Hitachi Solutions Create

HITACHI

「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」

受注者側企業がいま準備するべき対策とは

株式会社日立ソリューションズ・クリエイト

目次

※本資料は経済産業省「サプライチェーン強化に向けたセキュリティ対策 中間報告」を基に、2025年9月1日時点の情報を基に作成しています。

1-1. 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です。
サプライチェーン全体のセキュリティ信頼性の向上と、発注者・受注者双方の負担軽減を目的としています。

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

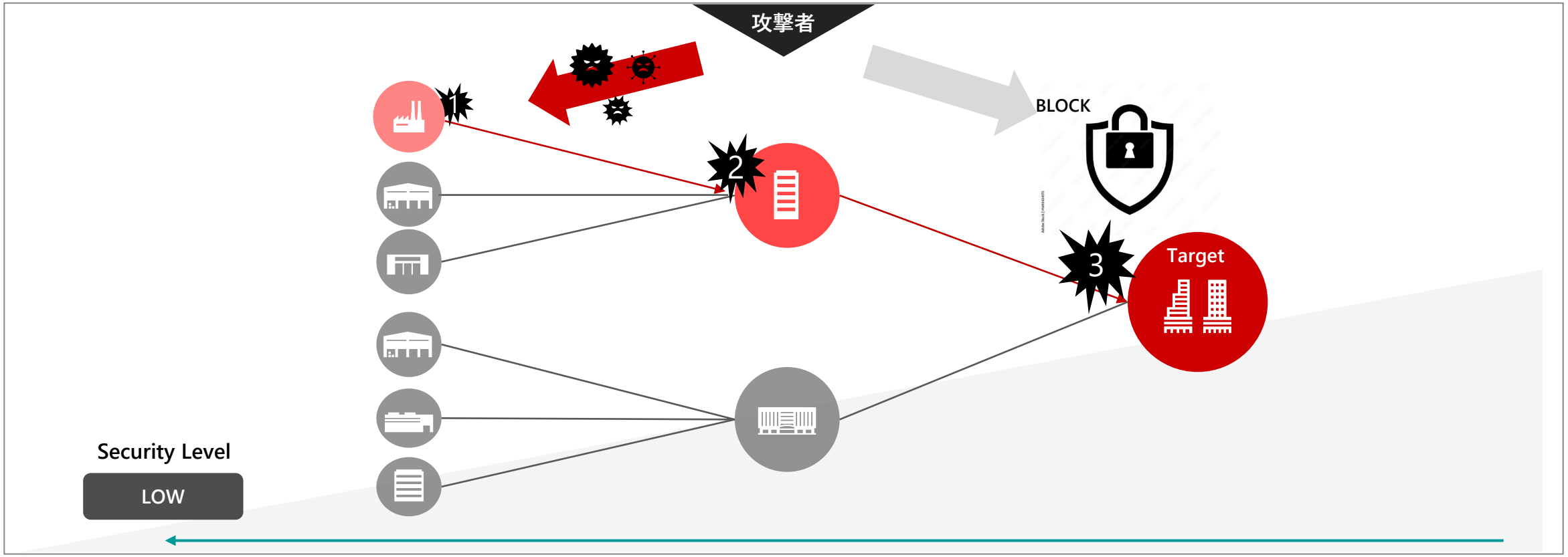
サプライチェーン強化に向けたセキュリティ対策評価制度

・**サプライチェーンを構成する企業を★3～★5で格付け**
・2026年下期（10月以降）の一部本格運用をめざし、検討が進む
・情報セキュリティの幅広い範囲をカバー
・発注・受注企業双方で事前準備が必要
・**早ければ2027年度から取引要件に含まれる可能性がある**

HITACHI

1-2. サプライチェーン攻撃とは

セキュリティ対策水準が高く、攻撃難易度が高い標的企業を直接攻撃するのではなく、**比較的対策水準が低い取引先企業などを攻撃の起点**とし、最終的に標的とした企業へ到達する攻撃の手法です。



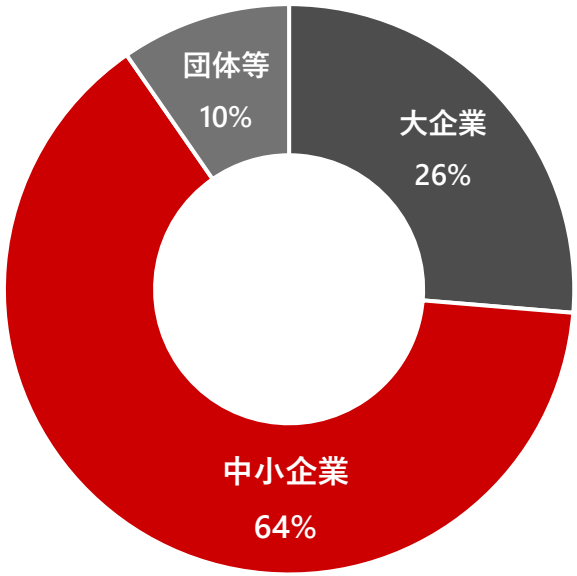
HITACHI

1-2. サプライチェーン攻撃とは

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**1st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

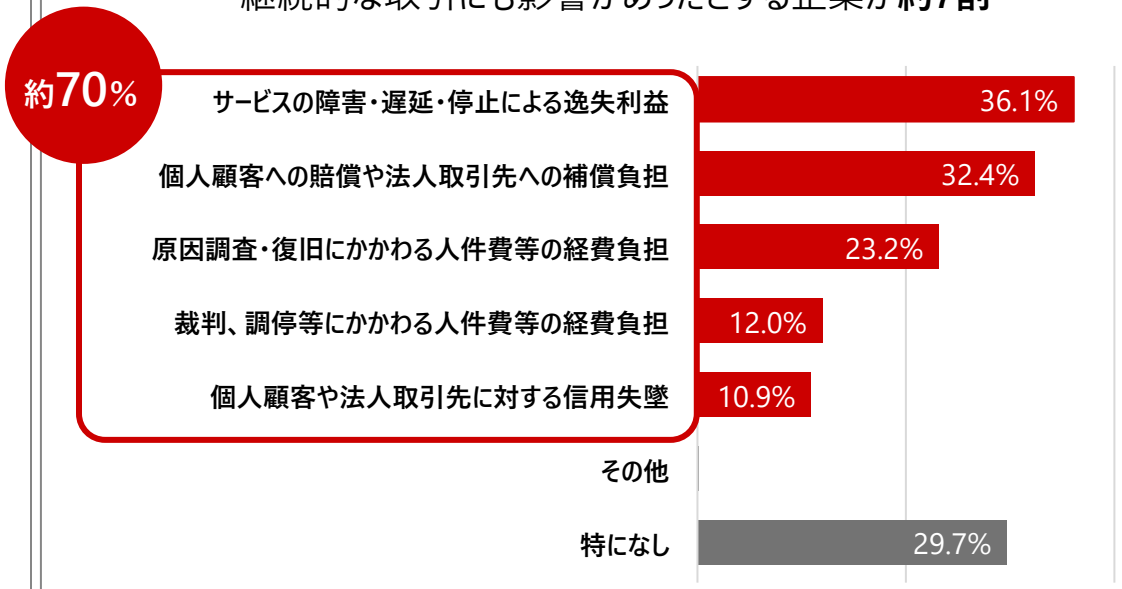
ランサムウェアの被害件数は、中堅中小の企業が64％と最多となっており、
攻撃者のターゲットとなっていることがうかがえる



参考：警視庁広報資料「令和6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」を基に作成

約7割が取引先に影響と解答

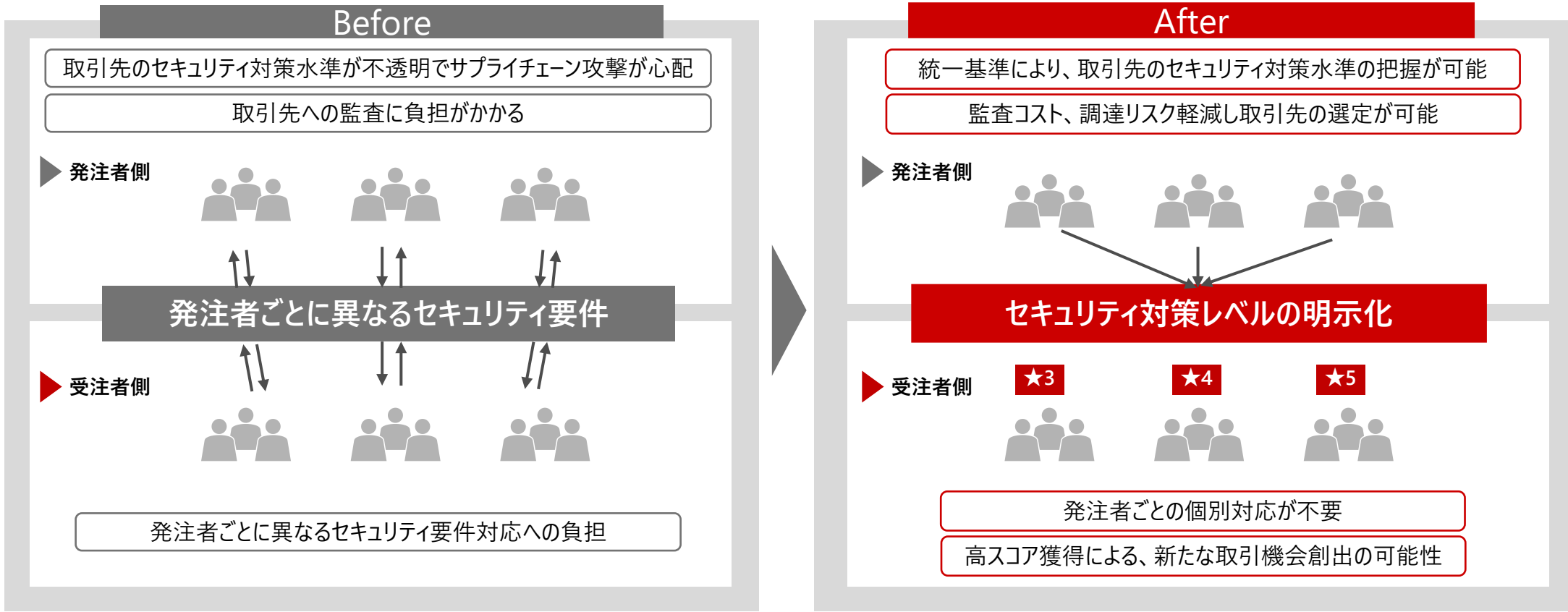
攻撃を受けた企業のうち、感染拡大による補償や経費の負担のみならず、
継続的な取引にも影響があったとする企業が**約7割**



出典：IPA　2024年度中小企業等実態調査結果

1-3. 制度施行による予測される「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

2-1. 制度の対象となる企業と、評価ランクの考え方

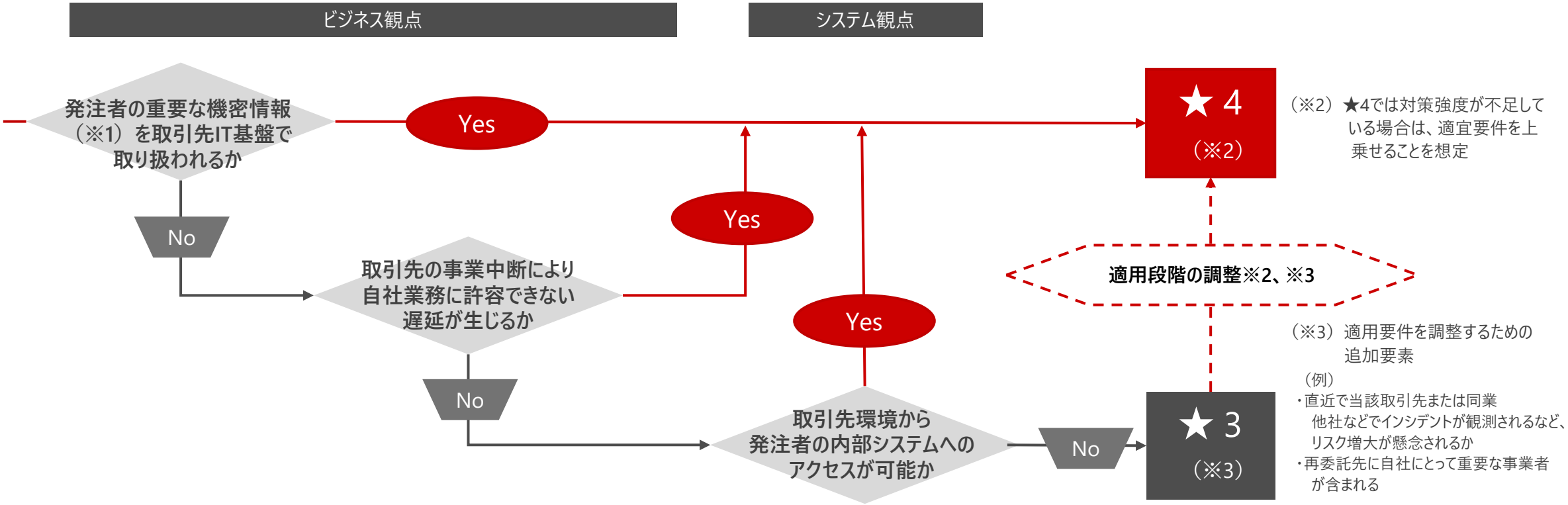
本制度はサプライチェーンを形成する全体のセキュリティ水準を底上げすることを目的としており、**サプライチェーンを構成する全ての企業に対応が求められています。**

	★3	★4	★5
対象事業者のイメージ	原則、 サプライチェーンを構成する全ての企業	サプライチェーンにおいて重要な機能・役割を担う企業	サプライチェーンにおいて特に重要な機能・役割を担う企業。特にインフラ事業など社会的影響度の高いもの。
対策の基本的な考え方	広く知られたぜい弱性を突くサイバー攻撃への対処を目的に、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なセキュリティ対策	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（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）	高度なサイバー攻撃への対処を念頭に、めざすべきセキュリティ対策として、侵入の早期検知と被害の極小化などシステムに対するより高度な対策にて構成
評価方法	自己評価	第三者評価	第三者評価
有効期間	1年	3年	未定

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作成

HITACHI

2-2.「★3」、「★4」のどちらを取得すべきか？



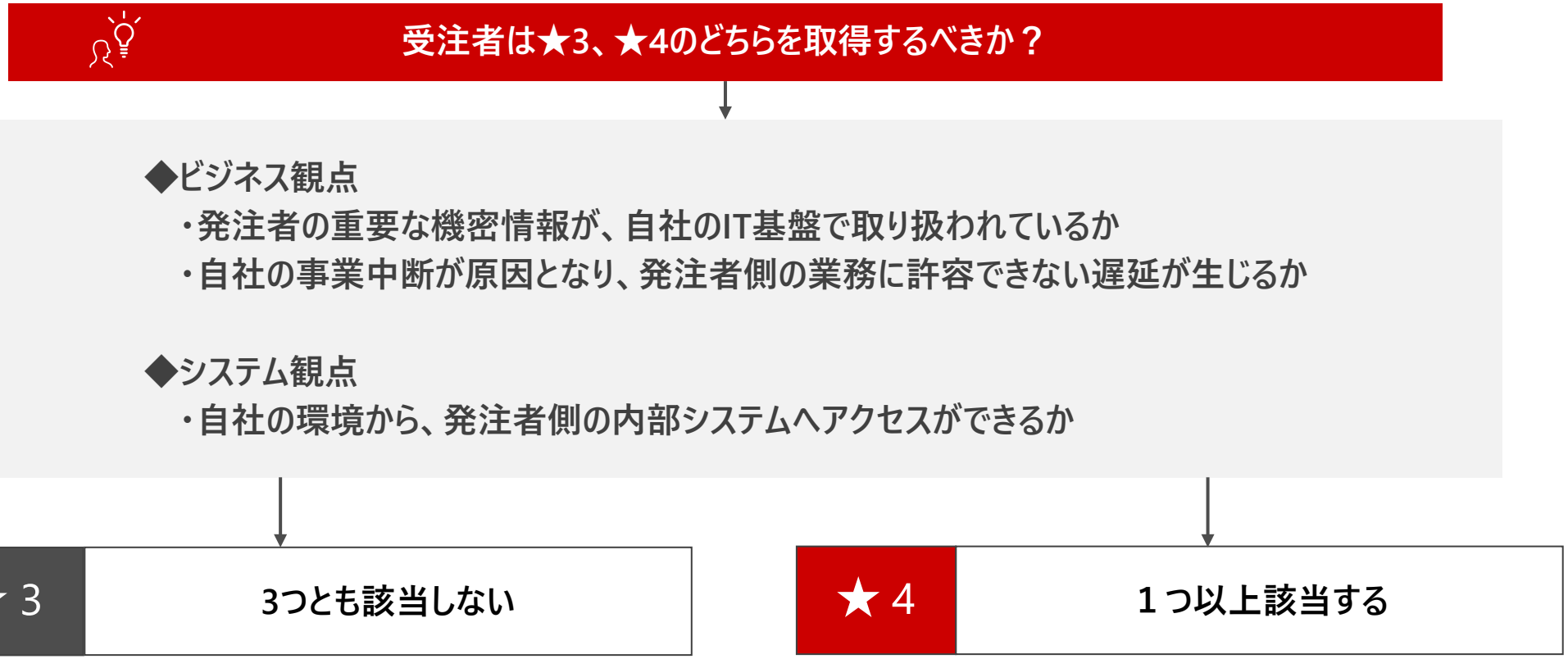
（※1）当該情報を漏えいした場合における、社会的信用低下や損害賠償などの訴訟リスクなどビジネスへの影響が大きいもの

（※4）単発・一過性の調達や、市販品など市場で用意に代替え可能な製品・サービスの調達などのうち、重要度が相対的に高いとは言えないものは、本フローから外すことも考えられる

出典：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

2-2.「★3」、「★4」のどちらを取得すべきか？

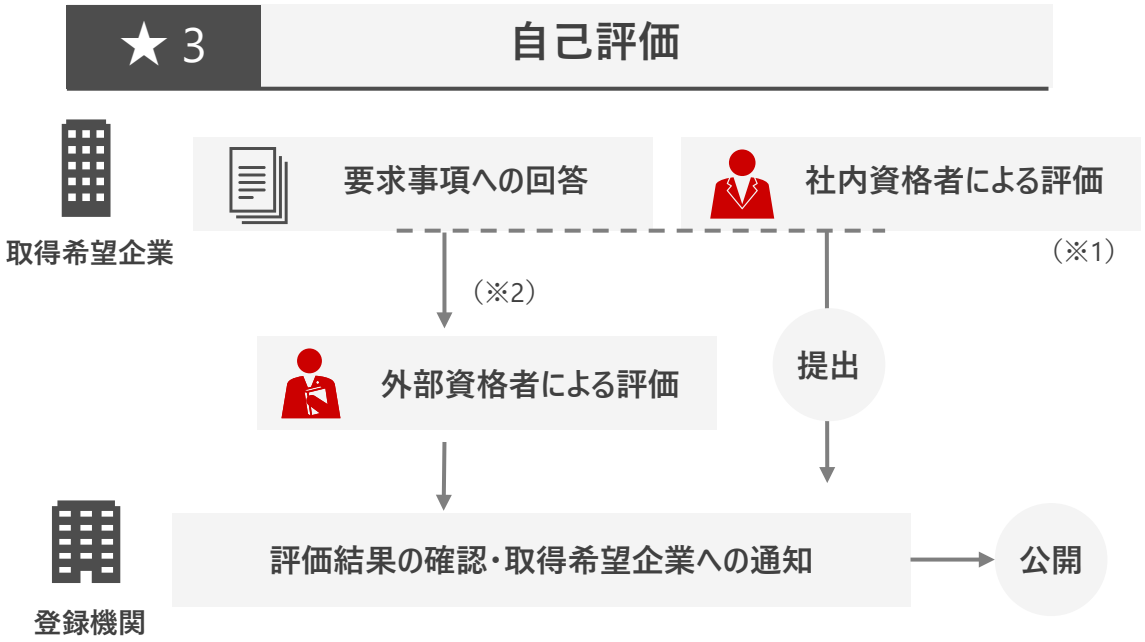
以下3点に全て当てはまらず★3に該当した場合でも、**直近のインシデント発生状況などに照らしての★4への段階調整や、対策要件自体の上乗せなどが発注者の判断で実施されることが想定されています。**

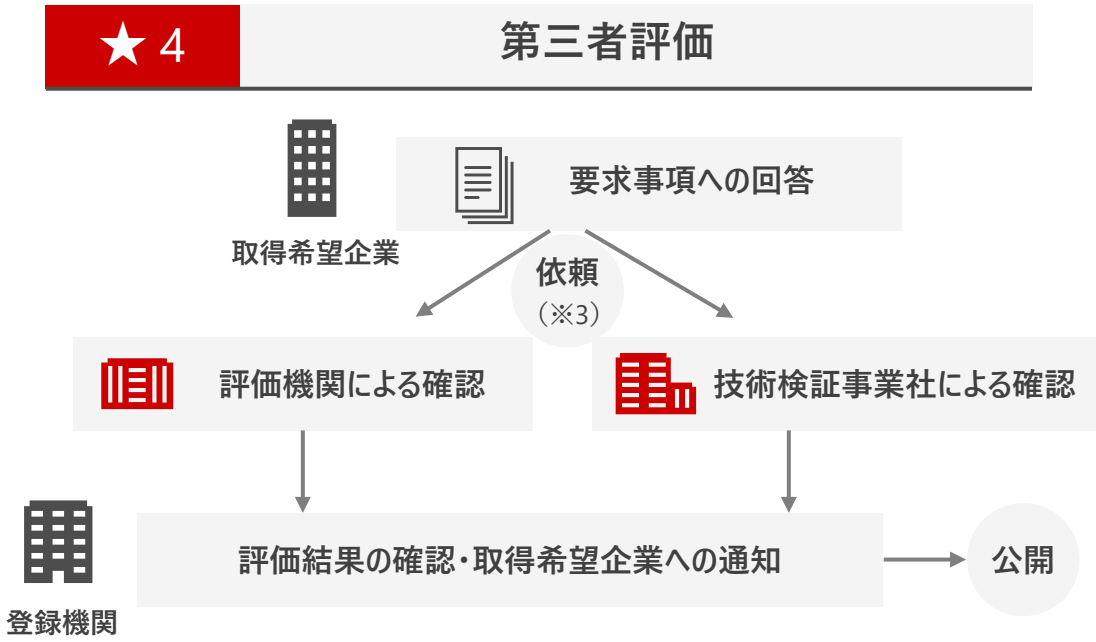


HITACHI

3-1. 評価スキーム

★3は自己評価制ですが、要求事項への回答について**社内・外の資格者（※1）による評価が必要。**
★4は**認定を受けた評価機関、または技術検証機関による第三者評価**が必要です。





（※1） 情報処理安全確保支援士、セキュリティプレゼンター、ITコーディネーター（候補）
（※2） 主に社内資格者がいない場合
（※3） 評価機関または、技術検証事業社へ評価の依頼

（※） 赤アイコンは評価主体

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作成

HITACHI

3-2. 要求事項の概要

★３、★4ともに、特にサプライチェーン攻撃への対応強化を念頭とした「アイデンティティ管理とアクセス制御」に重きを置きつつ、**技術的要件にとどまらず、情報資産の棚卸しや規定の策定、従業員教育など幅広い項目が設定されています。**

大分類	中分類	★3	技術的要件	★4	技術的要件
① ガバナンスの整備	組織的文脈	–		1	
	役割 / 責任 / 権限	2		3（5）	1
	ポリシー	1		1	
	監督	1		2（3）	
② 取引先管理	サイバーセキュリティ サプライチェーンマネジメント	2		5（6）	
③ リスクの特定	資産管理	4		4（7）	
	リスクアセスメント	–		1	1
④ 攻撃の防御	アイデンティティ管理とアクセス制御	7	7	9（11）	11
	意識向上及びトレーニング	1		3	
	データセキュリティ	1	1	4（5）	3
	プラットフォームセキュリティ	3	1	5（7）	4
	技術インフラのレジリエンス	1	1	2（3）	3
⑤ 攻撃などの検知	継続的モニタリング	1	1	2（3）	3
	有害イベントの分析	–		1	
⑥ インシデントへの対応	インシデントマネジメント	1		1	
⑦ インシデントからの復旧	インシデント復旧計画の実行	–		1	

★３		
25項目	技術的要件	11
	組織的要件	14

★４		
45項目 (59)	技術的要件	27
	組織的要件	32

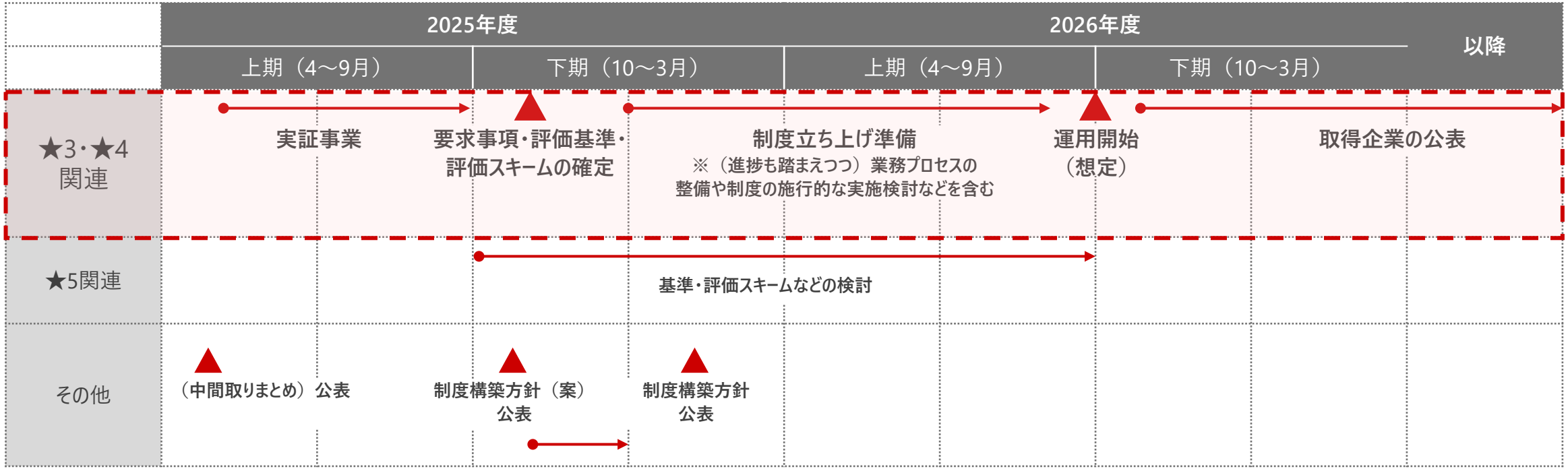
参考：経済産業省：サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめを基に作成

HITACHI

3-3. 制度開始に向けたスケジュール

★３、★4は、運用開始までの想定スケジュールが公表されています。**2027年度以降の本格運用開始に向けて、計画的な準備が必要です。**

■スケジュール（想定事項含む）



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作成

HITACHI

3-4. いま準備しておくべき対策とは？

本制度は、**情報セキュリティの幅広い領域への対応が求められています。受注者側企業に関しては、現時点で自社のセキュリティ対策水準の可視化と、専門家によるアドバイスを受け、制度対応への準備を進めることをお勧めします。**

2025年上期（～9月）

- 制度の理解と自社の影響分析
- 現状のセキュリティ対策状況の把握
- 目標とする評価制度の検討・決定

2025年下期（10～3月）

- 目標評価制度とのギャップ分析と対応計画案の策定
- 予算確保と経営層への説明
- 基礎的な対策の実装開始

2026年 上期（～9月）

- 予備評価の実施
- 是正措置の対応
- 評価申請の準備

2026年 下期（10～3月）

- 正式評価の受領
- 評価持続・改善活動の開始

HITACHI

診断にとどまらない、課題解決に向けた支援

お客さまの現状の対策水準に沿った、各種アセスメントサービスメニューを展開。
豊富な経験を持つ、当社のセキュリティ専門の技術者が対策水準の向上を支援します。

1. サイバーリスクアセスメント

「どこから始めればよいか分からない」、「現在のセキュリティ対策状況を十分に把握できていない」など、セキュリティ対策をこれから始めたいお客さまにマッチしたサービスです。国内のガイドラインを用い、情報資産の棚卸しや、基礎的な診断を行います。また、診断結果を基にしたアドバイザリーサポートを通じてセキュリティ対策水準の向上を支援します。

価格：￥600,000～（税別）

2. 情報セキュリティアセスメント支援サービス

「一定の対策を実施しているが、不安がある」、「現状把握をした上で、優先度の高い製品・サービスを検討したい」など、現状のセキュリティ対策の見直し（棚卸し）や、効果的なセキュリティ投資をご要望のお客さまにマッチしたサービスです。セキュリティの国際規格をベースに日立グループのノウハウを取り入れた診断を行い「どこにリスクが潜んでいるのか」、「本当に優先度の高い対策はなにか」を可視化します。

価格：個別見積

3. ISO/IEC 27001認証取得支援サービス

セキュリティ管理策の具体的な導入事例やそのポイントなどをご紹介することによりセキュリティ管理策のスムーズな展開が可能です。
ISMS*構築に必要な文書の作成を直接支援することで、お客さまのリソースの低減やISMS構築までの期間の短縮、文書の完成度の向上が可能です。

※ISMS：Information Security Management System（情報セキュリティマネジメントシステム）の略称

価格：個別見積

上記で紹介したサービス以外にも、ご要望に応じた多彩なサービスを用意しています。

より詳しいご相談、お問い合わせ

HITACHI

ご相談・お問い合わせ

ご相談・お問い合わせは専用メールアドレス宛にお問い合わせください。
ご不明点やご要望も受け付けております。
お客さまの環境に最適なご提案をいたします。

hsc-contact@mlc.hitachi-solutions.com

株式会社 日立ソリューションズ・クリエイト
代表者:取締役社長　南　章一
社員数: 4,013名（2025年4月1日時点）
所在地:東京都品川区東品川四丁目12番6号
（品川シーサイドキャナルタワー）

■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。

■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・製品の仕様は、2025年10月現在のものです。
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

わくわくをあなたと

想像を超える明日を創造する

当社はITを通じ 安心・快適を提供し、社会とともに持続的に成長します。
確かな技術力と深い知見で、想像を超える価値の創造に挑戦します。
協創を通じて すべての人が充実し、わくわくする明るい未来づくりに貢献します。


HITACHI