WHITE PAPER

フォーティネットの製造業向け サイバーセキュリティソリューション

製造業における高度な脅威から IT や OT リソースを 単一のプラットフォームで保護

概要

製造業では高価で洗練された設備を自社の工場で管理しており、設備を稼働させるシステムがインターネットに接続されるケースが増えています。この傾向はサイバーセキュリティに与える影響が重大であり、物理的な安全性や、場合によっては国家の安全保障上の脅威となる可能性もあります。企業は、業務効率、業務の継続性、製品の完全性、コンプライアンスといったビジネス上の重要事項を維持しながら、システムのセキュリティを確保するように努めています。フォーティネット セキュリティ ファブリックは、バックオフィスから製造現場まで、エアギャップのあるシステムから接続されたシステムまで、さらには社内ユーザーからサードパーティパートナーまで、製造業のあらゆる側面をカバーする、幅広い適用領域で（Broad）システム連携し（Integrated）自動化されたセキュリティアーキテクチャを提供します。

昨年は、ほぼすべての ICS / SCADA ベンダーで、エクスプロイトのボリュームと範囲の拡大がみられました [4]。

今日の製造業は、コンバージェンスの時代です。これまで独立して製品を生産していた企業が、現在では、プロセスのさまざまな部分を分担するパートナーのネットワークと緊密に連携しています [1]。また、従来はエアギャップの工場のオペレーションを実行する電子システムは、IT システム、つまりインターネットに接続される事例が増えています。その結果、産業用制御システム（ICS）や SCADA を含むこれらのオペレーショナルテクノロジー（OT）システムが、ますます高度化する脅威にさらされ、テロ、サイバー戦争、スパイ活動に関与するハッカーの標的となっています。

世界中でエアギャップがなくなるにつれて、OT システムは再利用された IT ベースの攻撃と、専用の OT のセキュリティ侵害の両方でますます集中的な攻撃にさらされています [2]。ある調査によると、OT の専門家の 74% が過去 12 ヵ月間にセキュリティ侵害を経験しています [3]。製造業の重要なインフラストラクチャへの攻撃は、金銭的な損失、ブランドの毀損リスク、そして時には人命の喪失や国家安全保障への脅威をもたらす可能性があります。

フォーティネットは 2005 年以来、エネルギー、防衛、製造、食品、輸送などの重要なインフラストラクチャ分野で OT 環境を保護してきました。フォーティネット セキュリティ ファブリックを活用してこれらの複雑なインフラストラクチャに組み込むサイバーセキュリティを設計することで、企業は製造現場からデータセンター、複数のクラウドに至るまで、OT および IT 環境全体にわたるサイバーセキュリティ保護を統合することができます。

製造業におけるサイバーセキュリティの主な課題

工場、従業員、地域社会の安全

製造施設には、故障したり正しく動作しなかったりした場合に、人身事故や死亡事故を引き起こす可能性のある機械が設置されています。現在の企業を取り巻くサイバー脅威は、サイバー物理攻撃によって業務を妨害しようとする攻撃者が、現場の従業員だけでなく、近隣の住民や通行人にも安全上のリスクをもたらす可能性があります [5]。加えて、そのような攻撃の結果、工場で生産される製品の安全性に影響が及んでしまい、広い地域にリスクを拡大してしまう可能性もあります。

ほとんどの組織では、IT、OT、物理的セキュリティのシステムがサイロ化されているのが通常であり、これでは問題は解決しません。データセンター、複数のクラウド、エッジの間で IT セキュリティアーキテクチャを統合するだけでも大変なことです。しかし、敵がサイバー攻撃と物理攻撃を同時に行うことができる時代にあっては、セキュリティのすべての要素を統合し、一元的に可視化することが人命を守るための唯一の実行可能な方法かもしれません。

生産性とアップタイム

予期しない業務の中断は、メーカーにとって多大なコストとなり、その中断によって問題が流通チャネルやサプライチェーン上に連鎖する可能性があります。残念ながら、製造業を狙うサイバー攻撃の多くは、まさにそのような混乱を引き起こすことを目的としています。侵入した後にネットワーク内を水平方向に移動しようとする攻撃もありますが、それでも業務に影響を与える可能性があります。

OT システムは、歴史的にエアギャップであることが多く、システムの更新頻度も低いため、IT システムと比較してサイバーセキュリティ保護が洗練されていないことが多いのです。その結果、比較的侵入しやすいという前提のもとで、サイバー犯罪者の標的にされることが多くなります [6]。エアギャップの OT システムであっても、メーカーのソフトウェアアップデートをインストール前に感染させることでシステムに侵入できます。

業務の効率

さまざまなセキュリティツールが統合されていないためにセキュリティ業務が分断されていると、業務の非効率性が必然的に高まることになります。統合されていないと、異なるシステムから取得したログレポートの相関関係を調べたり、コンプライアンスレポートを作成したりするような手作業が発生してしまい、サイバーセキュリティ専門家の作業時間が無駄になり、より戦略的な業務が疎かになってしまいます。

アーキテクチャがサイロ化されるにつれて、アプリケーションの管理にも冗長性が生まれてしまいます。ポイント製品が多数存在すると、すでに過労を強いられているサイバーセキュリティチームに、特定の製品のスキルがより多く求められてしまいます。また、ソフトウェアやハードウェアのライセンスコストが高くなり、スタッフにとってみれば複数のライセンスを管理するための余分な時間が必要になります。これらの要因により、全体的なオペレーションコストが大幅に増加します。

カスタマーエクスペリエンス

消費者向けの製品であれ、企業向けの製品であれ、メーカーは現在、Web 上のプレゼンスに加えてソーシャルメディアやその他のエンゲージメントツールを並行して使用し、ターゲットを絞った方法で顧客との関わりを持つことが日常的になっています。しかし、このような正当な努力は、ソーシャルネットワークを操作して利益を得ようとするサイバー犯罪者によって打ち消される可能性があります。ある調査によると、世界のソーシャルメディアのアカウントの半分以上が不正なものであるという結果が出ています [7]。

購入サイクルの初期段階にある潜在顧客から得たデータが失われると、企業の評判に壊滅的な影響が及んでしまう可能性があるため、Web プロパティやソーシャルメディア上での交流を保護することは、メーカーにとって最も重要です。Web サイトのダウンタイム、生産停止による製品の一時的な入手不能など、その他の要因もカスタマーエクスペリエンスに悪影響を及ぼします。

製品の信頼性

製品の品質低下は、それがたとえ一時的なものであっても、ブランドの評判を悪化させます。たとえば、食品加工業者の OT システムがサイバー攻撃を受け、温度や調理時間がわずかに変化しただけで、製品が腐敗してしまったり、品質が低下してしまったりする可能性があります。製品によっては、お客様の身体の健康や安全にも影響が及んでしまうことがあります。

コンプライアンス

どのような商品を作っているかによって、メーカーはさまざまな規制や基準の対象となります。コンプライアンス違反に対する罰則は時に高額になりますが、違反してしまったが故にブランドの評判が低下してしまった結果、罰則自体よりもさらに高いコストが発生してしまうことがよくあります [8]。

企業は、複数の規制や基準に準拠していることを証明できなければなりませんが、そのためには、スタッフを戦略的な取り組みから監査報告書の作成に再配置する必要があります。これにより、スタッフの貴重な時間が無駄になり、報告書の作成時において人為的ミスにつながる可能性が高まることになります。細分化されたサイバーセキュリティインフラストラクチャでは、ほとんどの場合、監査報告書を作成するためにデータを手動で相関させる必要があります。

「サイバー物理攻撃は、ここ数年、深刻な脅威として注目されてきました。しかし、近年、これらの攻撃は理論上のものから現実の世界へと忍び寄っています」[9]

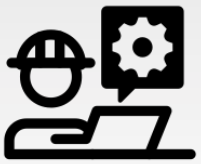
ソーシャルメディアサイトへのログインの 53%、新規アカウント申請の 25% が不正行為によるものです [10]。

ユースケース

フォーティネットのソリューションによって、メーカーが解決できる主なユースケースは以下のとおりです。

企業インフラストラクチャ

メーカーは、製造現場が生産の中心ではあるのですが、他の業界の組織と同様、企業 IT のニーズを抱えています。この企業 IT ネットワークには、財務、知的財産、人事、製品サポート、フィールドサポートなどに関連する重要なデータが格納されています。他の業界と同様に、メーカーでもクラウドベースのアプリケーションやインフラへの依存度が高まっており [11]、ネットワークエッジではモノのインターネット（IoT）デバイスが増加しています [12]。



SCADA / ICS オペレーターの 45% がロールベースのアクセス制御を使用していません [14]。

そこにどのような機密データが格納されているにせよ、企業のインフラストラクチャには、エンドツーエンドで統合された広範かつ自動化されたサイバーセキュリティソリューションが必要です。フォーティネット セキュリティ ファブリックは、FortiGate 次世代ファイアウォール（NGFW）と FortiGuard Labs が提供する人工知能（AI）を活用した脅威インテリジェンスを基盤としており、まさにそのようなソリューションを提供しています。セキュリティ ファブリックには、ファブリックパートナーが提供する多数のサードパーティソリューションとともに、さまざまなフォーティネットサイバーセキュリティツールがシームレスに統合されています。また、オープンなエコシステムと広範なアプリケーションプログラミングインタフェース（API）ツールにより、他のサードパーティツールの統合も可能です。

エアギャップの製造システム

現在、OT システムの大半は IT システムに接続されていますが、Forrester の最近の調査によると、OT システムの 40% は未だにエアギャップ（他のネットワークに接続されていない状態）であることが判明しました [13]。このようなシステムはサイバー攻撃に対して安全であると思われるかもしれませんが、IP ベースの制御システムを使用していることには変わりなく、管理者はメーカーが提供するソフトウェアの更新をインストールしています。これにより、敵対者がベンダーのネットワークを介して更新プログラムを感染させることで、システムに侵入する隙が生まれてしまいます。また、エアギャップシステムには機密データは含まれていないかもしれませんが、侵入されることで、コストのかかる混乱や安全上の問題が発生する可能性があります。

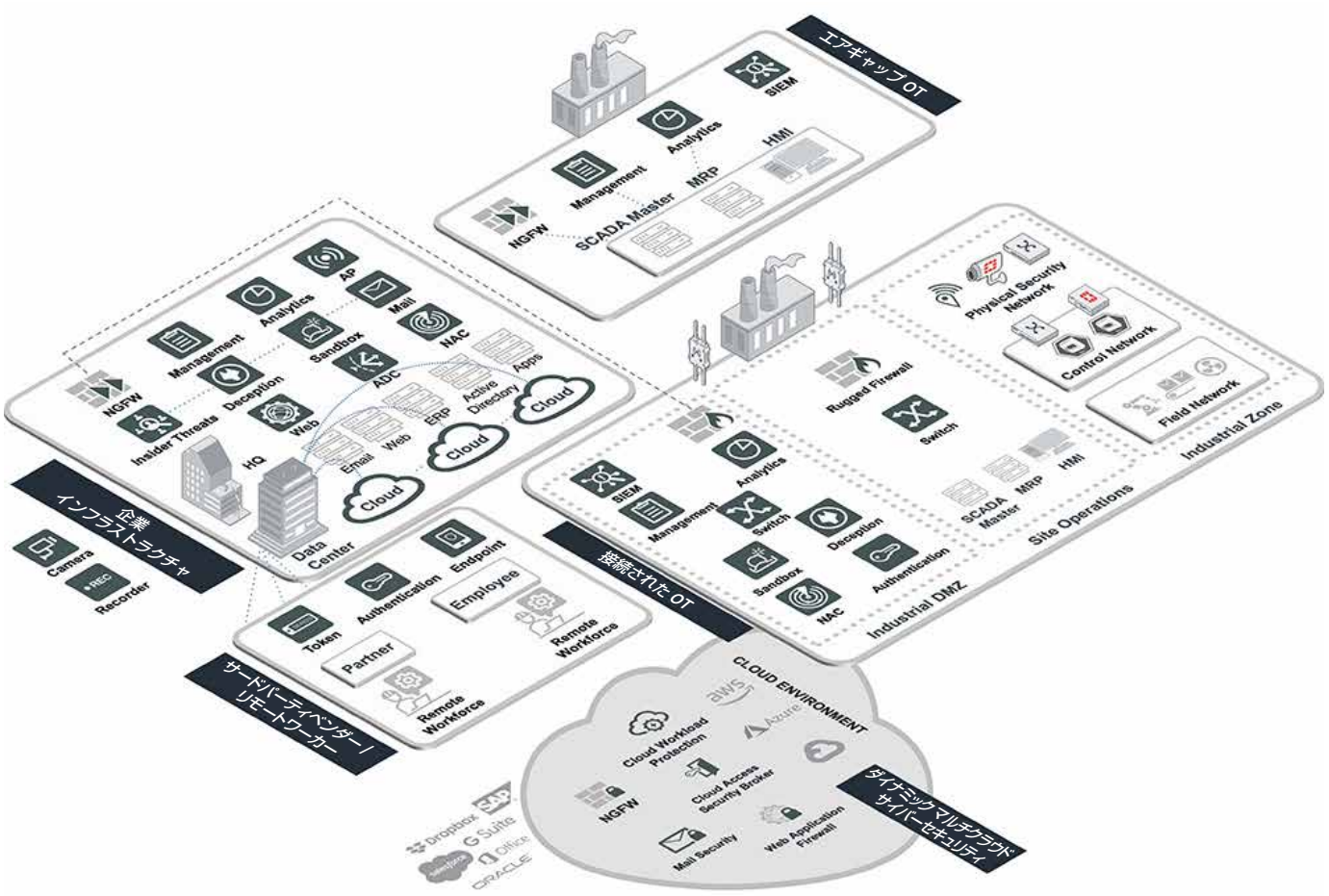
そのため、エアギャップシステムであっても NGFW による保護が必要であり、これに加えてサイバーセキュリティに関する包括的な追跡調査と報告が必要となります。FortiGate NGFW は、暗号化されたトラフィックと暗号化されていないトラフィックの両方を検査する際に、堅牢な保護と業界トップクラスのパフォーマンスを提供します。FortiManager は、単一画面による管理と、さまざまなレポートツールを提供します。FortiAnalyzer は、分析機能を備えたサイバーセキュリティとログ管理機能を提供し、可視性を最大限に高め、情報漏えいの検知を強化します。FortiSIEM サイバーセキュリティ情報とイベント管理ツールを使用することで、攻撃に対する協調的かつ自動化されたレスポンスが可能になります。

接続された製造システム

これまで述べてきたように、デジタルトランスフォーメーションとビジネスアジリティの必要性により、IT と OT の相互依存性が高まっています。製造工程を監視する産業用 IoT センサーから、意思決定を容易にするためにインターネットから公開データを取得するシステムに至るまで、OT システムの孤立が進んでいます。サイバーセキュリティの観点から見ると、このコンバージェンスの主な結果として、攻撃対象領域が大幅に拡大しています。また、OT システムには一貫したパッチが適用されないことが多く、サイバーセキュリティの保護が弱体化しているため、短期的には組織にとってリスクとなります。

しかし、サイバーセキュリティの問題を解決できれば、IT ネットワークと自動化ネットワークを安全で管理しやすい単一の環境に統合できる可能性が大きくなります。サイバーセキュリティチームは、すべてのシステムを一元的に把握し、ビジネスニーズに応じてネットワークをセグメント化し、有線ネットワークと無線ネットワークの両方を一元的に管理できる必要があります。

フォーティネット セキュリティ ファブリックは、攻撃対象領域をすべてカバーしており、ネットワーク上の誰が何をしているのかを幅広く可視化します。また、セキュリティ ファブリックは、各システムを統合的に制御することで、本来の役割を確実に果たせるようにします。さらに、インテリジェントなセグメンテーションが可能になり、管理性が向上し、既知および未知の脅威を自動的に認識できます。セキュリティ ファブリックは、FortiGate NGFW と、FortiGuard Labs が提供する AI を利用した脅威インテリジェンスを基盤に構築されており、フォーティネットとそのファブリックパートナーが提供する数十種類のサイバーセキュリティツールとのシームレスな統合を実現します。



フォーティネットの製造業向けサイバーセキュリティソリューションを利用することで、企業は IT、OT、物理的セキュリティにまたがるエンドツーエンドの統合セキュリティアーキテクチャを構築し、社内ユーザーやサードパーティパートナーのユーザーを対象にしながら、本社から製造工場までをカバーできます。

サードパーティベンダーの管理

業界が MaaS（Manufacturing-as-a-Service）モデルへと移行する中で [15]、サードパーティが企業ネットワークや OT システムにアクセスする機会がこれまで以上に増えています。これにより、信頼できるユーザーという概念が複雑になり、企業はサードパーティを含む内部の者による脅威に対する保護を継続的に評価する必要があります。定期的な調査を通じて、各パートナーのサイバーセキュリティ態勢を把握することが重要です。また、組織では、内部の者による脅威に対しては、それが偶発的なものであるか、悪意のあるものであるか、さらには、それが社内からの脅威であるか、パートナーネットワークの要素からの脅威であるかにかかわらず、強固な保護が必要です。

フォーティネット セキュリティ ファブリックの統合ソリューションは、これらの脅威に対する多層的な防御を実現します。FortiGate NGFW に搭載されているインテントベースのセグメンテーション機能により、絶えず変化する信頼性の世界において、組織はネットワークをインテリジェントにセグメント化できます。FortiAuthenticator アイデンティティおよびアクセス管理ソリューションと FortiToken トークンは、このセグメンテーションを活用して、必要に応じてユーザーにアクセスを許可します。FortiInsight は、ユーザー / エンティティ振る舞い分析（UEBA）を使用して、信頼されているユーザーやエンティティの予期される行動の異常を特定します。この異常は、アカウントが侵害されていることを示す可能性があります。さらに FortiDeceptor は、ディセプション技術を用いて、内部および外部から発信される攻撃を欺き、暴露し、排除します。

マルチクラウドサイバーセキュリティ

メーカーではクラウドベースのサービスの採用が急ピッチで進んでいます [16]。現在では、多くの企業がクラウドベースの製造資源計画（MRP）システムとエンタープライズリソースプランニング（ERP）システムを導入しています。これらのシステムは、迅速かつ効果的な意思決定を行うために、IT と OT の両方のシステムからデータを取り込むことが多く、このプロセスは「デジタルツイン」と呼ばれています。また、クラウドベースのソリューションは、カスタマーエクスペリエンスに影響を与えるサービスにも日常的に使用されています。これらのアセットのサイバーセキュリティを保護することは非常に重要であり、組織の統合されたサイバーセキュリティアーキテクチャは、データセンターから OT システム、複数のクラウドに至るまで拡張する必要があります。

フォーティネット セキュリティ ファブリックは、マルチクラウド環境における包括的な保護を可能にし、攻撃対象全体にわたって一貫したポリシー管理、設定管理、脅威の検知とレスポンスを実現します。FortiGate VM は、NGFW をクラウド環境と相性の良い仮想マシンに搭載し、複数のフォームファクタで提供される FortiWeb Web アプリケーションファイアウォール（WAF）は、インラインで AI を活用した脅威インテリジェンスによってアプリケーション層を保護します。

FortiCASB クラウドアクセスセキュリティブローカー（CASB）サービスは、包括的なレポートツールを使用して、クラウドに保存されているリソース、ユーザー、行動、データに関するインサイトを提供します。これにより、高度なポリシー制御を IaaS（Infrastructure-as-a-Service）リソースや SaaS（Software-as-a-Service）アプリケーションに拡張できます。サイバーセキュリティチームと DevOps チームは、FortiCWP クラウドワークロード保護（CWP）ツールを使用して、クラウド構成のサイバーセキュリティ態勢を評価し、設定ミスに起因する潜在的な脅威を特定できます。

フォーティネットの差別化要因

製造業のサイバーセキュリティにおけるフォーティネットの差別化要因

フォーティネットのソリューションは、製造業におけるさまざまな OT ネットワークや IT ネットワークのすべてを保護する能力を提供します。主な差別化要因は以下のとおりです。

- **統合**
  フォーティネットのテクノロジーは、IT と OT、サイバーセキュリティと物理的セキュリティ、工場と本社、データセンター、複数のクラウドをカバーするエンドツーエンドの統合サイバーセキュリティアーキテクチャをメーカーに提供します。これにより、正真正銘のセキュリティの自動化が可能になり、保護から検知、レスポンスまでの連携したワークフローが実現します。
- **監視と管理**
  メーカーは、フォーティネットを利用することで、ネットワーク、サイバーセキュリティ、監視機能を一元的なシステムに統合し、1 つの画面で完全な可視性と制御を実現できます。これにより、サイバー物理攻撃を防ぎ、異なるチーム間のサイロを排除することができます。
- **堅牢なハードウェア**
  製造現場では、ハードウェアは過酷な状況に置かれることが多く、ファイアウォール機器が物理的に破損すると、工場の操業停止につながることが多々あります。フォーティネットは、あらゆる環境のニーズに対応し、ビジネスの継続をサポートする耐久性に優れたアプライアンスを幅広く取り揃えています。
- **内部の者による脅威に対するプロアクティブな保護**
  サードパーティのサプライヤーやパートナーがネットワークにアクセスする機会が増えるにつれ、内部の者による脅威に関連するリスク管理はより複雑になります。フォーティネットは、インテントベースのセグメンテーション、ディセプター技術、UEBA など、内部の者による脅威を防御するための包括的なソリューションを提供しています。

製造業で実際にあった侵入事例 [17]（過去 12 ヵ月間）

- マルウェア：61%
- スパイウェア：45%
- DDoS：28%
- 内部の者による脅威：26%
- フィッシング：24%
- モバイル：21%
- ランサムウェア：21%
- 中間者攻撃：18%
- ゼロデイ攻撃：17%
- SQL インジェクション：8%

製造業における侵入の影響 [17]（過去 12 ヵ月間）

- 45% が生産性に影響を与えるような業務の停止を経験
- 40% がブランド認知度の低下を経験
- 35% が物理的な安全性が脅かされるような業務上の障害を経験
- 32% が業務停止による収益への影響を経験
- 26% がビジネスクリティカルなデータを損失

- **OT に特化した脅威インテリジェンス**
  FortiGuard Labs は、OT システムに特化した強固な脅威インテリジェンスを提供し、メーカーがより優れた戦略的意思決定を行えるように支援します。フォーティネットは 15 年にわたり、製造業のお客様と密接に協力してきました。
- **セキュリティ ファブリックのエコシステム**
  専門の OT ソリューションは、フォーティネットのセキュリティツールの幅広いポートフォリオに加え、フォーティネット ファブリック パートナーのエコシステムを通じて、フォーティネット セキュリティ ファブリックとシームレスに統合できます。これにより、データを 1 つの画面に合理化し、情報に基づいた意思決定を行うことができます。

終わりに

ジャストインタイムでの生産が求められる急激に進化する市場において、メーカーはサイバーセキュリティイベントやその防止策に振り回されている余裕はありません。フォーティネット セキュリティ ファブリックは、IT、OT、物理的セキュリティを保護するための統合プラットフォームであり、1 つの画面で広範な可視性を提供し、統合された制御が可能になります。

「CEO や経営陣の間で意見が一致しているのは、市場投入までの時間を短縮し、製品の品質を向上させ、顧客の声に耳を傾けることを目的とした戦略が功を奏しているという事実です」[18]

「季節変動やターゲットの多様性にかかわらず、データに関しては明確なのは、OT システムに対する IT ベースの攻撃が増加していることです」[19]

[1] 「Manufacturing-As-A-Service Platforms: The New Efficiency Revolution」、Marco Annunziata 著、Forbes、2019 年 5 月 13 日（英語）：https://www.forbes.com/sites/marcoannunziata/2019/05/13/manufacturing-as-a-service-platforms-the-new-efficiency-revolution/#ce9199157fdb

[2] 「Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems」、Fortinet、2019 年 5 月 8 日（英語）：https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-security-trends.pdf

[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

[4] 「Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems」、Fortinet、2019 年 5 月 8 日（英語）：https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-security-trends.pdf

[5] 「Cyber Physical Systems Security」、Department of Homeland Security、2019 年 11 月 7 日（英語）：https://www.dhs.gov/science-and-technology/cpssec

[6] 「Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems」、Fortinet、2019 年 5 月 8 日（英語）：https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-security-trends.pdf

[7] 「Q3 Fraud and Abuse Report」、Arkose Labs、2019 年 9 月 18 日（英語）：https://www.arkoselabs.com/blog/q3-fraud-report

[8] 「Ninth Annual Cost of Cybercrime Study」、Accenture and Ponemon Institute、2019 年 3 月 6 日（英語）：https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

[9] 「Six Cyber-Physical Attacks the World Could Live Without」、Elizabeth Montalbano 著、The Security Ledger、2017 年 1 月 18 日（英語）：https://securityledger.com/2017/01/six-cyber-physical-attacks-the-world-could-live-without/

[10] 「Q3 Fraud and Abuse Report」、Arkose Labs、2019 年 9 月 18 日（英語）：https://www.arkoselabs.com/blog/q3-fraud-report

[11] 「10 Ways Cloud Computing Will Drive Manufacturing Growth In 2018」、Louis Columbus 著、Manufacturing Business Technology、2018 年 2 月 23 日（英語）：https://www.mbtmag.com/cloud-computing/article/13228168/10-ways-cloud-computing-will-drive-manufacturing-growth-in-2018

[12] 「Applications of IoT in Manufacturing Plants」、The Manufacturer、2018 年 4 月 12 日（英語）：https://www.themanufacturer.com/articles/applications-iot-manufacturing-plants/

[13] 「Independent Study Pinpoints Significant SCADA/ICS Security Risks」、Fortinet、2019 年 4 月 16 日（英語）：https://ready.fortinet.com/expanding-attack-surface/independent-study-pinpoints-significant-scada-ics-cybersecurity-risks-2

[14] 同上

[15] 「Manufacturing-As-A-Service Platforms: The New Efficiency Revolution」、Marco Annunziata 著、Forbes、2019 年 5 月 13 日（英語）：https://www.forbes.com/sites/marcoannunziata/2019/05/13/manufacturing-as-a-service-platforms-the-new-efficiency-revolution/#5af6f6cb57fd

[16] 「10 Ways Cloud Computing Will Drive Manufacturing Growth In 2018」、Louis Columbus 著、Manufacturing Business Technology、2018 年 2 月 23 日（英語）：https://www.mbtmag.com/cloud-computing/article/13228168/10-ways-cloud-computing-will-drive-manufacturing-growth-in-2018

[17] フォーティネットが実施した異なる役割を対象とした一連の調査研究に基づいています。 調査レポートは近日中に公開予定です。

[18] 「10 Ways Cloud Computing Will Drive Manufacturing Growth In 2018」、Louis Columbus 著、Manufacturing Business Technology、2018 年 2 月 23 日（英語）：https://www.mbtmag.com/cloud-computing/article/13228168/10-ways-cloud-computing-will-drive-manufacturing-growth-in-2018

[19] 「Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems」、Fortinet、2019 年 5 月 8 日（英語）：https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-security-trends.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

Copyright© 2021 Fortinet, Inc. All rights reserved. この文書のいかなる部分も、いかなる方法によっても複製、または電子媒体に複写することを禁じます。この文書に記載されている仕様は、予告なしに変更されることがあります。この文書に含まれている情報の正確性および信頼性には万全を期しておりますが、Fortinet, Inc. は、いかなる利用についても一切の責任を負わないものとします。Fortinet®、FortiGate®、FortiCare®、および FortiGuard® は Fortinet, Inc. の登録商標です。その他記載されているフォーティネット製品はフォーティネットの商標です。その他の製品または社名は各社の商標です。