

ICT-24セキュリティオペレーションサービス (ICT-24SOC)

セキュリティインシデントの早期検知から早期収束まで、専門のアナリストにお任せください！



インターネット
(VPN)



御社内ネットワーク

ログ分析

SIEM

NWセキュリティデバイス

ファイアウォール

IDS/IPS

エンドポイント

マルウェア

WAF

プロキシ

ログ管理

DDoS

サンドボックス

ID管理

メールフィルタ

パケットキャプチャー

サーバー

こんな
課題に

サイバー攻撃の予兆やインシデントの発生をいち早く検知し、事態の早期収束に向けて迅速に対応したい。

▶ 対応可能なセキュリティデバイスの種類が豊富

世の中で利用されている様々なセキュリティ製品をマルチベンダで幅広く対応しています。

▶ 重大なアラートに絞ったお知らせを実施

セキュリティデバイスのログをアナリストが分析し、過検知を排除して重大なアラートのみをお知らせすることで、お客様の運用負担を軽減します。

▶ SOCに加え、NOCやインシデント発生時の初動対応のCSIRT支援まで、ワンストップで提供可能

セキュリティアラートのイベント通知やレポート提供などのSOC業務(セキュリティオペレーションセンター業務)に加え、機器の稼働監視やパフォーマンス監視、保守業務などのNOC業務(ネットワークオペレーション業務)、さらにインシデント発生時にお客様CSIRT組織※を支援するための初動対応支援まで、ワンストップでご提供します。

価格

価格応相談

※お客様の構成にあわせて、監視構成をご提案し、お見積もりさせていただきます。

※CSIRT(Computer Security Incident Response Team、シーサート):コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデントの報告にもとづき、対応方針や手順の策定・対応指揮をします。

詳細・お問合せ

<https://www.ntt-at.co.jp/product/ict24soc/>

対象業界: 全ての業界

提供形態: 運用

