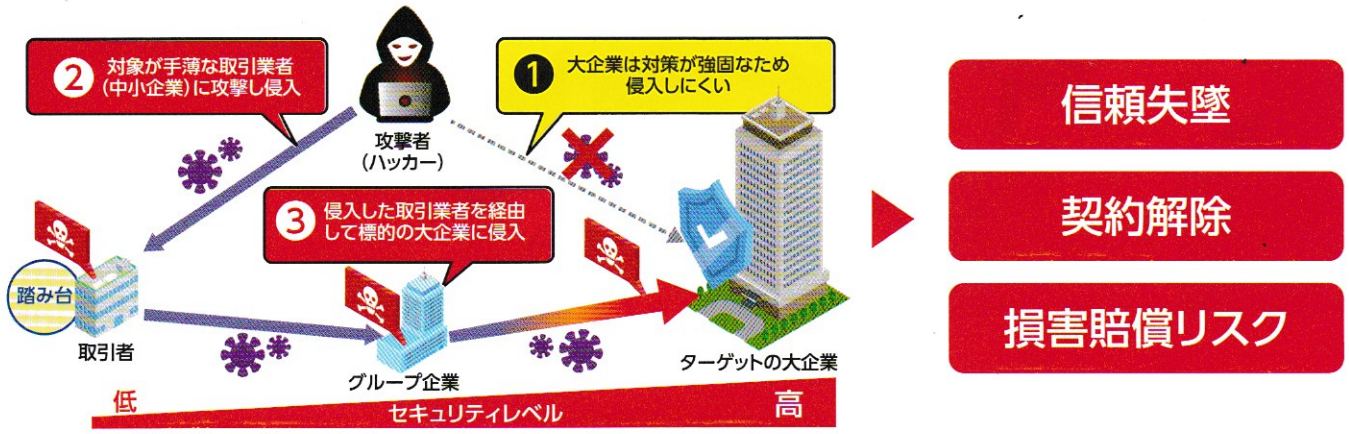
セキュリティ対策評価制度とは

本制度は、企業のサイバーセキュリティ対策状況を★3～★5で可視化する仕組みであり、
今後企業の★取得状況が「既存取引継続」や「新規取引の可否」に影響する可能性がございます。

発注者 → セキュリティ対策状況確認（★取得状況など） → 取引先

IT基盤（オンプレスミス環境、クラウド環境すべて）が対象となります。

大手企業を直接狙うのではなく、取引先である中小企業を踏み台にしたサイバー攻撃の増加..
IT基盤強化は、自社の防御だけではなく、サプライチェーン全体の課題となっています。



評価制度の目的

発注企業への効果
取引先に求める対策水準の決定や、対策状況の把握が容易となる

受注企業への効果
受注者側はセキュリティ対策のレベルを明確に示すことができる

社会全体での効果
サイバー攻撃への備えある企業等への適切な評価が行える

どのように評価される？

IPA SECURITY ACTION		セキュリティ対策評価制度		
★1	★2	★3 ※3	★4 ※3	★5
企業自らが、情報セキュリティ対策に取組むことを自己宣言する	自社による情報セキュリティを診断※2をおこない情報セキュリティ基本方針を策定し、外部に公開する	評価の主体は**有資格者** 有資格者による厳格な審査が想定されます	評価の主体は**評価機関** 技術検証が課せられる可能性があります	
① 「情報セキュリティ5か条」※1に取組む	① 「5分でできる! 情報セキュリティ自社診断」※2を自社評価	① 自社で自己評価結果の記入	① 自社で解答準備	★5に関しては令和8年度以降に対策基準や評価スキームの具体的はあり方などが検討される予定です。
② SECURITY ACTION 自己宣言の申し込み	② 情報セキュリティ基本方針を策定し、外部へ公開	② 有資格者による評価※	② 評価機関による評価の実施	
③ ロゴマーク使用許諾	③ ロゴマーク使用許諾	③ 登録機関に提出／台帳へ登録	③ 技術検証事業者による検証の実施	
			④ 登録機関に提出台帳へ登録	

※1 独立行政法人 情報処理推進機構（IPA）「情報セキュリティ5か条」
https://www.ipa.go.jp/security/sme/f55m8k0000001wb3-att/000055516.pdf

※2 独立行政法人 情報処理推進機構（IPA）「中小企業の情報セキュリティ対策ガイドライン付録の付録3「5分でできる!情報セキュリティ自社診断」
https://www.ipa.go.jp/security/sme/f55m8k0000001waj-att/000055848.pdf

※3 産業サイバーセキュリティ研究会 ワーキンググループ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サブワーキンググループ（第7回）
資料4 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）
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/pdf/007_04_00.pdf

ISMSやPマークとの違い
「ISMS」「Pマーク」とは相互補完的な制度として両輪で発展予定です。
「ISMS」「Pマーク」取得済企業も「セキュリティ対策評価制度」の取得が推奨されます。

NTT西日本