

能動型SOC構築支援サービス

「人・プロセス・テクノロジー」の統合による
持続可能なサイバーセキュリティ運用の実現

SOCの定義と主要な役割

24/365 継続的監視

組織のネットワーク、エンドポイント、クラウド環境を常時監視し、サイバー攻撃の兆候をリアルタイムで検知します。死角のない防御体制を構築します。

迅速な初期対応

検知されたアラートの「トリージ（優先順位付け）」を行い、重大な脅威に対して即座に封じ込めや調査を開始。被害の最小化を図ります。

SOCを支える3つの重要要素



People (人)

熟練したアナリストによる正確な判断と、インシデントへの深い洞察力がSOCの質を決定します。



Process (プロセス)

「プレイブック」に基づく標準化された手順。誰が、いつ、何をすべきかを明確に定義します。



Technology (技術)

SIEM, EDR, SOARなどの最新ツールを駆使し、自動化と相関分析による高度な検知を実現します。

構築の5フェーズ

01 戦略策定

守るべき資産の特定
組織モデルの選択
目標設定(KPI)

02 技術選定

SIEM/EDR等の
インフラ構築

03 運用設計

手順書(プレイブック)の
作成

04 体制構築

3つ階層(Tier)
・アナリスト
・レスポnder
・ハンター/エンジニア
SOCマネージャーの採用
教育研修

05 運用開始

24/365監視の開始と
継続改善