未来を、ひろげる。
HIROGIN HOLDINGS

経済産業Report

2026年8月25日
Vol.17

高まるサプライチェーンの情報セキュリティリスク
～重要度増す中小企業のセキュリティ対策～

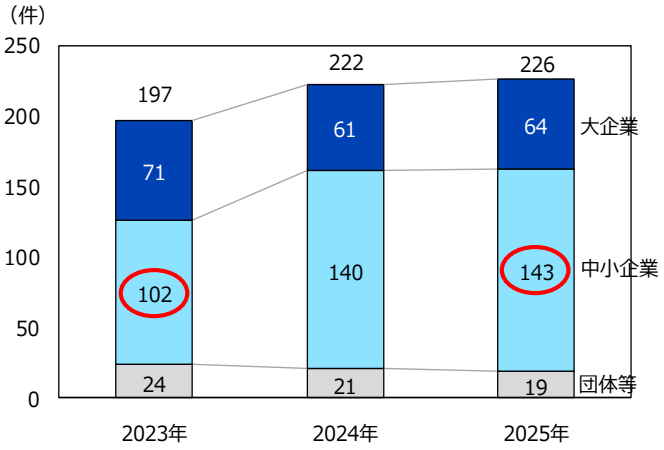
深刻化するサイバー攻撃被害

近年、企業に対するサイバー攻撃が頻発化する中で、顧客情報・機密情報等の流出や製品・サービスの供給停止など、事業活動への影響が深刻化しています。

最近では、サイバー攻撃被害は大手企業にとどまらず、中小企業の被害が大きく増加しています。警察庁によれば、2025年のランサムウェア被害の報告件数は226件（23年比＋29件）で、うち中小企業の被害は143件（同＋41件）と全体の増加幅を上回っています**（図表1）**。

このことは、取引先や委託先等を経由した情報セキュリティリスクが一段と高まっている状況を示しており、自社のみならずサプライチェーン全体での対策の強化が急務となっています。

図表1　ランサムウェア（注）被害報告件数の推移



（注）企業や組織の情報資産を暗号化等により利用不能な状態にし、復旧のための対価として身代金を要求する悪意のあるソフトウェア
（資料）警察庁資料よりひろぎんHD経済産業調査部作成

信頼構築に必要となるセキュリティ水準の向上

こうした中で、経済産業省は「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（SCS評価制度）」を2026年度末を目途に開始することとしています。この制度は、「求められるサイバーセキュリティ対策の水準を定めて企業の対応状況を可視化」するもので、取引先ごとに異なっていたセキュリティ対策の要求内容を標準化することで、中小企業を中心とした対応負担の低減とサプライチェーン全体でのセキュリティ水準の向上を図ることを目的としています**（図表2）**。

経済産業省では現在、対策にかかるガイドラインの整備のほか、低コストで導入可能なサービスメニューの創設や専門家とのマッチングなど、中小企業への普及施策の検討を進めています。中小企業においてはこうした制度を活用してセキュリティ水準の向上に着実に取り組み、発注元企業との信頼関係をより強固にしていくことが求められます。

図表2　SCS（Supply Chain Security）評価制度の概要

評価水準（注）	★3	2026年度末開始予定 ★4	★5（検討中）
想定される脅威	一般的なサイバー攻撃 （脆弱性等を悪用）	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	高度なサイバー攻撃 （未知の攻撃含む）
対策レベル	**全てのサプライチェーン企業が** **最低限実装すべき対策** （基礎的な組織的対策、システム防御策等）	**サプライチェーン企業等が** **標準的に目指すべき対策** （組織ガバナンス・取引先管理、 インシデント対応等の包括的対策）	**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**
評価スキーム	専門家確認付き自己評価	第三者評価	第三者評価
有効期間	1年	3年（自己評価結果を毎年提出）	今後検討

（注）SCS評価制度は、情報処理推進機構（IPA）が運営する自己宣言制度「SECURITY ACTION」（★1・★2）につながる形で設計されている
（資料）経済産業省資料よりひろぎんHD経済産業調査部作成

品質向上のため
アンケートにご協力ください。
PCの方は
コチラを
クリック
※ ナインアウト株式会社が提供するアンケートサイトへ遷移します。

◆ 本件に関するご照会は、ひろぎんHD経済産業調査部　担当：古谷（℡082-247-4958）までお願いします。