SOLUTION BRIEF

アプリケーション制御による産業用制御システムの保護

概要

デジタルイノベーションのイニシアチブによって OT（オペレーショナルテクノロジー）と IT ネットワークとの「エアギャップ」が消失し、OT のネットワークを標的とする攻撃が増加しています。FortiGate NGFW（次世代ファイアウォール）に統合されているアプリケーション制御テクノロジーでは、48 の OT アプリケーションからのトラフィックとプロトコル内の 1,500 以上のシグネチャを識別できます。

FortiGuard Labs では OT の知識を活用して 1 日あたり数十億のセキュリティイベントを分析し、OT 専用の脅威に関する脅威インテリジェンスを作成しています。この OT 専用の脅威インテリジェンスとアプリケーション制御を組み合わせることで、アプリケーション固有のセキュリティポリシーの定義と適用が可能になり、ネットワークセグメンテーションによってパフォーマンスへの影響を最小限に抑えながら OT ネットワークを強力に保護できます。

OT 組織の 10 社中 9 社が、過去 1 年間に OT システムへの侵入を少なくとも 1 回は経験しており、マルウェアとフィッシングが最も多い結果となっています [1]。

脅威に合わせて進化が求められる OT の保護

これまで、OT ネットワークのセキュリティは、OT と IT のネットワーク間の物理的な切断（エアギャップ）に依存していました。しかし、このモデルはもはや適用できない場合が増えています。コンバージェンスは、ビジネス上のメリットを確実にもたらすものの、そのプロセスには多くのセキュリティ上の課題が伴い、IT / OT システムを完全に統合している企業は 15% にとどまっています [2]。

OT オペレーターは OT プロトコルを可視化してネットワーク内での流れを把握し、制御する必要があります。FortiGate NGFW にはアプリケーション制御が統合されているため、OT ネットワークのトラフィックに対してアプリケーション固有のセキュリティポリシーを適用できます。

アプリケーション制御がOTに必要な理由

OT 環境では、OT 固有のアプローチによって脅威を検知してレスポンスする必要があります。従来のウイルス対策ソリューションでは、シグネチャの頻繁な更新や大容量メモリを必要とし、不正なプロセスを止める機能も十分ではないため、OT 環境には適していません。こうした問題は、OT デバイスの可用性やメッセージの遅延に影響を与えるため、このようなソリューションは OT 環境では実現できないことを意味します。

OT システムを保護するには、ネットワークレベルでセキュリティ制御を導入する必要があります。FortiGate NGFW では、ICS（産業用制御システム）で送受信するすべてのトラフィックが監視、フィルタリングされるため、必要なレベルの保護を確保できます。

IT 環境と OT 環境の統合によって産業用制御システムは多様な脅威に直面しているため、それぞれの脅威に合わせたセキュリティ監視が必要です。フォーティネットは長年にわたって OT 環境を保護し、業界最大の OT 専用のパートナーエコシステムを構築した経験から、OT 固有の脅威を深く理解しています。その知識を活用して、FortiGuard Labs は 1 日あたり 1,000 億を超えるセキュリティイベントを分析し、OT 専用の脅威インテリジェンスを開発しています [3]。

FortiGate 向けの FortiGuard 産業用セキュリティサービスは、OT に特化した IPS とアプリケーション制御用シグネチャを組み合わせたものになります。また、ネットワークレベルの脅威を検知して保護する機能を産業用制御システムに提供するとともに、こうした環境で使用されている産業用アプリケーションに対する広範な可視性を実現します。

アプリケーション制御エンジンは Modbus、BACnet、OPC Classic などの 48 の異なる OT 固有のネットワークプロトコルと 1,500 以上の異なるシグネチャを識別できます。このような機能と FortiGuard Labs の OT 専用の脅威インテリジェンスを組み合わせることで、ネットワークトラフィックのタイプの識別と監視が可能になり、きめ細かい制御によって OT 環境内のデータフローを制限できます。

図 1：アプリケーション制御が統合された FortiGate NGFW のトラフィックフロー

ICS 環境のアプリケーション制御

これまで多くの OT 環境では「エアギャップ」をセキュリティ戦略の中核に据えていました。IT と OT のネットワーク間を接続しないことで、ICS のコンポーネントへのサイバー脅威の侵入を防止していました。

しかし、現在では IT と OT のネットワーク間のエアギャップは急速に消滅しています。デジタルイノベーションのイニシアチブによって生産性と効率性を向上させるため、センサーなどの監視デバイスをインターネットに接続する IIoT（産業用 IoT）が推進されたためです。IT と OT のネットワークの接続が増えると、OT 環境を保護するにはネットワークのセグメンテーションが必要になります。

図 2 は ICS 環境への FortiGate NGFW の導入例を示しています。ICS ネットワークを複数のゾーンに分割します。

- 非武装地帯（DMZ）ネットワーク：データ ヒストリアン
- プロセスネットワーク：サーバーとヒューマンマシンインタフェース（HMI）
- 制御ネットワーク：プログラマブルロジックコントローラ（PLC）
- フィールドネットワーク：バルブ、ファン、ポンプ

OT ネットワーク内の異なるゾーン間、企業のイントラネット、インターネット、リモートサイトへの通信は、FortiGate NGFW によって監視および保護されます。

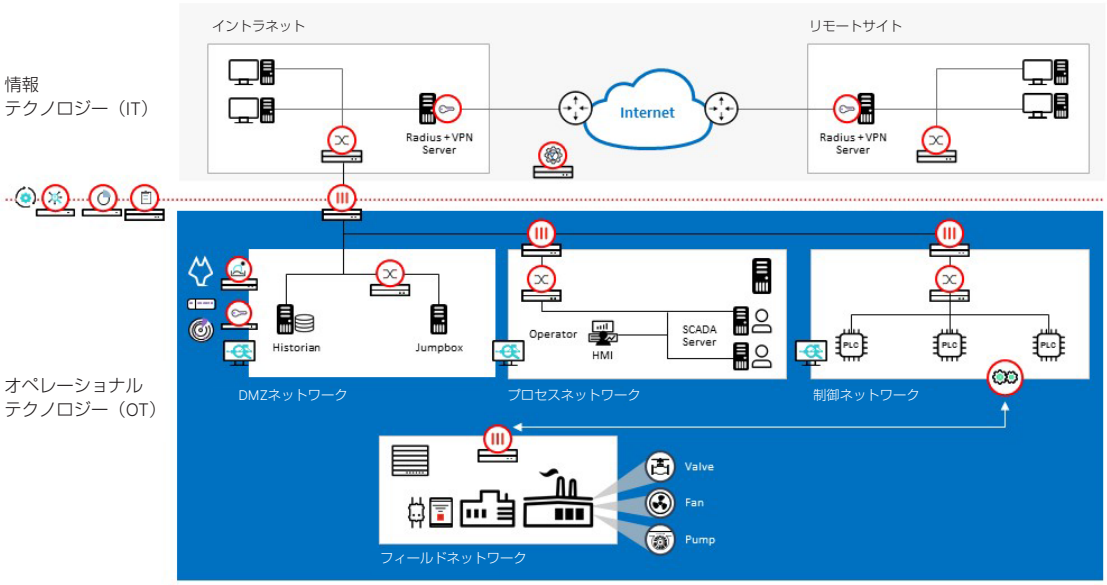

図 2：ICS 環境への FortiGate NGFW の導入例

ICS の脅威減災シナリオ

アプリケーション制御では、アプリケーションレベルでトラフィックを識別してフィルタリングできるため、セキュリティをきめ細かく制御できます。また、OT 環境の運用や生産性に悪影響を与えることなく、高度な脅威からの保護が可能です。

ヒストリアンは通常、OT ネットワークの DMZ に配置されるため、サイバー攻撃に対して脆弱です。しかし、運用データを収集して保存するために、ヒストリアンは PLC にアクセスしてデータを読み取る必要があります。そのため、それらのデータを要求するときに使用した Modbus プロトコルが攻撃者に悪用され、不正なコマンドを PLC に送信される可能性があります。

アクセスしてデータを読み取るには、ヒストリアンと PLC の間にネットワーク接続が必要なため、2 つのシステム間のトラフィックをすべてブロックすることはできません。2 つのシステム間のトラフィックをフィルタリングし、正規のアクセスと不正なコマンドを区別するには、Modbus プロトコルに含まれる特定のコマンドを理解する必要があります。

アプリケーション制御では、適切なレベルのフィルタリングが提供されます。また、FortiGate NGFW では、ヒストリアンから PLC への読み取り専用のアクセスを許可するように設定できます。攻撃者がヒストリアンを侵害して PLC にコマンドを送信しても、要求は FortiGate NGFW によって識別され、ブロックされます。また、NGFW ではアラートが自動的に生成され、フォーティネット セキュリティ ファブリックから SOC（セキュリティオペレーションセンター）に送信されます。それによって SOC はインシデントを調査し、侵害されたデータヒストリアンを修正することができます。

終わりに

OT の脅威は拡大と進化を繰り返しているため、OT オペレーターは ICS デバイスに送信されるトラフィックのタイプを詳細に把握する必要があります。FortiGate NGFW に統合されたアプリケーション制御を使用することで、必要な可視化と制御を確保できます。

OT デバイスを保護するには OT 固有のセキュリティソリューションが必要です。FortiGate NGFW でマイクロセグメンテーションを適用することにより、OT ネットワークのサイバー脅威のリスクが減少し、組織のセキュリティアーキテクチャの可視化と管理を一元化することができます。

[1]「2021 年オペレーショナルテクノロジーとサイバーセキュリティに関する現状レポート」、フォーティネット、2021 年 5 月 26 日：https://www.fortinet.com/content/dam/fortinet/assets/white-papers/ja_jp/report-2021-ot-cybersecurity.pdf

[2]「セキュリティリスクが IT と OT の統合を遅らせていることが独自調査により判明」、フォーティネット、2021 年 5 月 23 日：https://www.fortinet.com/content/dam/fortinet/assets/white-papers/ja_jp/report-forrester-it-ot-covergence-jp.pdf

[3]「FortiGuard Security Services」、Fortinet、2021 年 7 月 11 日（英語）：https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGuard_Security_Services.pdf

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

SB-Application-Control-Secures-ICS-202110-R1