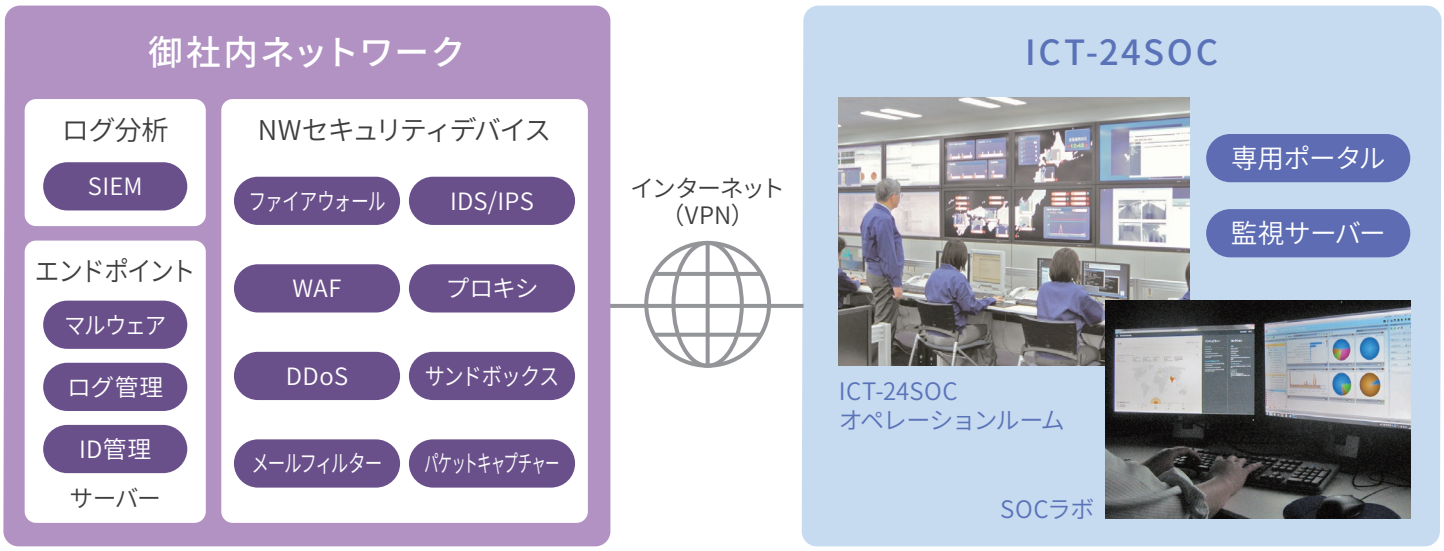
企業向けサイバーセキュリティソリューション

ICT-24SOC（セキュリティオペレーションサービス）

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。



不正アクセス/標的型攻撃に対する企業向けSOCサービス

昨今、多くの企業で不正侵入防御システム（IPS）やWebアプリケーションファイアウォール（WAF）、標的型攻撃対策システムといったセキュリティ対策製品を導入し、サイバー攻撃を回避する努力を行なっています。ですが、日々発見される新たな攻撃手法や脆弱性の悪用は絶えることがなく、単に対策機器を導入しただけでは守りきれない時代になって来ています。

そのような状況の中でもっとも重要なのは、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することです。NTT-ATのICT-24SOCは、そのような課題をお持ちのお客様に最適な取り組みをご提供します。

POINT 1
対応可能なセキュリティデバイスの種類が豊富

ファイアウォール、IPS、Sandbox等のインターネット環境向けおよび、マルウェア防御などのエンドポイント環境向けセキュリティデバイスまで、幅広い製品に対応可能です。

POINT 2
重大なアラートに絞った通知を実施

お客様のセキュリティ機器からのログを専門のアナリストが分析し、誤検知を排除した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。

POINT 3
NOC／SOC／CSIRTをワンストップで提供可能

機器監視等のNOC、セキュリティアラート通知やレポート提供等のSOC、さらにインシデント発生時にお客様CSIRT組織をサポートする初動対応支援やフォレンジック解析まで、ワンストップでご提供します。

セキュリティ Security

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

対応デバイス

● 豊富な対応セキュリティデバイス。今後もさらに増える予定です。

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, IntelSecurity
	WAF	F5, Imperva
	Proxy(Webフィルター)	BlueCoat, DigitalArts, TrendMicro
	DDoS	Radware
	サンドボックス	Fortinet, FireEye
	メールフィルター	Baracuda, DigitalArts, TrendMicro
	パケットキャプチャー	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
ログ分析	SIEM	IntelSecurity, RSA, Logstorage

サービスメニュー

● お客様の環境やニーズに最適なメニューをご提供します。

機器メンテナンス	コンテンツアップデート	最新ルール(セキュリティデバイスシグネチャ、パーサ/相関分析ルール等)の更新
	設定等チューニング	検知イベントやパケットを監視して検知・防御を最適化
	ソフトウェアアップデート	ソフトウェアの更新(安定バージョンを推奨で提供)
	正常稼働監視	機器の正常稼働を監視、切り分け、原因調査※
	イベント保全	Syslogサーバーへの自動転送による保全(期間は要相談)
	設定バックアップ	設定変更時はすべてバックアップし、故障時の復旧時間を短縮
	ライセンス更新	ライセンスの更新代行
イベントハンドリング	アラーム分析・通知	未知の攻撃や不審な通信を分析し、インシデントの可能性がある場合はメール通知
	設定変更	アラーム分析からのフィードバックによる設定変更
	問い合わせ対応	お客様からの申告に基づき、オペレーターが対応
アナリティクス	レポート提供	イベント傾向分析、および影響度分析結果を提示(月次。報告会は応相談)
	脆弱性検査(オプション)	定期的な公開系サーバーへの脆弱性検査を実施
	セキュリティ情報提供	対象ソフトウェアの重大な脆弱性情報を提供
インシデントレスポンス(オプション)	初動対応	インシデント発生時、または外部組織・団体等からの指摘に基づくリモート調査
	駆け付け対応	インシデント発生時、または外部組織・団体等からの指摘に基づく現地調査
	デジタルフォレンジック	ホストのデジタルフォレンジック調査

※機器交換はオンサイト保守契約に限る。

関連サービス

SIEM構築／運用支援サービス

・導入支援（監視方針の策定、イベント分析、相関分析ルール作成等）
・運用支援（チューニング、技術アドバイス、研修等）等

FortiGateSOCサービス

・専門技術者が選別した重要性の高いアラートのみをお知らせ
・影響度が分析されたレポートやインシデント対応支援 等

お問い合わせ **https://www.ntt-at.co.jp/product/ict24soc/**

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