.【★4】取得支援サービス（全般）

★4取得に向けてはマネジメントシステム（PDCA）として取り組むことが必要です。



フェーズ	フェーズ名	作業内容
Plan：計画	アセスメント	① 自己評価の実施　② 自己評価結果の妥当性確認 ③ 改善課題一覧の作成
	対応計画確定	①アセスメント結果報告書の作成　② 取得計画の作成
Do：構築	改善・支援	① セキュリティルール見直し・修正　② 改善課題への対策 ③ セキュリティ運用の実施　④ 組織内への周知（セキュリティ教育など）
Check：確認	確認	① 事前評価計画書作成　② 事前文書評価実施 ③ 現地審査シミュレーション
Act：検証	検証	① 評価機関による評価・技術検証対応（初年度、以降3年ごと） ② 是正処置実施　③評価機関への提出（毎年）

ご参考

HITACHI

当社は以下の特長を生かし、コンサルティングサービスを提供いたします

実績・スキルを持つコンサルタントの対応

さまざまな業界におけるガイドライン／標準などの適用支援やプロセス改善支援の
実績を豊富に有した要員により、お客さまのご要件に合わせて柔軟に対応します

ノウハウ・知見の活用

ベースラインとなる国際規格・各種基準・ガイドラインやテンプレートの活用などに関する
ノウハウ・知見を最大限に活用します

強力なバックアップ体制の確保

状況に応じ、CSIRT、セキュリティ診断チーム・品質管理部門などの社内有識者と連携し、
後方支援を受けられる体制を整えています

**豊富なコンサルティング実績を有する要員により、
ノウハウ・知見を最大限に活用した対応を行います**

HITACHI

近年における当社の主なコンサルティング実績は次の通り

コンサルティング実績

支援実績 80件以上　　長期支援実績 約20年継続

NO	サービス名称	実績	
1	ISO27001・Pマーク認証 （ポリシー策定含む）	◆【食品】 菓子製造会社関連 ◆【輸送用機器】 自動車関連 ◆【精密・諸工業】 精密機器製造関連	◆【電気機器】 基盤系製造関連 ◆【卸売業】 商社関連 ◆【小売業】 レストラン運営関連
		◆【情報・通信】 テレビ会社関連、独立系システム開発関連、証券系ソフト開発関連、証券系運用サービス関連、損保系システム関連、生保系システム関連 他多数	
2	ISO9001認証	◆【情報・通信】 システムコンサルティング関連 独立系システム開発関連 他多数	
3	ISO20000認証	◆【情報・通信】 損保系運用サービス関連、金融系運用サービス関連、生保系運用サービス関連、システム運用サービス会社 自動車関連会社	
4	ISO22301認証	◆ 製造系センターサービス関連	◆ 病院関連、 他BCMS関連構築

お問い合わせ先

HITACHI

■お問い合わせ先

株式会社 日立ソリューションズ・クリエイト

- **Webでのお問い合わせ**
  https://www.hitachi-solutions-create.co.jp/solution/attestation/
- **メールでのお問い合わせ**
  hsc-contact@mlc.hitachi-solutions.com

■お問い合わせ情報について

ご相談、ご依頼いただいた内容は回答などのため、当社の関連会社（日立ソリューションズグループ会社）および株式会社日立製作所に提供（共同利用含む）することがあります。
取り扱いには充分注意し、お客さまの許可なく他の目的に使用することはありません。

表示に関する注意事項

HITACHI

■サービス・製品の仕様に対する表示

本資料に記載しているサービス・製品の仕様・価格は、2026年6月時点のものです。
サービス・製品の改良などにより予告なく記載されている仕様が変更になることがあります。

HITACHI