WHITE PAPER

フォーティネット セキュリティ ファブリックによる OT サイバーリスクの軽減

OT のサイバーセキュリティリーダーのための戦略

概要

DX（デジタルトランスフォーメーション）によって 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）の統合は加速し、ビジネスも進化しています。企業は IoT（モノのインターネット）、クラウドコンピューティング、AI（人工知能）などのデジタルテクノロジーを活用して運用を最適化し、安全性と信頼性を向上させることで競争力を強化しています。OT と IT の統合とデジタル技術の採用には多くのメリットがありますが、OT の攻撃対象領域が増加し、サイバー脅威に対してより脆弱になるというデメリットもあります。

では、どうしたら OT のサイバーリスクを軽減できるでしょうか。その答えは、フォーティネット独自の革新的なセキュリティアーキテクチャであるフォーティネット セキュリティ ファブリックにあります。セキュリティ ファブリックにはクラス最高のセキュリティソリューションが統合されているため、OT と IT の攻撃対象領域を幅広く可視化できるだけでなく、運用を自動化し、信頼性を継続的に評価することもできます。以下では、OT のサイバーセキュリティを強化するサイバーセキュリティの 5 つのベストプラクティスと、それぞれに対応するセキュリティ ファブリックのコンポーネントについて説明します。フォーティネット セキュリティ ファブリックを IT 環境と OT 環境の統合の安全な基盤として活用する方法をご紹介します。

無料の脅威評価はリスクの特定と優先順位付けに役立ちます。

*ICS は OT の部分要素ですが、最近は同じものとして扱うケースも増えています。OT はプロトコル、ベンダー、ユースケースが IT とは異なり、IT との対比で使用されることがあります。SCADA（監視制御 / データ取得）システムは OT に含まれます。SCADA システムではグラフィカルユーザーインタフェースを使用して OT / ICS プロセスにおける高位の管理を行います。

OT / IT ネットワーク統合のためのフォーティネットのサイバーセキュリティ

IT と OT の統合と DX を実現するには、両方のインフラストラクチャを適応させるだけでなく、セキュリティトランスフォーメーションによってサイバー脅威から保護する必要があります。フォーティネットでは、サイバーセキュリティに対するプロアクティブで革新的なアプローチとしてフォーティネット セキュリティ ファブリックを提供しています（図 1 参照）。セキュリティ ファブリックでは以下が可能になります。

- OT と IT の攻撃対象領域の幅広い可視化による迅速な脅威の検知とポリシー適用
- テクノロジー、場所、展開の異なるセキュリティ、運用、パフォーマンスの統合による完全な可視化
- AI と機械学習（ML）を活用した自動による運用とレスポンス、およびユーザーからアプリケーションまでカバーするほぼリアルタイムの保護

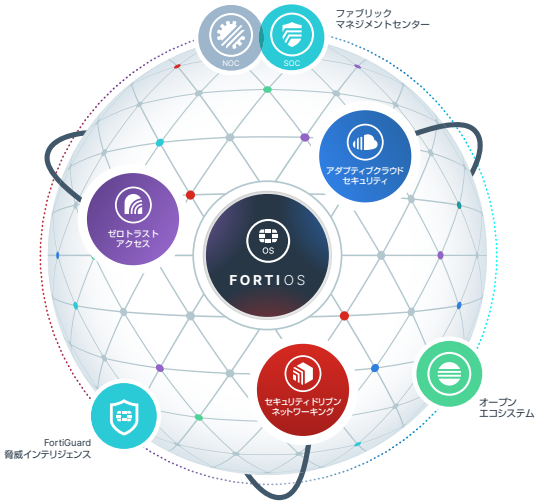

図 1：OT 環境と IT 環境に対応した複数のテクノロジーである FortiOS をベースに統合したフォーティネット セキュリティ ファブリック。セキュリティ ファブリックではオープンエコシステムを活用し、拡大するデジタルの攻撃対象とサイクル全体に自己修復型のセキュリティとデバイス、データ、アプリケーションを保護するネットワークが提供されます。

OT サイバーセキュリティのベストプラクティス

セキュリティ ファブリックを導入することで、可視化、統合、自動化、修復に必要な機能がすべて提供され、セキュリティも維持できます。セキュリティ ファブリックは、組織のセキュリティの優先順位に合わせて段階的に導入できます。段階的に導入する場合、以下のベストプラクティスをお勧めします。

ネットワークセグメンテーションはネットワーク内とネットワーク間の攻撃者の移動を制限します。

1. 資産の特定、分類、優先順位付け

組織の OT セキュリティ態勢の改善を目指すなら、まず、ネットワーク上で実行しているデバイスとアプリケーションの最新のインベントリを取得する必要があります。フォーティネットではそのために、無償で Fortinet Cyber Threat Assessment を提供しています（ご利用には条件があります）。このアプローチでは、まず、FortiGate 次世代ファイアウォール（NGFW）または FortiNAC ネットワークアクセス制御（NAC）ソリューションを使用して、ネットワークトラフィックの受動的な監視が行われます。そうして得られたトラフィックデータが分析され、特性と動作に基づいてデバイスの特定と確認が行われます。その結果、以下のレポートが作成されます。

- 高リスクのアプリケーション
- アプリケーションの脆弱性の重大なエクスプロイト
- 各資産のリスク値の評価
- マルウェア、ボットネット、および侵害された可能性があるデバイス
- アプリケーションの分類と各アプリケーションによるネットワークの使用状況の分析

フォーティネットのソリューションを使用することにより、CISO はこれらの情報を基盤としてセキュリティを最適化できます。

2. ネットワークセグメンテーション

OT の侵害では多くの場合、攻撃者は IT と OT の各ネットワーク内とネットワーク間を水平方向に移動しますが、ネットワークセグメンテーションによって移動を制限できます。これは、ISA / IEC-62443（旧 ISA-99）のセキュリティ標準で示されているように、OT 保護の基本的なベストプラクティスです [1]。

ネットワークセグメンテーションでは、ネットワークは機能のセグメントまたは「ゾーン」（サブゾーンまたはマイクロセグメントを含む場合もあります）と「コンジット」（ゾーン間のチャネル）に分割されます。**FortiGate 内部セグメンテーションファイアウォール（ISFW）**では**フォーティネットのインテントベースト セグメンテーション**を使用して、ゾーンとコンジットが定義されて適用されます。このアプローチでは、ユーザー、デバイス、アプリケーションの信頼性が継続的に監視され、ビジネスの目的、振る舞い、リスクに基づいてアクセスが動的に制御されます。そのため、攻撃対象領域が大幅に縮小され、侵入者による脆弱性の特定と悪用が困難になります。

3. トラフィック分析による脅威と脆弱性に対する保護

脅威をブロックするにはネットワークトラフィックを分析して特定する必要があります。フォーティネットでは管理と分析のために、以下からの情報を統合して提供しています。

FortiSIEM（セキュリティ情報 / イベント管理）では、ネットワークに接続しているすべての要素が自動的に検知され、構成管理データベース（CMDB）が構築されます。また、プロアクティブにリスクを軽減し、規制とセキュリティ標準への準拠を実証するために使用する監査可能なトラフィックレコードも作成されます。

FortiManager では最新のセキュリティ ファブリックのステータスが表示されるダッシュボードに加え、セキュリティオペレーションセンター（SOC）とネットワークオペレーションセンター（NOC）の両チームの統合ビューも提供されます。これらを通して SOC チームはセキュリティアラートの内容と問題を確認でき、NOC チームはパフォーマンスの低下がセキュリティインシデントの結果であるかどうかを確認できます。また、オペレーションチームはセキュリティチームが求める資産の再構成や隔離の必要性を容易に理解して、スムーズに対応できるようになります。

FortiAnalyzer ではログ管理とリアルタイムの脅威分析を自動化できます。FortiGuard Labs は世界中のさまざまな情報源から毎日約 50 万の IOC（Indicators of Compromise：侵害指標）を収集しています。FortiAnalizer ではその情報を利用して不正が確認されたサーバーとの通信が特定されます。また、FortiGuard セキュリティレーティングサービスを通して、社内の経時的リスクや他社のリスクを定量化したリスクスコアリングによって比較できます。

上記に加えて、FortiGate NGFW を使用してトラフィックを検査し、不正なファイル、アプリケーション、エクスプロイトから保護できます。

FortiGate NGFW で使用する **FortiGuard 産業用セキュリティサービス**は、FortiGate Enterprise バンドルと 360 バンドルのサブスクリプションサービスに含まれています。最新のシグニチャを使用して、一般的な OT プロトコルの特定と監視、OT の既知の脆弱性の悪用の検知とブロックを行います（表 1 参照）。ファームウェアのパッチや更新を適用せずに機器を日常的に使用する OT 環境では、既知のエクスプロイトをブロックすることは特に重要です。

脅威を検知してポリシーを適用するために、FortiGate NGFW では暗号化された SSL（Secure Sockets Layer）/ TLS（Transport Layer Security）トラフィックがスキャンされます。FortiGuard Labs によると、現在、暗号化された Web トラフィックは全体の約 85% を占めるため、暗号化トラフィックの検査は不可欠です [2]。パフォーマンスに大きな影響を与える他のファイアウォールソリューションとは異なり、FortiGate NGFW は専用のセキュリティプロセッサ（SPU）を使用するため、パフォーマンスの低下を極力抑制することができます。そのため、データセンターやネットワークのエッジなどのファイアウォールインフラストラクチャにアプライアンスを後付けしたり追加したりする必要はなくなります。

OT プロトコル		OT アプリケーションとベンダー		
BACnet	MMS	7-Technologies / Schneider Electric	Honeywell	RealFlex
DNP3	Modbus	ABB	ICONICS	Rockwell Automation
Elcom	OPC	Advantech	InduSoft	RSLogix
EtherCAT	PROFINET	Broadwin	intellicom	Siemens
EtherNet / IP	S7	CitectSCADA	Measuresoft	Sunway
HART	SafetyNET	CODESYS	Microsys	TeeChart
IEC 60870-5-104	Synchrophasor	Cogent	Moxa	VxWorks
IEC 60870-6（TASE.2）/ ICCP	MMS	DATAC	PcVue	Wellintech
IEC 61850		Eaton	Progea	Yokogawa
LonTalk		GE	QNX	

表 1：FortiGuard 産業用セキュリティサービス

トラフィックを分析し、脅威から保護するセキュリティ ファブリックにはそのほかにも以下のようなソリューションがあります。

FortiMail の E メールゲートウェイは、認証情報を窃取する OT の侵害で一般的なスピアフィッシングなどの脅威を軽減できます。OT にとってマルウェアとフィッシングは最も一般的な攻撃です [3]。FortiMail では設定によって不審な未知の脅威を **FortiSandbox** に送信することができ、それによって振る舞いを分析して、エンドユーザーに配信される前に脅威を特定できます。FortiSandbox はエンドポイント、ネットワーク、クラウドなど他のアクセスポイント（AP）やファイル共有による潜在的な脅威にも対応できます。また、セキュリティ ファブリックに完全に統合されているため、すべてのセキュリティソリューション間で脅威インテリジェンスをリアルタイムで自動的に共有できます。

FortiDeceptor はおとり（デコイ）を使用して脅威を分析および回避し、情報はセキュリティ ファブリック全体で共有できます。**FortiIsolator** はユーザーのブラウザと Web サイトの間に視覚的なエアギャップを作成するブラウザ分離ソリューションです。Web コンテンツをリモートの使い捨てコンテナに表示することでマルウェアの脅威を隔離します。

4. ユーザーとデバイスのアクセス制御

セキュリティ ファブリックでは以下の機能を組み合わせて、ユーザーとデバイスのネットワークアクセスを制御します。

FortiGate NGFW はユーザーグループとデバイスグループを作成し、それぞれにセキュリティポリシーを適用するために使用します。たとえば、リモートユーザーとローカルユーザーには異なる制御を設定できます。

FortiAuthenticator ではユーザーのアイデンティティを検証して、各ゾーンとコンジットへのユーザーアクセスのきめ細かい制御を適用できます。ユーザーとサードパーティシステムからのアクセス許可を確認し、その情報を FortiGate デバイスに送信できるため、各デバイスでアイデンティティベースのポリシーを適用できます

FortiToken では多要素認証（MFA）を使用してアイデンティティの検証を強化できます。ユーザーの認証情報をハードウェアやソフトウェアトークン、指紋などの他の生体認証と組み合わせるため、窃取した認証情報だけでは通過することができません。

多要素認証を導入することで、窃取した認証情報の使用や OT の侵害が困難になります。

FortiNAC ではネットワークに接続しているデバイスの特性を観察して認証が行われます。認証後、ネットワークへの接続の可否、接続方法、アクセス可能なネットワークセグメントを制御するポリシーをデバイスに適用できます。また、FortiNAC では必要に応じてポートを切断することもできます。デバイスやアプリケーションは許可を受けない限りアクセスできません。デバイスが認証されるまでネットワークへの接続はポートによって拒否されます。また、OT ネットワークにデバイスを追加した場合は接続前に権限のあるスタッフの承認を受けるようポリシーを設定することもできます。

FortiClient は FortiGate NGFW と統合することにより、OT 環境のエンドポイントデバイスの可視化と脆弱性のアラート発信が可能になります。

5. 有線 / 無線アクセスの保護

多くの OT 環境では、有線と無線の AP が攻撃に悪用されるリスクが増大しています。DX によって情況がさらに悪化することもあります。たとえば、一部の製造工場や倉庫では無人搬送車（AGV）を使用していますが、これらは無線接続して製品や資材を移動します。OT ネットワークへの接続を含め、無線や IoT を導入する場合、攻撃対象領域が拡大します。

リスクを最小限に抑えるために、セキュリティチームは有線と無線のアクセスを 1 つのインタフェースによって一元管理する必要があります。FortiGate NGFW では独自の安全な暗号化トンネルを使用して、ファイアウォール機能とポリシーを **FortiSwitch** と **FortiAP** すべてのポートに適用できます。

また、セキュリティチームは FortiNAC を使用して、170 社のベンダーにおける最大 2,000 のネットワークデバイスなど、サードパーティのスイッチとワイヤレス AP の構成を一元化することもできます。

耐環境仕様の FortiSwitch、FortiAP、FortiGate NGFW は、海上の石油掘削装置や輸送コンテナから工場までの多様な OT 環境における衝撃、振動、ほこり、湿気、極端な温度に耐えられるように設計されています。

OT のセキュリティ強化

OT のテクノロジーは、IT が登場するはるか以前の 20 世紀初頭に開発されました。そのため、OT と IT のネットワークはエアギャップによって分離されていました。しかし、ビジネス価値を向上させるため、現在ではこの 2 つは統合されつつあります。IT と OT を統合するとデジタルの攻撃対象領域は拡大しますが、以下を可能にする適切な制御とテクノロジーを導入すれば OT 環境を保護できます。

1. 攻撃対象領域の幅広い可視化
2. ネットワークセグメンテーションによる侵入の制限
3. 暗号化トラフィックや OT の一般的なプロトコルなどのトラフィック分析による脅威からの保護
4. ユーザーとデバイスのアクセス制御、アイデンティティベースのポリシー適用、継続的な信頼性評価
5. 単一のインタフェースによる有線 / 無線アクセスの保護と制御の一元管理

フォーティネット セキュリティ ファブリックでは、共通の FortiOS オペレーティングシステムを通して IT と OT のセキュリティソリューションが統合されます。また、攻撃対象領域の幅広い可視化、AI による侵害防止、自動化、オーケストレーション、レスポンスなどの機能も提供されます。その機能と利点をすべてご活用いただくため、まずは無償の脅威評価を利用されてから、御社のセキュリティの優先順位に合わせて段階的に導入されることをお勧めします。

[1]「ISA Standards: Numerical Order」、International Society of Automation、2018 年 1 月 3 日時点の情報、（英語）：
https://www.isa.org/standards-and-publications/isa-standards/find-isa-standards-in-numerical-order

[2]「Keeping Up With the Performance Demands of Encrypted Web Traffic」、Nirav Shah 著、Fortinet、2020 年 8 月 4 日、（英語）：
https://www.fortinet.com/blog/industry-trends/keeping-up-with-performance-demands-of-encrypted-web-traffic

[3]「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」、Fortinet、2021 年 7 月 19 日：
https://www.fortinet.com/content/dam/fortinet/assets/white-papers/ja_jp/report-2021-ot-cybersecurity.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

WP-OT-CISO-Solution-Selection-202109-R1