WHITE PAPER

フォーティネット セキュリティ ファブリックを使用した 医薬品製造における OT サイバーリスクの軽減

概要

製薬会社は、業務効率の改善、サプライチェーンの弾力性の向上、そしていっそう柔軟な生産戦略の導入方法を模索しています。こうしたデジタルトランスフォーメーション（DX）の取り組みは、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）の融合を加速し、ビジネスを前進させています。製薬会社は、IoT（モノのインターネット）、クラウドコンピューティング、人工知能（AI）などのデジタルテクノロジーを活用して、プロセスの最適化、安全性と信頼性の向上、競争力の強化を実現しています。しかし、多くのメリットがあるにもかかわらず、OT と IT の融合とデジタルテクノロジーの導入の増加によって、OT の攻撃対象領域が拡大し、サイバー脅威に対する脆弱性が高まっています。

では、このような会社はどのようにして OT のサイバーリスクを軽減できるのでしょうか。その答えは、変革をもたらす独自のセキュリティアーキテクチャを活用したフォーティネット セキュリティ ファブリックにあります。セキュリティ ファブリックは、クラス最高のセキュリティソリューションを統合することで、OT と IT の両方の攻撃対象領域を幅広く可視化するとともに、オペレーションの自動化と継続的な信頼性評価を実現します。このホワイトペーパーでは、OT のサイバーセキュリティ対策を強化する 5 つのサイバーセキュリティのベストプラクティスについて説明し、それぞれにセキュリティ ファブリックのコンポーネントをマッピングします。フォーティネットの集約されたソリューションは、IT と OT 環境を融合させ、新たなビジネス価値を実現するための基盤として、お客様の成長を支え、ビジネスをサポートします。

OT / IT ネットワークを集約するためにフォーティネットが設計したサイバーセキュリティ

製薬会社がコンバージェンスや DX を考慮して IT と OT のインフラストラクチャを適応させる際には、進化するサイバー脅威から保護するためにセキュリティの変革も行わなければなりません。フォーティネットは、図 1 に示すように、サイバーセキュリティに対して、プロアクティブで変革的なアプローチであるフォーティネット セキュリティ ファブリックを提供します。セキュリティ ファブリックには以下のようなメリットがあります。

- OT と IT の攻撃対象領域全体にわたる広範な可視性
- すべてのデバイス、ネットワーク、アプリケーションにわたる統合された保護
- AI と機械学習（ML）によるオペレーションとレスポンスの自動化
- OT と IT の境界を越えた包括的で拡張性の高いセキュリティ
- オペレーションが規制要件（例：GDPR、NIST、FDA、OECD）を満たしていることを確認するための継続的な検証

セキュリティ ファブリックの導入は、可視性、統合、自動化、復元力を備えた望ましいセキュリティ環境へと至るプロセスです。セキュリティ ファブリックは、組織のセキュリティ上の優先順位に合わせて段階的に実現していくことができます。その各段階を計画する際には、以下のベストプラクティスを組み込むことが賢明です。

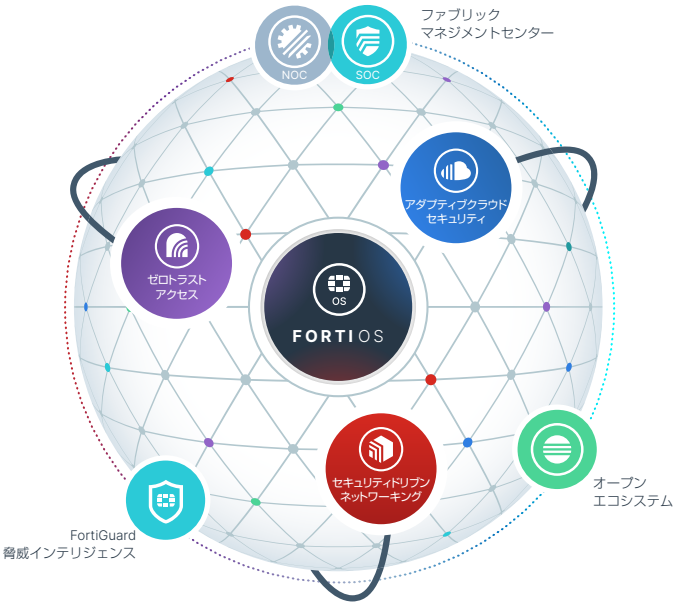

図 1：フォーティネット セキュリティ ファブリックを使用することで、OT と IT の環境全体で複数のテクノロジーを連携させることができます。
これらはすべて、脅威インテリジェンスの単一ソースによってサポートされ、ネットワーク内のセキュリティギャップを解消し、あらゆる攻撃ベクトルに対応します。

推奨される OT サイバーセキュリティのベストプラクティス

アセットの特定、価値の分類、優先順位付け

組織の OT セキュリティ態勢を改善しようとする CISO にとって最初のステップは、ネットワーク上で稼働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ことです。フォーティネットでは、フォーティネットのサイバー脅威評価（Fortinet Cyber Threat Assessment）を無償で提供しています。このサービスは、認定を受けたお客様が利用できます。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 コントロール（NAC）を使用して、ネットワークトラフィックをパッシブに監視します。次に、このパッシブなトラフィック分析をもとに、デバイスの特性や動作に基づいてデバイスを識別し、プロファイリングします。その結果、以下の情報がレポートされます。

- 高リスクのアプリケーションを指摘
- アプリケーションの脆弱性の重大なエクスプロイトを検知して特定
- 各アセットのリスク価値を評価
- マルウェア、ボットネット、侵害された可能性があるデバイスの兆候を特定
- アプリケーションを分類し、アプリケーションによるネットワークの使用状況を分析

CISO は、フォーティネットと協力し、セキュリティ計画を最適化するための基礎として情報を利用できます。

セグメンテーションは、ネットワークを一連の機能的なセグメントや「ゾーン」（サブゾーンやマイクロセグメントを含む場合もある）、「導管」（ゾーン間のチャネル）に分割します。

ネットワークのセグメンテーション

セグメンテーションは、ネットワークを一連の機能的なセグメントや「ゾーン」（サブゾーンやマイクロセグメントを含む場合もある）、「導管」（ゾーン間のチャネル）に分割します。**FortiGate 内部セグメンテーションファイアウォール（ISFW）**は、ゾーンと導管を定義して適用します。これはフォーティネットの**インテントベースセグメンテーション**と呼ばれるアプローチで、ユーザー、デバイス、アプリケーションの信頼度を継続的に監視し、ビジネスの意図、行動、リスクに基づいてアクセスを動的に制御します。これにより、侵入者が脆弱性を見つけて悪用することがより困難になり、攻撃対象領域が劇的に縮小します。

脅威と脆弱性に対するトラフィックの分析と保護

脅威を特定してブロックするためには、ネットワークトラフィックを分析することが重要です。フォーティネットの管理 / 分析ソリューションは、以下の情報を統合することでこの機能を実現しています。

FortiSIEM（セキュリティ情報 / イベント管理）は、ネットワークに接続されているすべてのデバイスを自動的に検出し、構成管理データベース（CMDB）を構築します。また、プロアクティブなリスク軽減や、規制およびセキュリティ標準へのコンプライアンスの実証に使用される監査可能なトラフィックレコードも作成します。

FortiManager は、最新のセキュリティ ファブリックのステータスを示すダッシュボードビュー、および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）の両チームに役立つ統合ビューを提供します。SOC チームはセキュリティアラートや問題の範囲を確認でき、NOC チームはセキュリティインシデントの結果としてパフォーマンスが低下したかどうかを確認できます。こうした知見を獲得したオペレーションチームは、ネットワーク資産の再構成や隔離を求めるセキュリティチームの要求をよく理解できるようになり、合意に至りやすくなります。

FortiAnalyzer は、ログ管理とリアルタイムの脅威分析を自動化します。これは、FortiGuard Labs が提供する IOC（Indicators of compromise、侵害指標）サービスを活用しており、世界中のさまざまなソースから収集した約 50 万件の IOC を日々パッケージ化します。これにより、悪意のあることが判明したサーバーとの通信を特定できます。また、FortiAnalyzer は、FortiGuard セキュリティレーティングサービスを利用して、社内での経年変化や類似組織との比較など、リスクを定量的にスコアリングできます。

上記に加えて、フォーティネットの管理 / 分析ソリューションは、**FortiGate** NGFW を活用してトラフィックを検査し、悪意のあるファイル、アプリケーション、セキュリティ侵害から保護します。

FortiGate NGFW は、FortiGate エンタープライズバンドルと 360 バンドルのサブスクリプションサービスの一部である **FortiGuard 産業用セキュリティサービス**を利用してシグネチャを更新し、最も一般的な OT のプロトコルを特定して監視するとともに、既知の OT の脆弱性のセキュリティ侵害の試みを検知してブロックします（表 1 参照）。既知のセキュリティ侵害をブロックすることは、パッチやファームウェアを更新せずに日常的に機器が稼働している OT 環境では特に重要です。

FortiGate NGFW は、脅威を検知してポリシーを適用するために、暗号化された SSL（Secure Sockets Layer）/ TLS（Transport Layer Security）トラフィックをスキャンします。現在、暗号化されたトラフィックは全ネットワークトラフィックの 72% を占め、サイバー攻撃の 50% が隠れて見えないため、暗号化されたトラフィックを検査することが必要不可欠です [1、2]。FortiGate NGFW は、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、専用のセキュリティプロセッサ（SPU）を使用してパフォーマンスの低下を最小限に抑えます。これにより、組織はデータセンター内であるか、ネットワークのエッジであるかを問わず、ファイアウォールのインフラストラクチャにアプライアンスを追加する必要がなくなります。その結果、FortiGate NGFW は、暗号化されたトラフィックをスキャンする際に、競合テストで最高の価格性能比を実現しています。また、巧妙な攻撃を 100% ブロックすることができました [3]。

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		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 ファブリックの他の機能は以下のとおりです。

FortiMail メールゲートウェイは、認証情報を窃取するために OT の侵害を目的として頻繁に使用される手口である、スピアフィッシングなどの脅威を軽減します。FortiMail は、疑わしい未知の脅威を FortiSandbox に渡すように設定することもできます。FortiSandbox はアクションを分析し、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、クラウド環境、ファイル共有など、他のアクセスポイントからの潜在的な脅威にも対応できます。FortiSandbox はセキュリティ 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要素にわたって脅威インテリジェンスを自動的にリアルタイムで共有します。

FortiDeceptor は、デコイ（おとり）を使って脅威アクティビティを迂回させて分析し、セキュリティ ファブリック全体で情報を共有します。**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り出す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排除します。

アクセス制御ユーザーとデバイスのアクセス

セキュリティ ファブリックは、以下のような機能を連携させてネットワークへのアクセスを制御します。

FortiGate NGFW を使用して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できます。たとえば、ローカルユーザーとリモートユーザーでは設定できる内容が異なります。

FortiAuthenticator は、ユーザーのアイデンティティを検証し、各ゾーンや導管へのユーザーのアクセスをきめ細かく制御します。そのためにユーザーを識別し、サードパーティのシステムからのアクセス権限を問い合わせて、その情報を FortiGate デバイスに伝達し、それらのデバイスがアイデンティティベースのポリシーを実施できるようにします。

FortiToken は、さらに多要素認証（MFA）によってアイデンティティを検証し、ユーザーの認証情報をハードウェアまたはソフトウェアのトークンや指紋などのバイオメトリックと組み合わせます。MFA は、盗まれた認証情報を使用することをより困難にします。

多様な種類の OT 環境で、有線および無線のアクセスポイントを介した潜在的な攻撃にさらされる機会が増えています。このようなリスクの増加は、しばしば DX が原因となっています。

FortiNAC は、ネットワークに接続されているデバイスの特性を観察し、デバイスを認証します。プロファイリングが完了すると、FortiNAC はデバイスにポリシーを適用し、デバイスがネットワークに接続するかどうか、どの方法で接続するか、ネットワークのどのセグメントにアクセスできるかを制御できます。また、必要に応じてポートをロックすることもできます。デバイスやアプリケーションは、許可されるまでアクセスできません。ポートは、ネットワークに接続しようとしているデバイスが認証されるまではそのデバイスをネットワークに接続しません。これによって、OT ネットワークに追加されたデバイスはまず権限のあるスタッフによる承認を受ける必要があるというポリシーを実施できます。

FortiClient は FortiGate NGFW と統合することで、OT 環境のエンドポイントデバイスの可視化し、脆弱性の警告をトリガーします。

有線 / 無線アクセスの保護

多様な種類の OT 環境で、有線および無線のアクセスポイントを介した潜在的な攻撃にさらされる機会が増えています。このようなリスクの増加は、しばしば DX が原因となっています。たとえば、一部の製造工場や倉庫では、商品や材料を移動する際に無線接続された無人搬送車（AGV）を使用しています。Forrester が実施した調査では、すべての企業が無線または IoT 技術を導入することで攻撃対象領域が拡大してしまっており、これには OT ネットワークへの接続も含まれています [4]。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 / 無線アクセスを 1 つのインタフェースで一元管理する必要があります。FortiGate NGFW 経由で、独自のセキュアな暗号化トンネルを使用して、ファイアウォール機能やポリシーを組織全体の **FortiSwitch** および **FortiAP** のポートにプッシュできます。

また、セキュリティチームは FortiNAC を使用して、170 のベンダーから提供される最大 2,000 台のネットワークデバイスを含む、サードパーティのスイッチや無線 AP を一元的に設定できます。

耐久性に優れた FortiSwitch、FortiAP アクセスポイント、FortiGate NGFW は、海洋石油掘削装置、輸送用コンテナ、工場のフロアなど、OT 環境で見られる衝撃、振動、埃、湿気、極端な温度に対応するように設計されています。

OT セキュリティの強化

OT 技術は、IT が台頭する何十年も前の 20 世紀初頭に開発されました。従来、OT ネットワークと IT ネットワークは、エアギャップで隔てられていました。現在では、ビジネスの価値を高めるために、この 2 つが統合されています。

IT と OT を統合すると、デジタル攻撃対象領域が拡大してしまいます。しかし、適切な管理と技術を導入することで、製薬会社は以下のように OT 環境を保護できます。

1. 攻撃対象領域の広範な可視性を確保する
2. ネットワークをセグメント化して侵入の影響を抑える
3. 暗号化されたトラフィックや一般的な OT プロトコルを含むトラフィックを分析し、脅威から保護する
4. ユーザーやデバイスによるアクセスを制御し、継続的な信頼性評価によるアイデンティティベースのポリシーを実施する
5. 有線 / 無線の両方のアクセスを保護し、1 つのインタフェースで制御を一元的に管理する

フォーティネット セキュリティ ファブリックは、共通のオペレーティングシステムである FortiOS を使用して、IT と OT のセキュリティソリューションを統合します。攻撃対象領域全体の広範な可視化、AI を活用した統合的な侵害防止、自動化されたオペレーション、オーケストレーション、レスポンスを実現します。ビジネスの成長や新機能の必要性に応じて段階的に技術を導入できるため、バラバラにして交換することなく、複雑さを管理し、既存のセキュリティアプローチを強化できます。つまりフォーティネットは、進化する脅威に対応しながら、セキュリティエコシステムを発展させる展開を積極的にサポートできます。

製薬会社は、セキュリティ ファブリックを利用することで、クラウド、データ、デジタル化、パートナーシップにこれまで以上に依存する必要のあるインフラストラクチャにおいて、データの整合性の維持、運用効率の向上、コスト管理、コンプライアンス報告などに関連する課題を克服できます。

[1] 「Encrypted Traffic Reaches A New Threshold」、John Maddison 著、Network Computing、2018 年 11 月 28 日（英語）：
https://www.networkcomputing.com/network-security/encrypted-traffic-reaches-new-threshold

[2] 「Study Reveals Hackers Increasingly Use Encryption to Hide Criminal Activity」、Lifeline Data Centers、2021 年 5 月 13 日（英語）：
https://lifelinedatacenters.com/data-center/hackers-use-encryption/

[3] 「フォーティネット、NSS Labs の最新 NGFW レポートで「Recommended（推奨）」評価を獲得、暗号化されたクラウドアクセスに適した高い SSL パフォーマンスを提供」、フォーティネット、2018 年 7 月 17 日：https://www.fortinet.com/jp/corporate/about-us/newsroom/press-releases/2018/nss-labs-ngfw-report

[4] 「SCADA / ICS セキュリティリスクが独自調査で明らかに」、フォーティネット、2019 年 6 月 28 日：
https://www.fortinet.com/content/dam/fortinet/assets/white-papers/ja_jp/report-ot-forrester.pdf

* OT は**産業用制御システム（ICS）**と同義です。「OT」という用語は、OT プロトコル、ベンダー、ユースケースが異なるため、IT と対比する用語として使用されるようになりました。**監視制御データ収集システム（SCADA）**システムも OT の一種です。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 プロセスを高度に管理します。

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-Pharmaceutical-Manufacturing-Security-Fabric-202108-R1