PRESS RELEASE

2026 年 5 月 12 日

サイバー攻撃による被害の発生リスクを低減する

「TOiNX-SOC　-未然防止に特化した統合セキュリティ監視-」提供開始について

株式会社トインクス

株式会社トインクス（本社：宮城県仙台市青葉区、取締役社長：河田　伸、以下　トインクス）は、企業のサイバーセキュリティ強化を支援するため、セキュリティ監視等サービス「TOiNX-SOC　-未然防止に特化した統合セキュリティ監視-」（以下、「TOiNX-SOC」）の提供を開始いたしました。

本サービスでは、お客さまの IT 環境やニーズに応じたセキュリティ監視の設計・構築を柔軟に行うとともに、サイバー攻撃の未然防止にフォーカスした各種サービスを提供いたします。非常に高い品質が求められる東北電力企業グループの IT 業務を行ってきた当社の実績を生かし、あらゆる業種のお客さまのサイバーセキュリティ強化を支援いたします。

■サービスの特長

▶東北電力企業グループのサイバーセキュリティを担うスタッフが、24 時間 365 日監視

サイバー攻撃の発生が許されない重要インフラを運営する東北電力企業グループのセキュリティを担ってきた専門スタッフが、24 時間 365 日体制でお客さまの IT 環境を監視します。

▶脆弱性分析やサイバー攻撃準備行為の検知

サイバー攻撃の侵入経路となることが非常に多い脆弱性について、お客さまの IT 資産に対する分析および報告を行い、リスク低減に貢献いたします。また、EDR[1]や IPS[2]等の監視に加え、ランサムウェア等が被害を与える前の侵入・偵察等の準備行為を検知する仕組みを構築し、監視することも可能です。これにより攻撃が成立する前の対処が可能となります。

▶報告会の開催と継続的な改善活動

打合せ形式による月次報告が可能です。報告だけではなく、お客さまとの対話によるご要望のヒアリングや改善提案を行うことで、継続的にお客さまのセキュリティ強化をご支援します。

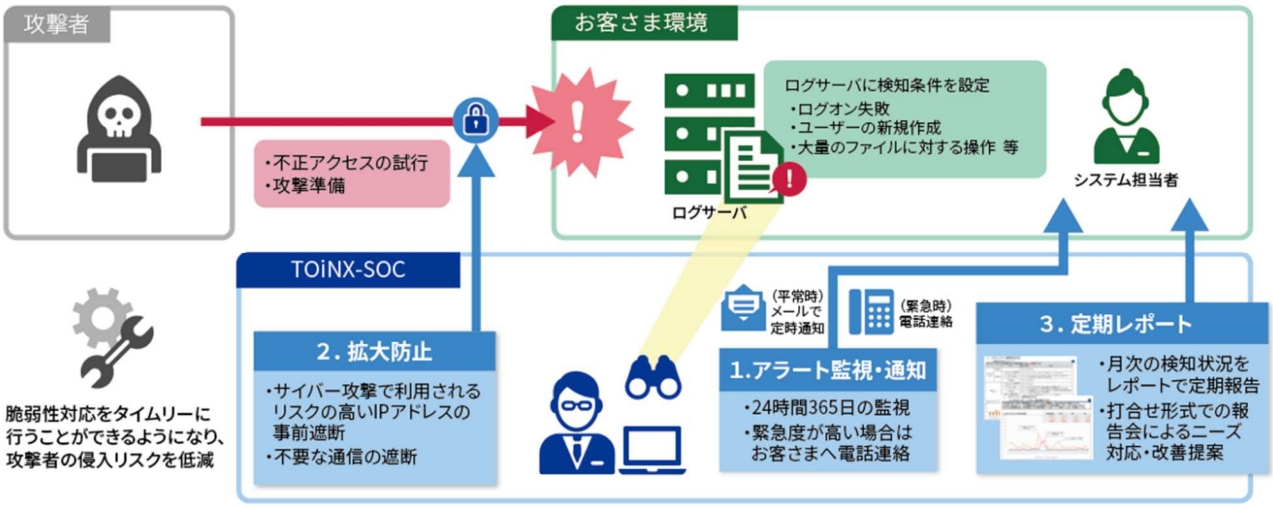
---

[1] Endpoint Detection and Response の略。PC やサーバ等の端末（エンドポイント）を常時監視し、サイバー攻撃の侵入を前提としてその検知と対応を行うセキュリティ対策。

[2] Intrusion Prevention System の略。ネットワークの通信を監視し、不正アクセスや攻撃の兆候を検知・自動遮断するセキュリティツール。

PRESS RELEASE

▼ご利用イメージ



■サービス提供の背景

近年、国内企業におけるサイバー攻撃の被害が激甚化しております。特にランサムウェアについては、業務停止・影響が長期化する特性から、大企業に対しても深刻な被害を与えており、IPA（情報処理推進機構）が公表する「情報セキュリティ 10 大脅威」にて 2021 年以降連続で 1 位となっています。このようなサイバー攻撃では、復旧が困難になるよう攻撃前に事前準備を終えるため、未然防止の重要性がますます高まってきております。

こうした社会の課題に対応するため、当社がこれまで行ってきた東北電力企業グループの IT セキュリティ業務で培ったノウハウを生かし、サイバー攻撃の未然防止に特化した「TOiNX-SOC」サービスをリリースいたしました。

■導入効果

以下のような導入効果により、サイバー攻撃の発生リスクを低減し、お客さま企業の業務停止やネガティブコスト発生リスクの低減、社会的信頼の維持等に貢献いたします。

・24 時間 365 日のセキュリティ監視による、インシデントの早期発見と即時対応
・脆弱性分析による、迅速かつ的確な脆弱性対応と攻撃者の侵入リスク低減
・サイバー攻撃の準備行為検知による、セキュリティ被害の未然対応
・インターネット経由の不正アクセス遮断による、社内 IT 環境への侵入リスク低減
・報告会で改善提案を通じた、顧客ニーズや最新セキュリティトレンドの継続的な反映

トインクスは、本サービスを通じてお客さまのサイバーセキュリティ強化の取り組みを支援し、幅広い業界におけるサイバー攻撃の未然防止に貢献してまいります。

【本件に関するお問い合わせ先】

株式会社トインクス　営業本部　営業部
問い合わせフォーム：https://service.toinx.co.jp/contact/ct-toinx-soc/
TEL：022-214-3032　　トインクス サービス情報サイト：https://service.toinx.co.jp/