中小企業のセキュリティ対策

対策状況の可視化へ

（独立行政法人情報処理推進機構・江島将和）

評価制度の構築方針案公表

経済産業省および内閣官房国家サイバー統括室は、サプライチェーンにおける重要性を踏まえた上で満たすべき各企業のセキュリティ対策を提示しつつ、その対策状況を可視化する仕組みの構築に向けた検討の結果として、2025年12月、「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）」を公表し、意見公募を開始した。

本制度では、サプライチェーンにおけるリスクを対象にした上で、各企業の立ち位置に応じて必要なセキュリティ対策を提示するため、複数のセキュリティ対策の段階（★）を設けている。こうした段階を設けることにより、特に、限られたリソースの中で自社のリスクを踏まえてセキュリティ対策を行うことが困難な中小企業を中心に、サプライチェーンに属する全ての企業が、容易かつ適切に必要なセキュリティ対策を決定できるようになることが期待される。

本制度の活用促進を通じて、取引先へのサイバー攻撃を起因とした不正侵入などのリスクや製品・サービスの提供が途絶えるリスクの軽減を図り、サプライチェーン全体のセキュリティ対策水準を向上させることが、本制度の目的である。

三つの段階を設け発注元が提示

具体的には、２社間の取引契約などにおいて、発注元企業は委託先企業に適切な段階（★）を提示し、委託先企業は示された対策を実施して発注元企業に実施状況を示すことを想定している。

本制度では、以下の三つのセキュリティ対策の段階を設けることを予定している。

★3

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として、基礎的なシステム防御策と体制整備を中心に実施する段階（セキュリティ専門家による自己評価結果の確認を実施）

★4

サプライチェーン企業などが標準的に目指すべきセキュリティ対策として、組織ガバナンス・取引先管理、システム防御・検知およびインシデント対応など包括的な対策を実施する段階（第三者評価を実施）

★5

サプライチェーン企業などが到達点として目指すべき対策として、国際規格などにおけるリスクベースの考え方に基づき、自組織に必要な改善プロセスを整備した上で、システムに対しては現時点でのベストプラクティスに基づく対策を実施する段階（第三者評価を実施）

構築する評価制度（案）において設けるセキュリティ対策の段階

成熟度の定義	★3	★4	★5（検討中）
想定される脅威	・広く認知された脆弱性など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： ・基礎的な技術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目指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目指すべき対策： ・国際規格などにおけるリスクベースの考え方に基づき、自組織に必要な改善プロセスを整備した上で、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	第三者評価	第三者評価

26年度末に開始　広く活用を期待

３段階の水準のうち、★３および★４について、26年度末の制度開始を目指し、制度運営基盤の整備や制度の導入促進などを進めていく。

また、★５については、26年度以降、対策基準や評価スキームの具体化の検討を進めていく。

本制度の検討段階において、関心を示す業界団体は多く、広く活用されることが想定される。

制度開始までの対応として、制度構築方針（案）と併せて公表された「別添★３・★４要求事項案及び評価基準案」を参考にして、自社の対策状況とのギャップ把握や対策実施を検討することをお勧めしたい。

（会議所ニュース１月21日号（日本商工会議所発行）より転載）

「制度構築方針（案）」については
こちらを参照