

2023年7月12日

NTT アドバンステクノロジー株式会社

「FortiGate SOC サービス プラス OT オプション」を提供開始 ～IT 機器だけでなく、OT 機器のセキュリティもまとめて見守ります！～

NTT アドバンステクノロジー株式会社(以下:NTT-AT、本社:東京都新宿区、代表取締役社長:伊東 匡)は、インターネットと社内ネットワークの境界でのセキュリティ監視に加えて、各種 OT 機器の通信もまとめて監視する「FortiGate SOC サービス プラス OT オプション」(以下:本サービス)の提供を開始します。

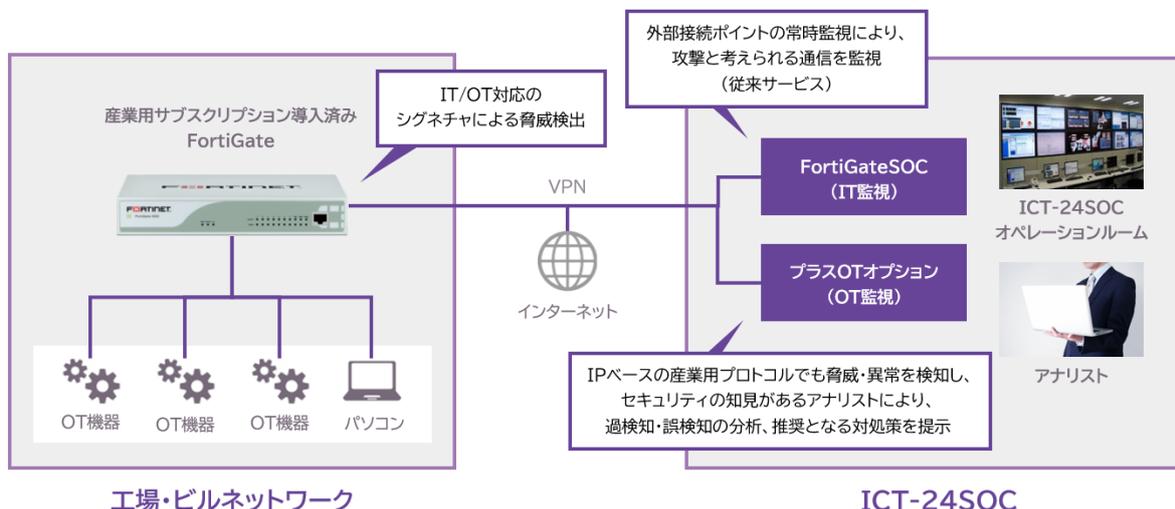
NTT-AT は、現在、米フォーティネット社が開発した次世代ファイアウォール(NGFW)/統合脅威管理(UTM:Unified Threat Management)アプライアンス製品である FortiGate を導入されたお客様に対し、ICT-24 セキュリティオペレーションセンター(ICT-24SOC)が FortiGate を監視することで、インシデントの早期発見をサポートする「FortiGate SOC サービス」を提供しています。

今回、本サービスを「FortiGate SOC サービス」のラインナップに加えることにより、社内ネットワークのパソコンなどの IT 機器のみならず工場のネットワークに IP プロトコルベースで接続した OT 機器も ICT-24SOC がまとめて監視し、お客様の環境を 24 時間 365 日セキュアに見守ります。

1. 提供開始の背景

OT(オペレーショナルテクノロジー)と IT(情報テクノロジー)の統合は、製造分野のサイバーセキュリティに大きな影響を及ぼしています。これまで、ICS(産業用制御システム)や SCADA(監視制御・データ収集システム)と IT システムのネットワークは、物理的に接続されていないなどギャップが存在していました。しかし、今では、このギャップは取り払われ、IT システムや、ひいてはインターネットと接続されるようになっていきます。このため、これらのシステムは拡大する脅威にさらされ、テロ行為・サイバー戦争・スパイ活動に関与するハッカーの標的とされるようになりました*1。

このようなお客様の課題を解決するため、従来の FortiGate を使用したインターネットと社内ネットワークの境界における内外の通信監視に加えて、産業用サブスクリプション(FortiGuard Industrial Security Service)を導入した FortiGate により、IP プロトコルベースで IT 機器と OT 機器が混在したネットワーク上の脅威となる通信も監視する本サービスを提供します。



【サービス提供イメージ】

2.「FortiGate SOC サービス プラス OT オプション」について

サイバーセキュリティの脅威に対して、工場・ビルなどを運営する事業者様に安心して事業を運営していただくため、工場・ビル内の OT 向けに産業用サブスクリプションを導入した FortiGate を 24 時間 365 日で監視するとともに、NTT-AT の「工場・ビル向け OT/IoT セキュリティサービス」*2 で提供される可視化の内容を定期的に確認します。

本サービスは、工場のセキュリティ担当者などで、以下の悩みをお持ちのお客様に最適です。

- ・工場に接続した OT 機器とパソコンなどの IT 機器の両方について、攻撃がないかを監視したい。
- ・OT 向けに産業用サブスクリプションを導入した FortiGate を導入したが、過検知・誤検知なのか、実際にサイバー攻撃を受けているかわからない。

■主なサービス

(1)OT 系ネットワークの脅威検知

FortiGate の機能である OT 向けの産業用サブスクリプションのシグネチャを利用して、IP ベースの産業用プロトコルでも脅威・異常を検知し、セキュリティの知見があるアナリストにより、過検知・誤検知の分析、推奨となる対処策の提示などを行います。

(2)外部接続の監視

従来から「FortiGate SOC サービス」にて提供している外部接続ポイントの常時監視により、ランサムウェアなどのマルウェアに感染した端末から悪意のあるサイトへの通信など、攻撃と考えられる通信の監視が可能です。

■サービスメニュー

OT 向けの産業用サブスクリプションを導入した FortiGate に対して、以下のサービスを提供します。また、お客様の要件に応じて必要なメニューを取捨選択することも可能です。

大項目	中項目	内容
1.機器メンテナンス	1.1 コンテンツアップデート	最新シグネチャへの定期的な更新確認
	1.2 設定等チューニング	検知イベントを観測し、検知・防御を最適化
	1.3 正常稼働監視	機器の正常稼働を監視
	1.4 イベント保全	Syslog サーバーへの自動転送による保全
	1.5 設定バックアップ	設定変更時は一世代前までバックアップ
	1.6 ポリシー設定変更	ユーザーからのリクエストを受けて実施(チケット制)
2.イベントハンドリング	2.1 アラーム分析・通知	防御していない攻撃、不審な通信を分析し、インシデントの可能性がある場合、お客様へメール通知
	2.2 設定変更	定期アラーム分析からのフィードバックによる設定変更
	2.3 問い合わせ対応	お客様からの申告等に基づき、オペレーターが対応
3.アナリティクス	3.1 レポート	月次で傾向分析・接続機器を提示
	3.2 インシデント初動対応	リモートで FortiGate のログ分析で対応できる範囲で、インシデント初動対応を支援

3. 提供開始について

2023年7月14日(予定)

4. 提供価格について

サービスの仕様・価格は構成内容により変更になる場合があります。詳細につきましては、下記にお問い合わせをさせていただきます。

お問い合わせ先:<https://www.ntt-at.co.jp/product/fortigate-soc/ot.html>

5. 今後の展望

NTT-ATは、本サービスを提供していく中で、工場向け・ビル向けのお客様から運用に関する要件を確認し、サービスの改善を図っていきます。

■フォーティネットジャパン合同会社様からのエンドースメント

この度、NTT アドバンステクノロジー様が発表された「FortiGate SOC サービス プラス OT オプション」の提供開始を心より歓迎申し上げます。

本サービスで導入された FortiGate は、世界で最も導入されているネットワークファイアウォールの一つで、エントリー～ハイエンドモデルを取り揃えており、UTM 機能、SD-WAN やゼロトラストなどの先進機能を含めて、あらゆる環境で幅広くご活用いただいております。

今回、産業用サブスクリプションを導入いただいたことで、IP プロトコルベースで接続した OT 機器の監視も可能となり、OT 環境でのセキュリティ対策の強化を実現いたします。

この NTT アドバンステクノロジー様の新しいサービスを利用することで、お客様は迅速にサイバーセキュリティ対策を導入でき、運用負荷の軽減を実現できるようになります。フォーティネットは OT ビジネスの「自助・共助・公助」のエコシステム構築に向けて、NTT アドバンステクノロジー様と共に日々脅威が増している OT/IoT 機器に強力なセキュリティ対策を提供し、お客様のセキュアな DX 推進を支援して参ります。

フォーティネットジャパン合同会社
OT ビジネス開発部長 佐々木 弘志

- *1:参考 Fortinet 社「製造分野のサイバーセキュリティ」
<https://www.fortinet.com/jp/solutions/industries/manufacturing>
- *2:NTT-AT「製造業に必須!工場・ビル向け OT/IoT セキュリティサービス」
<https://www.ntt-at.co.jp/product/ot-iot/>

※記載された会社名及び製品名は、各社の商標または登録商標です。
※掲載のデータは発表日現在の情報です。予告なしに変更されることがございますので、あらかじめご了承ください。

本件に関するお問い合わせ先

【商品に関するお問い合わせ先】

NTT アドバンステクノロジー株式会社

セキュリティ事業本部

トータルセキュリティソリューションビジネスユニット

FortiGateSOC 担当

<https://www.ntt-at.co.jp/product/fortigate-soc/ot.html>

【報道関係のお問い合わせ先】

NTT アドバンステクノロジー株式会社

ビジネス推進部

コーポレート・コミュニケーション部門

担当:加藤・増田

