発表日：2026 年 11 月 11 日

報道関係各位

伊藤忠テクノソリューションズ株式会社

攻撃経路に沿ってセキュリティ対策を評価するアセスメントサービスの提供を開始

対策の不足箇所と優先課題を整理し、改善計画の検討を支援

伊藤忠テクノソリューションズ株式会社（代表取締役社長：新宮　達史、本社：東京都港区、略称：CTC）は、独自に開発した「CTC アタックパス クイックアセスメント」の提供を開始します。攻撃者の侵入から事業に被害が及ぶまでの経路（アタックパス）に沿って、企業のセキュリティ対策を評価し、不足箇所と優先課題を整理するサービスです。評価結果をもとに、対策の選定から実装までを一貫して支援します。相次ぐ情報漏洩の事案を受けて取引先を含めた対策が急がれる中、ランサムウェア対策、AI 利用ルールの整備を進める企業に展開します。

情報処理推進機構（IPA）が公表した「情報セキュリティ 10 大脅威 2026」※1 では、「ランサム攻撃による被害」「サプライチェーンや委託先を狙った攻撃」「AI の利用をめぐるサイバーリスク」が組織向けの上位 3 項目を占め、AI のリスクが初めて選ばれました。2026 年 9 月以降、取引先を経由したとみられるサイバー攻撃が続き、企業は取引先や委託先を含めた対策状況の把握が求められています。限られた予算や人員で対策を進めるには、現状を把握し、優先課題を明確にすることが重要です。

本サービスは、ランサムウェア、サプライチェーン攻撃、AI 利活用の 3 領域を評価します。利用企業は、証跡などの資料を事前に用意することなく、CTC が提供する設問一覧で対策状況を回答します。

11 年連続で 10 大脅威に選ばれているランサムウェアについては、侵入から事業停止までの段階ごとに強化すべき箇所を特定します。サプライチェーン攻撃では、取引先や委託先を経由した侵入への対策を、契約上のセキュリティ要件や認証管理などに関する設問で確認します。AI 利活用では、シャドー AI 対策や入力できる情報の基準などの利用ルールを評価します。

設問は「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）」※2 の「★3」の評価基準と照合しており、回答内容をもとに、同制度への準備状況を参考情報として確認できます。

報告書には、経営層向けの重点課題と優先して取り組む方針、担当者向けの判定根拠をまとめ、不足している項目ごとに推奨する対策と参考となるソリューションも示します。社内説明や予算化の検討に活用できます。

CTC は、NIST のフレームワークや CIS Controls といった公的なセキュリティ対策の枠組みを参照し、評価方法と設問を独自に設計しました。利用企業向けの説明会から、結果を説明する報告会までの期間は約 1 か月です。評価結果に応じて RFP（提案依頼書）の作成を支援し、製品導入の機能要件や判定根拠などを調達要件として整理したうえで、実装に向けた検討につなげます。

今後も CTC は、巧妙化するサイバー攻撃に対応するセキュリティサービスやソリューションを拡充し、企業が安心して事業を継続できる環境づくりに貢献します。

■CTC アタックパス クイックアセスメント サービスイメージ



■CTC アタックパス クイックアセスメント 紹介資料
https://www.ctc-g.co.jp/keys/download/attack-path-quick-assessment

※1 出典：独立行政法人情報処理推進機構（IPA）「情報セキュリティ 10 大脅威 2026」［組織］
https://www.ipa.go.jp/security/10threats/10threats2026.html

※2 SCS 評価制度：経済産業省と内閣官房国家サイバー統括室が制度構築方針を定め、IPA が運営する制度です。企業のセキュリティ対策の状況を★の段階で評価し、見える化します。★3 は基礎的な対策の水準で、専門家の確認を受けた自己評価で取得します。本サービスは、同制度の評価の取得を保証するものではありません。
https://www.ipa.go.jp/security/scs/details.html

※ 記載されている商品名などの固有名詞は、各社の商標または登録商標です。

※ 掲載されている情報は、発表日現在の情報です。最新の情報と異なる場合がありますのでご了承ください。

以上

＜報道機関からのお問い合わせ先＞
伊藤忠テクノソリューションズ株式会社
広報部
E-mail：press@ctc-g.co.jp