企業向けサイバーセキュリティソリューション

McAfee SIEMマネージドサービス

「SIEMの運用は難しい・・・」

という不安がある御社に朗報です。

お客様の環境に合わせた相関ルールの適用とリアルタイム分析を提供するICT-24 SOCサービス

昨今のサイバー攻撃は高度化する一方で、対策に“絶対”はありません。企業の信頼を守るためには最新の防御体制が必須ですが、100%防ぐことは不可能です。 そのような現状において、お客様がご利用のセキュリティ機器のログを一元管理し、リアルタイムに相関分析を行うことで不正侵入の兆候を早期に検知し、セキュリティアナリストの分析を加えた対応策を提示します。

POINT 1
SIEMの運用経験豊富な ICT-24SOCによる提供

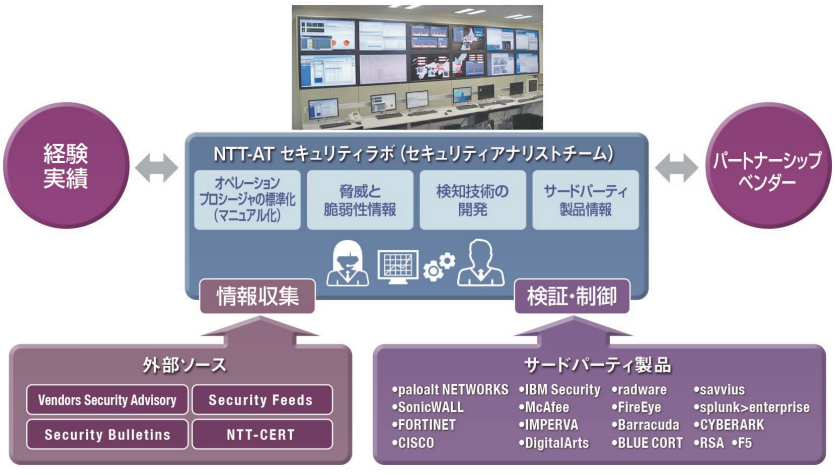
POINT 2
相関分析の対象となる監視 対象デバイスの種類が豊富

POINT 3
インシデント発生時の CSIRT支援も対応可能

※オプション

高度なセキュリティ分析が実施可能な セキュリティラボを完備(ICT-24 SOC)

ICT-24 SOCでは、NTTグループならではの豊富な外部ソースからの脅威情報収集や、検出技術の開発が可能なセキュリティエンジニアリング、およびインシデント対応支援も可能なセキュリティアナリストを保有した高度なセキュリティラボを完備し、最新の相関ルールやウォッチリストを迅速にご提供します。

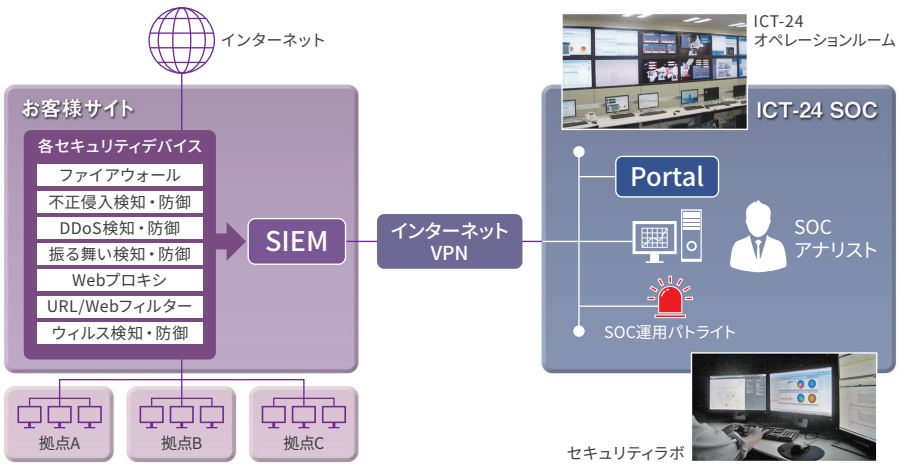


セキュリティ Security

http://www.ntt-at.co.jp/product/mcafee-siem-soc/

サービス環境と体制

お客様サイトと弊社のICT-24 SOC間をIP-VPN接続で結び、遠隔監視によって各種の高度なセキュリティ対策関連サービスをご提供します。



サービス内容／監視対象機器

平常時のデバイスのメンテナンスからセキュリティインシデント発生時などのイベントハンドリング、イベント後のアナリティクスなど多岐に渡っており、全方位的かつ深いエリアまで包括的なサービス構成となっています。

サービス項目		詳　細
専用ポータルの提供		ICT-24 SOC 専用ポータルにおいて、お知らせ、問い合わせ、レポート、FAQ等を提供
SIEMデバイスメンテナンス	コンテンツアップデート	最新コンテンツ（パーサー／相関ルール／ウォッチリスト等）への更新を実施
	ソフトウェアアップデート	ソフトウエアの更新判断、および実施
	ルール等のチューニング	パーサー、相関ルール、ウォッチリストを最適化
	正常稼働監視	SIEMデバイスの正常稼働を監視、切り分け、原因調査、オンサイト保守手配を実施
	設定バックアップ	オペレーション実施時該当の設定をバックアップ
	ライセンス更新	ライセンス等の保守更新の代行を実施
イベントハンドリング	リアルタイム監視・通知	重要なセキュリティインシデントを発見した場合、即座に通知
	問い合わせ対応	ICT-24 SOC 専用ポータル経由で問い合わせ対応
アナリティクス	イベント追跡・提供	お客様からの依頼に基づいてイベント追跡を実施し、詳細情報を提供
	定期イベント分析・改善	定期的（月次）のイベント分析による改善
	レポート提供	ICT-24 SOC 専用ポータル経由で月次レポートを提供

対応している監視対象機器の一覧です。お客様のニーズに合わせてマルチベンダーで幅広く対応しており、対象ラインナップは随時更新しています。

分　類		メーカー
ネットワークセキュリティ監視	ファイアウォール	Fortinet、Paloalto、SonicWall
	IDS/IPS	IBM Security、Cisco、McAfee
	WAF	F5、Imperva
	Proxy（Webフィルタ）	BlueCoat、DigitalArts、TrendMicro
	DDoS	Radware
	サンドボックス	Fortinet、FireEye
	メールフィルター	Barracuda、DigitalArts、TrendMicro
	パケットキャプチャ	Savvius
エンドポイントセキュリティ監視	マルウェア	Yarai
	ログ管理	SML
サーバー監視	ID管理	CyberARK

価格：・初期導入費用：4,400,000円～ ／一式　・マネージドサービス費用：980,000円～ ／月（最低契約期間は1年。次年度以降も年単位契約。）

オプションサービス／インシデント対応支援

現地駆け付け支援サービス

インシデント発生直後に専門スタッフが現地に駆け付け、ログ分析・データ保全・簡易フォレンジック等を迅速に実施し、証拠の保全と二次被害を防止します。

デジタルフォレンジック解析サービス

インシデント発生後、該当するHDD等をフォレンジック専用の解析装置で保全・分析し、インシデント発生時の技術的詳細を明らかにします。

お問い合わせ　http://www.ntt-at.co.jp/product/mcafee-siem-soc/

NTTアドバンステクノロジ株式会社　セキュリティ事業本部 マネージドサービスビジネスユニット
〒220-0012 神奈川県横浜市西区みなとみらい3-6-3 MMパークビル