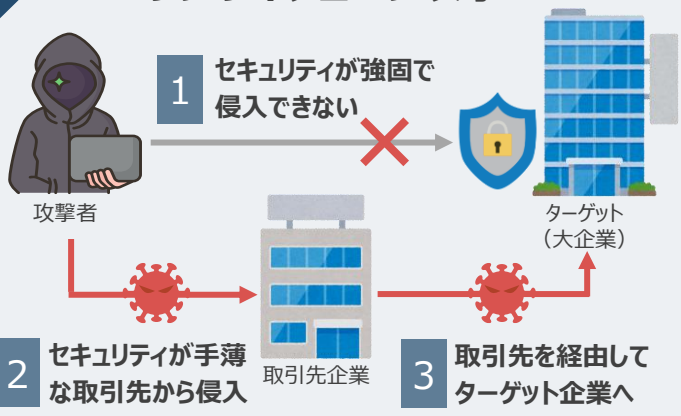
令和8年度末頃 **制度開始予定**

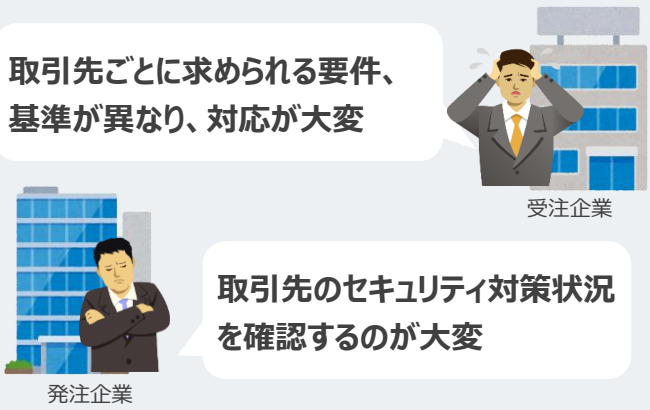
サプライチェーン強化に向けた
セキュリティ対策評価制度

近年、サプライチェーンを狙ったサイバー攻撃が増加し、企業間取引において適切なセキュリティ対策の実施が重要となっています。こうした状況を踏まえ、経済産業省では、サプライチェーン全体のリスク低減とサイバー攻撃に強い体制の構築を目的として、企業のセキュリティ対策状況を可視化する**「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」**の検討を進めています。
本制度は、令和8年（2026年）度末頃の制度開始を予定しています。

01 中小企業を入り口に広がるサプライチェーン攻撃



02 受注企業は取引先ごとに異なる対策基準への対応を迫られ、発注企業は各社の対策状況を把握するのが困難



セキュリティ対策状況を**共通基準で評価する制度**を開始予定

	★1	★2	★3	★4	★5
	SECURITY ACTION		セキュリティ対策評価制度		
概要	情報セキュリティ5か条への取り組み宣言	自社診断＋基本方針策定＆公開	最低限実装すべきセキュリティ対策	標準的に目指すべきセキュリティ対策	重要インフラ事業者関連サプライヤーが満たすべき基準
評価	自己宣言（IPA「SECURITY ACTION」）		専門家確認付き自己評価	第三者認証型	

詳しくは裏面へ

要求事項を支援するサービス例

	★3	★4	要求事項(案)	支援サービス例
ガバナンスの整備	-	1-2-2	サイバー攻撃及び予兆を監視・分析をする体制を整備すること	2 7 8
リスクの特定	3-1-1	3-1-1	ハードウェア、OS及びソフトウェアに関する情報を把握すること	1
	3-1-2	3-1-2	ネットワークの情報に関する一覧を作成すること	1
	-	3-2-1	脆弱性の管理体制、管理プロセスを定め、それに基づく管理を行うこと	2 8
攻撃等の防御	4-1-1	4-1-1	ユーザID の発行・変更・削除の手続を定め、適切に運用すること	5
	4-1-2	4-1-2	管理者IDの発行・変更・削除の手続を定め、適切に運用すること	5
	4-1-3	4-1-3	システム及び情報の重要度に応じて認証の強度及び実装方法を決定すること	5
	-	4-2-1	経営層を含むすべての要員に対して、セキュリティの意識向上のための教育・研修を実施すること	6
	4-2-2	4-2-2	セキュリティインシデント発生時の対応に関する教育・訓練を行うこと	6
	-	4-3-1	情報機器及び情報システムの保管データを適切に暗号化するようルールを定め、周知すること	2
	4-3-4	4-3-4	適切なバックアップを行うこと	4
	4-4-1	4-4-1	ハードウェア、OS及びソフトウェアの安全な構成を確立し、維持すること	1
	-	4-4-2	サポート期限の切れたOS及びソフトウェアの利用停止及び更改を実施すること	1
	-	4-4-3	情報機器及びシステムに関するログを取得し、異常を検知するため、定期的にレビューを行うこと	3 7
	4-4-4	4-4-4	ハードウェア、OS及びソフトウェアへのセキュリティパッチ及びアップデートの適用に係る手続を策定し、実行すること	1
	4-4-5	4-4-5	システムをマルウェア感染から保護すること	2 3
	4-5-1	4-5-1	内外のネットワークを適切に分離し、境界部分を防護すること	3
	-	4-5-2	社内から社外への不正な通信を遮断する対策を実施すること	3
攻撃の検知	5-1-1	5-1-1	ネットワーク上の適切な場所でネットワーク接続及びデータ転送を監視すること	2 3
	-	5-1-2	ハードウェア及びソフトウェアの状態及び挙動を監視すること	1
インシデントからの復旧	7-1-1	7-1-1	事業上重要なシステムについて、事業継続の要件に沿う復旧に必要な準備を行うこと	4

対応サービス例

1 資産管理

端末・OS・ソフトを一元管理し、挙動監視やパッチ管理、サポート期限切れ資産への対応により、不正を検知し情報漏えいを防止
【取扱商品】
SS1、ISM Cloudone、SKYSEA

2 ウイルス対策ソフト・EDR

端末に対するマルウェア対策と侵入後の監視により脅威を検知・防御し、被害拡大を防止。脆弱性管理機能オプションも提供。
【取扱商品】
ESETセキュリティソリューション

3 UTM・SASE

社内外のネットワーク通信を一元管理し、制御・分離・可視化およびログ取得を通じて脅威を防御し、安全なアクセス環境を実現
【取扱商品】
HOME、FortiGate、CatoSASE

4 バックアップ

重要なデータを定期的にバックアップし、障害やサイバー攻撃発生時に復旧を可能とすることで、情報資産保護と業務継続性を確保
【取扱商品】
Barracuda Backup

5 認証

ID管理と多要素認証によりアカウントを統合管理し、ユーザIDおよび管理者IDを適切に管理し、重要度に応じた認証強化を実現
【取扱商品】
ID Entrance

6 セキュリティ教育

従業員の情報セキュリティ意識およびリテラシーを向上させ、インシデントの未然防止と発生時の対応力の向上を図る
【取扱商品】
セキュリティ教育、メール訓練

7 ログ管理

複数のシステムのログを収集・分析し、不審な行動を迅速に検知。不正行為の予兆を早期に発見し、即座に対応
【取扱商品】
Alog

8 脆弱性関連サービス

サーバー、NW機器に存在する脆弱性を発見する調査、お客様環境に合致した脆弱性情報を提供
【取扱商品】
脆弱性診断サービス、脆弱性情報提供サービス

本チラシに記載の内容は、2026年1月時点の「★3・★4要求事項案および評価基準案」に基づいて作成したものです。
今後の方針や内容の確定に伴い、記載事項が変更となる可能性があります。あらかじめご了承ください。

セキュリティソリューション ホームページ
canon.jp/it-sec

サービス提供元：キヤノンITソリューションズ株式会社

●お求めは信用のある当社で

2026年1月現在

Canon キヤノンマーケティングジャパン株式会社
〒108-8011 東京都港区港南 2-16-6 CANON S TOWER