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

～ CISO をサポートする戦略 ～

概要

デジタルトランスフォーメーション（DX）は、運用テクノロジー（OT）* と情報テクノロジー（IT）のコンバージェンスを促し、ビジネスを前進させています。組織は、運用の最適化、安全性と信頼性の向上、競争力の強化を目的に、モノのインターネット（IoT）、クラウドコンピューティング、人工知能（AI）などを活用しています。IT / OT コンバージェンスとデジタルテクノロジーにはさまざまなメリットがある一方で、OT 攻撃対象領域が拡大し、サイバー攻撃に対する脆弱性が増すというデメリットも存在します。

では、どのような方法で OT サイバーリスクを軽減すればよいでしょうか。その答えが、フォーティネット セキュリティ ファブリックです。革新的な独自のセキュリティアーキテクチャを採用したフォーティネット 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 両方の攻撃対象領域を幅広く可視化すると同時に、運用の自動化と継続的な信頼性評価の提供を実現します。本書では、OT サイバーセキュリティ態勢を強化する 5 つのベストプラクティスと、それに対応するセキュリティ ファブリックコンポーネントをご紹介します。フォーティネットの統合ソリューションは、IT / OT コンバージェンスと新たなビジネス価値実現の基盤となります。

OT / IT ネットワークコンバージェンスに向けたフォーティネットのサイバーセキュリティ設計

コンバージェンスと DX に向けて IT / OT インフラストラクチャを適応させる取り組みでは、進化するサイバー脅威に対応するため、セキュリティトランスフォーメーションも必要になります。フォーティネット セキュリティ ファブリックは、プロアクティブで革新的なサイバーセキュリティ対策です（図 1）。セキュリティ ファブリックには、次のような機能があります。

- OT と IT の攻撃対象領域全体を幅広く可視化
- あらゆるデバイス、ネットワーク、アプリケーションを包括的に保護
- AI と機械学習（ML）により、運用と対応を自動化

* OT は、**産業用制御システム（ICS）**と同義です。プロトコル、ベンダー、ユースケースが異なるという理由から、「OT」は IT と対比した用語として使用されています。**SCADA（監視制御・データ収集）**システムは、OT の要素の 1 つです。SCADA システムは、グラフィカルユーザーインタフェースを使用し、OT / ICS プロセスの高度な監視 / 管理を行います。

セキュリティ ファブリックの導入とは、セキュリティ環境で可視化、統合、自動化、耐障害性を望ましいレベルへと引き上げる取り組みです。セキュリティ保護に関する組織の優先順位に沿って、セキュリティ ファブリックを段階的に実装することが可能です。実装計画では、次のベストプラクティスを考慮することをお勧めします。

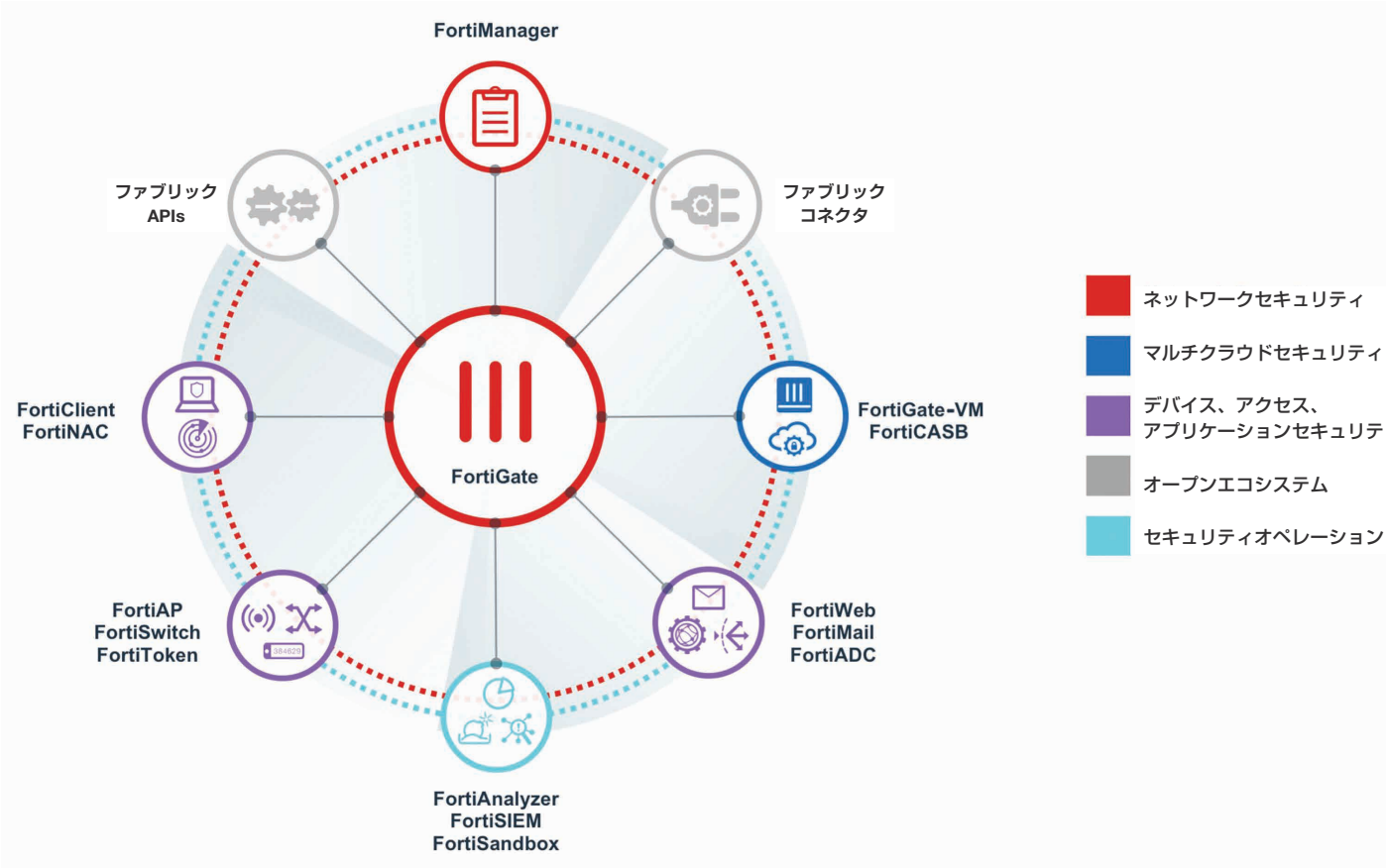

図 1：フォーティネット セキュリティ ファブリックは、IT / OT 環境全体で複数のテクノロジーを連携させます。
単一の脅威インテリジェンスですべてをサポートすることにより、ネットワークに存在するセキュリティギャップを排除し、あらゆる攻撃ベクトルに対抗します。

OT サイバーセキュリティのベストプラクティス

1. 資産の特定、価値の分類、優先順位付け

組織の OT セキュリティ態勢の強化において、CISO が最初に行うべきことは、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把握する作業です。フォーティネットは、条件を満たしたお客様を対象に、サイバー脅威評価プログラムを無償で提供しています[1]。このプログラムでは、まず FortiGate NGFW（次世代ファイアウォール）や FortiNAC（ネットワークアクセス制御）を使用して、ネットワークトラフィックを受動的に観察します。このトラフィック分析で示されるデバイスの特徴や振る舞いから、デバイスを特定およびプロファイリングします。評価レポートでは、次の内容が示されます。

- リスクの高いアプリケーションを提示
- アプリケーション脆弱性の上位のエクスプロイトを検知および特定
- 各資産のリスク値を評価
- マルウェア、ボットネット、侵害の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、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連携し、この情報をもとに最適なセキュリティ計画を立案します。

他の脅威評価は、
リスクの特定と優先順位付けに
役立ちます。

攻撃者がネットワーク内および
ネットワーク間を移動する
能力を制限します。

2. ネットワークのセグメンテーション

上記4つのOTセキュリティ侵害では、攻撃者はIT / OTネットワーク内とおよびIT / OTネットワーク間を水平移動します。この移動を制限できるのが、ネットワークのセグメンテーションです。これは、OT セキュリティ保護における基本的なベストプラクティスであり、ISA / IEC-62443（旧 ISA-99）セキュリティ標準で規定されています[2]。

セグメンテーションとは、ネットワークを複数の機能セグメントに分割することを指し、セグメントは「ゾーン」（サブゾーンやマイクロセグメントを含む）や「導管」（ゾーン間のチャネル）と呼ばれます。**FortiGate ISFW（内部セグメンテーションファイアウォール）**は、ゾーンと導管を定義し、適用します[3]。ここで使用されるのが、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**です。これは、ユーザー、デバイス、アプリケーションの信頼レベルを継続的に監視し、ビジネスの意図（インテント）、振る舞い、リスクに基づいて動的なアクセス制御を行うアプローチです。侵入者による脆弱性の発見や悪用が困難になるため、攻撃対象領域を大幅に縮小できます。

3. 脅威と脆弱性に対するトラフィックの分析と保護

ネットワークトラフィック分析は、脅威を特定および阻止する上で有効な方法です。フォーティネットの管理 / 分析ソリューションは、次のコンポーネントからの情報を統合することで、ネットワークトラフィックを分析します。

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あらゆるものを自動検出し、CMDB（構成管理データベース）を構築します。また、監査可能なトラフィックレコードを構築することで、プロアクティブにリスクを軽減し、法規制やセキュリティ標準のコンプライアンスを実証します。

FortiManager のダッシュボードは、セキュリティ ファブリックの最新のステータスを表示し、SOC（セキュリティオペレーションセンター）チームと NOC（ネットワークオペレーションセンター）チームが利用できる統合ビューを提供します。SOC チームはセキュリティのアラートと問題を確認し、NOC チームはセキュリティインシデントが原因でパフォーマンス低下が発生していないかどうかをチェックできます。また、オペレーションチームは、セキュリティチームが資産の再構成や隔離を要請した場合に、状況を把握しすぐに同意することができます。

FortiAnalyzer は、ログ管理とリアルタイム脅威分析を自動実行します。この処理には、FortiGuard Labs の IOC（侵害指標）サービスが使用されます。世界中の幅広いソースから約 50 万件の IOC パッケージが毎日収集され、有害とされるサーバーとのコミュニケーションを特定する上で役立ちます。また、FortiAnalyzer のリスクスコアリングは、FortiGuard セキュリティレーティングサービスを使用し、組織内での時系列での比較や、同等の組織との比較を行うことができます。

さらにフォーティネットの管理 / 分析ソリューションは、FortiGate NGFW を使用してトラフィックのインスペクションを行い、悪意のあるファイル、アプリケーション、エクスプロイトの対策を講じます。

FortiGate NGFW は、**FortiGuard Industrial Security Services**[4]（FortiGate Enterprise バンドル [5] および 360 バンドル [6] サブスクリプションサービスの一部）を使用してシグネチャを更新し、最も一般的な OT プロトコルの特定と規制、既知の OT 脆弱性の悪用の検出とブロックを行います。OT 環境では、ファームウェアのパッチ適用や更新を行わない状態で機器を連続稼働するため、既知のエクスプロイトのブロックは特に重要です。

脅威を検出してポリシーを適用するために、FortiGate NGFW は暗号化された 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% が暗号化トラフィックに潜伏しています。このような環境では、暗号化トラフィックのインスペクションは絶対条件です [7, 8]。インスペクションがパフォーマンスに大きな影響を与える競合他社のファイアウォールソリューションとは異なり、FortiGate NGFW は SPU（専用設計のセキュリティプロセッサ）を採用することで、パフォーマンス低下を最小限に抑えています。そのため、データセンターやネットワークエッジのいずれにおいても、ファイアウォールインフラストラクチャの改良やアプライアンスの追加は必要ありません。FortiGate NGFW は、暗号化トラフィックのスキャンに関する製品比較において、業界トップの価格性能比を誇ります。回避技術のブロック率 100% も、その実績の 1 つです [9]。

OT プロトコル	
BACnet	MMS
DNP3	Modbus
Elcom	OPC
EtherCAT	PROFINET
EtherNet / IP	S7
HART	SafetyNET
IEC 60870-5-104	Synchrophasor
IEC 60870-6 (TASE.2) / ICCP	MMS
IEC 61850	
LonTalk	

OT アプリケーションとベンダー		
7-Technologies / Schneider Electric	Honeywell	RealFlex
ABB	ICONICS	Rockwell Automation
Advantech	InduSoft	RSLogix
Broadwin	intellicom	Siemens
CitectSCADA	Measuresoft	Sunway
CODESYS	Microsys	TeeChart
Cogent	Moxa	VxWorks
DATAC	PcVue	Wellintech
Eaton	Progea	Yokogawa
GE	QNX	

表 1：FortiGuard 産業用セキュリティサービス

セキュリティ ファブリックでは、他にもトラフィック分析と脅威対策を行う機能が提供されています。

FortiMail メールゲートウェイは、スピアフィッシングなどの脅威を軽減します。スピアフィッシングは、認証情報を窃取する目的でよく悪用される OT セキュリティ侵害であり、このようにメールを悪用した攻撃は今日のマルウェア感染の 3 分の 2 を占めます [10]。また、FortiMail は、未知の不審な脅威を **FortiSandbox** に送信します。サンドボックスは、エンドユーザーにトラフィックを送信する前に、アクションの分析と脅威の特定を行います。FortiSandbox は、エンドポイント、ネットワーク、クラウド展開、ファイル共有といった他のアクセスポイントからも、潜在的な脅威を受信します。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、他のすべてのセキュリティ要素と、脅威インテリジェンスをリアルタイムで自動的に共有します。

FortiDeceptor[11] は、デコイを使用して脅威の対策と分析を行い、情報をセキュリティ ファブリック全体で共有します。**FortiIsolator**[12] は、ブラウザを分離することで、ユーザーのブラウザと Web サイト間に仮想的なエアギャップを作ります。リモートの一時的なコンテナで Web コンテンツを表示し、マルウェア脅威を隔離します。

サイバー攻撃の 50% が、暗号化トラフィックに潜伏しています [13]。

認証情報の窃取は、OT セキュリティ侵害のよくある手口です。多要素認証を採用することで、盗み出された認証情報の悪用は非常に難しくなります。

4. ユーザー / デバイス単位のアクセス制御

セキュリティ ファブリックでは、次の機能を調整することで、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 / デバイスグループを作成し、セキュリティポリシーを適用します。たとえば、ローカルユーザーとリモートユーザーに異なるセキュリティポリシーを適用することが可能です。

FortiAuthenticator は、ユーザーアイデンティティを検証し、ゾーンと導管に対するユーザーアクセスをきめ細かく制御します。ユーザーを識別し、サードパーティシステムからのアクセス許可を問い合わせ、この情報を FortiGate デバイスに送信することで、アイデンティティレベルのポリシー適用を可能にします。

FortiToken は、多要素認証（MFA）によりアイデンティティを検証します。ユーザーの認証情報と、ハードウェア / ソフトウェアトークンや指紋といった生体認証を組み合わせることで、盗み出された認証情報が悪用されるリスクを大幅に減らします。

FortiNAC は、ネットワーク接続デバイスの特性を監視することで、デバイスを認証します。FortiNAC は、プロファイリングしたデバイスに対して、ネットワーク接続の有無、制御方法、アクセスするネットワークセグメントを規定したポリシーを適用します。また、ポートをロックすることで、デバイスやアプリケーションの接続を禁止することも可能です。この場合、デバイスの接続を認証しない限り、ポートにはネットワーク接続できなくなります。これにより、OT ネットワークにデバイスを追加する際に、担当者による事前の許可を要求するポリシーを適用することができます。

FortiClient は、FortiGate NGFW と連携することで、OT 環境にあるエンドポイントデバイスを可視化し、脆弱性アラートをトリガーします。

5. 有線 / 無線アクセスのセキュリティ保護

多くの OT 環境では、有線 / 無線アクセスポイントを経由した攻撃リスクが高まりつつあります。DX も、このリスクを増大させる要因になっています。たとえば、製造工場や倉庫では、無線接続された無人搬送車（AGV）が製品や原材料を運搬しています [14]。Forrester が実施した調査によると、調査に参加したすべての企業において、無線または IoT テクノロジーの導入後に攻撃対象領域が拡大していました。これには、OT ネットワークへの接続も含まれます [15]。

リスクを最小限に抑えるには、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 は、独自のセキュアな暗号化トンネルを使用して、組織全体にわたる **FortiSwitch** と **FortiAP** のポートにファイアウォール機能とポリシーをプッシュします。

また、FortiNAC では、ベンダー 170 社が提供する最大 2,000 のサードパーティ製スイッチと無線 AP の構成作業を一元化できます。

調査対象となった企業はいずれも無線や IoT を導入しており、リスクは格段に高くなっています。

FortiSwitch、FortiAP アクセスポイント、および FortiGate NGFW は耐久性に優れており、衝撃、振動、塵埃、湿度、高温を考慮した設計を採用してオフショアの油田掘削現場、運搬コンテナ、工場といった OT 環境に対応します [16、17、18]。

OT セキュリティの強化

OT テクノロジーが開発されたのは、IT が登場する何十年も前にさかのぼる 20 世紀初頭です。これまで OT ネットワークと IT 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。現在、この 2 つのネットワークは統合され、ビジネス価値を高めています。

一方で、IT と OT の統合は、デジタル攻撃対象領域の拡大へとつながっています。次に示すように、適切な制御とテクノロジーの導入で、CISO は OT 環境を保護できます。

1. 攻撃対象領域を幅広く可視化
2. ネットワークセグメンテーションにより、侵入が及ぼす影響を制限
3. トラフィック分析（暗号化トラフィックや一般的な OT プロトコルを含む）により、脅威に対抗
4. ユーザーとデバイス単位のアクセス制御、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. 有線 / 無線アクセスのセキュリティ保護、単一のインタフェースによる一元管理

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 を介して、IT と OT のセキュリティソリューションを統合します。AI による侵害防止機能、運用 / オーケストレーション / 対応の自動化を特徴とする FortiOS は、攻撃対象領域全体を幅広く可視化します。現状を完全に把握し、セキュリティ対策がもたらすメリットを実現する作業は、組織の優先事項に応じて段階的に進めることができます。その第一歩として、リスクの優先順位付けを行う無料の脅威評価をご利用ください。

[1] 「Know Your Vulnerabilities—Get the Facts About Your Network Security」、フォーティネット、2019 年 3 月 25 日（英語）：
https://www.fortinet.com/offers/cyber-threat-assessment.html

[2] 「ISA Standards: Numerical Order（ISA 標準：番号順）」、国際計測制御学界（ISA: International Society of Automation）、2018 年 1 月 3 日（英語）：
https://www.isa.org/standards-and-publications/isa-standards/find-isa-standards-in-numerical-order/

[3] 「Protecting Your Network from the Inside-Out: Internal Segmentation Firewall (ISFW)」、フォーティネット、2016 年 12 月（英語）：
https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-protecting-your-network-from-the-inside-out.pdf

[4] 「FortiGuard 産業用セキュリティサービス」、フォーティネット：
https://www.fortinet.com/jp/support/support-services/fortiguard-security-subscriptions/industrial-control-systems.html

[5] 「Comprehensive Security with the FortiGate Enterprise Protection Bundle」、フォーティネット、2019 年 1 月 21 日（英語）：
https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-fortigate-enterprise-protection-bundle.pdf

[6] 「360 Protection Bundle: Delivering Real-Time Network Management, Comprehensive Security and Operational Services, and Advanced Support」、フォーティネット、2019 年 3 月 26 日（英語）：https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/02_Collateral/SolutionBrief/sb-360 Protection Bundle.pdf

[7] 「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

[8] 「Study Reveals Hackers Increasingly Use Encryption to Hide Criminal Activity」、Lifeline Data Centers、2019 年 3 月 21 日（英語）：
https://lifelinedatacenters.com/data-center/hackers-use-encryption/

[9] 「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 25 日：https://www.fortinet.com/jp/corporate/about-us/newsroom/press-releases/2018/nss-labs-ngfw-report.html

[10] 「Provide Customers with Advanced Threat Defense Against Email-Based Attacks」David Finger 著、フォーティネット、2018 年 4 月 26 日（英語）：
https://www.fortinet.com/blog/business-and-technology/provide-customers-with-advanced-threat-defense-against-email-bas.html

[11] 「FortiDeceptor Enables a New Breach Protection Approach」、フォーティネット、2019 年 3 月 21 日（英語）：
https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-fortideceptor.pdf

[12] 「FortiIsolator」、フォーティネット、（英語）：https://docs.fortinet.com/product/fortiisolator/1.1

[13] 「Study Reveals Hackers Increasingly Use Encryption to Hide Criminal Activity」、Lifeline Data Centers、2019 年 3 月 21 日（英語）：
https://lifelinedatacenters.com/data-center/hackers-use-encryption/

[14] 「Automated Guided Vehicle Market worth $2.74 billion by 2023」、MarketsandMarkets、2019 年 3 月 27 日（英語）：
https://www.marketsandmarkets.com/PressReleases/automated-guided-vehicle.asp

[15] 「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/WP-Independent-Study-Pinpoints-Significant-Scada-ICS-Cybersecurity-Risks.pdf

[16] 「FortiSwitch Rugged」、フォーティネット：https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/ja_jp/FortiSwitchRugged_DS.pdf

[17] 「Wireless Product Matrix」、Fortinet 222C Wireless AP、2019 年 3 月（英語）：
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Wireless_Product_Matrix.pdf

[18] 「FortiGate Rugged シリーズ」、フォーティネット：https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/ja_jp/FortiGateRugged_DS.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-Section-202001-R1