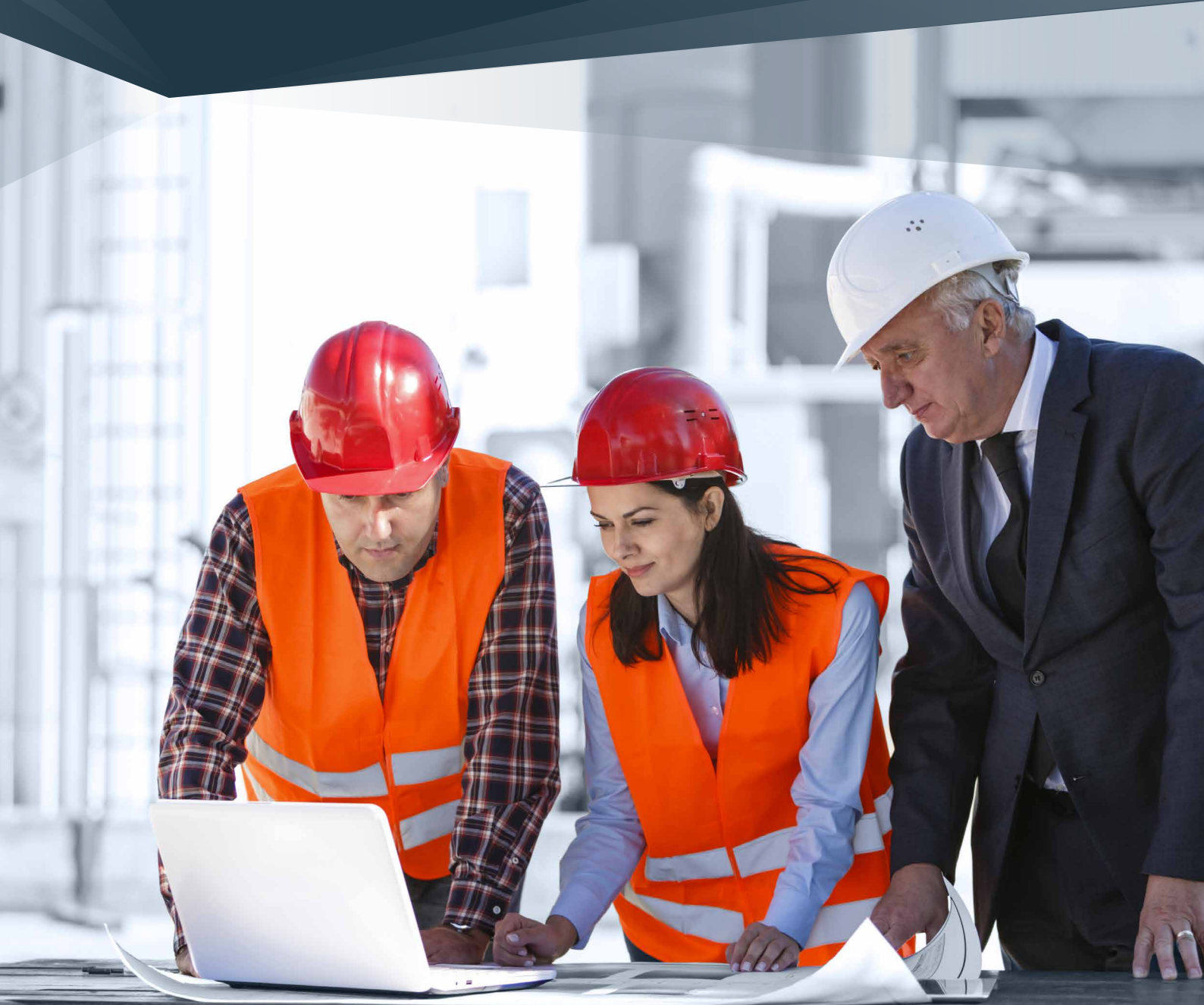
WHITE PAPER

フォーティネット セキュリティ ファブリックで 電力 / 公益事業分野を保護する



概要

OT（運用テクノロジー）と IT（情報テクノロジー）がともに抱える重大な脆弱性に対処するために、電力 / 公益事業分野はその両方を効率的に保護できる詳細な防御戦略の採用が必須となります。このニーズに応えるのが、フォーティネット セキュリティ ファブリックです。セキュリティ ファブリックは、発電、送電、配電、企業インフラストラクチャ、顧客エクスペリエンスにおけるセキュリティのニーズに統合型で自動化された脅威保護を提供します。

CEO の 48% が、重要なインフラストラクチャへの攻撃対策が急務だと述べています [1]。

IT との統合が OT リスクを高める

電力 / 公益事業分野は、重要なインフラストラクチャの近代化を進める際に、OT および IT ネットワークを統合して運用効率を高めています。ところが、これによって IT と OT の間にあったエアギャップと呼ばれる物理的に分離された状態が解消され、サイバー犯罪者にとって絶好の攻撃のチャンスが生まれました。最近の調査によると、電力 / 公益業界は米国で最も攻撃の標的になりやすい分野のトップ 3 に入っていることがわかっています [2]。欧州、オーストラリア、日本といった地域にも同様の傾向があり、電力 / 公益事業分野の重要なインフラストラクチャに対する脅威は飛躍的に増大しています。

その要因の 1 つが、重要なインフラストラクチャを制御する OT ネットワークの近代化です。IT ネットワークやパブリックインターネットから OT システムを隔離していたエアギャップがなくなった結果、悪意のある攻撃だけでなく、善意からの行為または偶発的な誤りに起因するリスクは、これまで以上に大きくなっています。

電力 / 公益事業分野が直面する主なセキュリティ課題

電力会社 ./ 公益事業会社のシステムを標的にした攻撃は、デジタル的な影響と物理的な影響を及ぼします。十分に保護されていない電子通信は、機密性の高い企業情報や顧客の個人情報をリスクにさらします。また、サイバー攻撃によるサービス中断はプロバイダーに金銭的被害をもたらし、プロバイダーのインフラストラクチャを利用する顧客にもより深刻な影響が及ぶ恐れがあります。ネットワークで実施される業務が妨害されると、オンサイトの従業員や近隣住民にも物理的な影響が及びます。このようなタイプの攻撃に対抗できなければ、風評被害だけでなく業界で施行されるさまざまな法規制に違反することになり、罰金が科せられる可能性もあります。

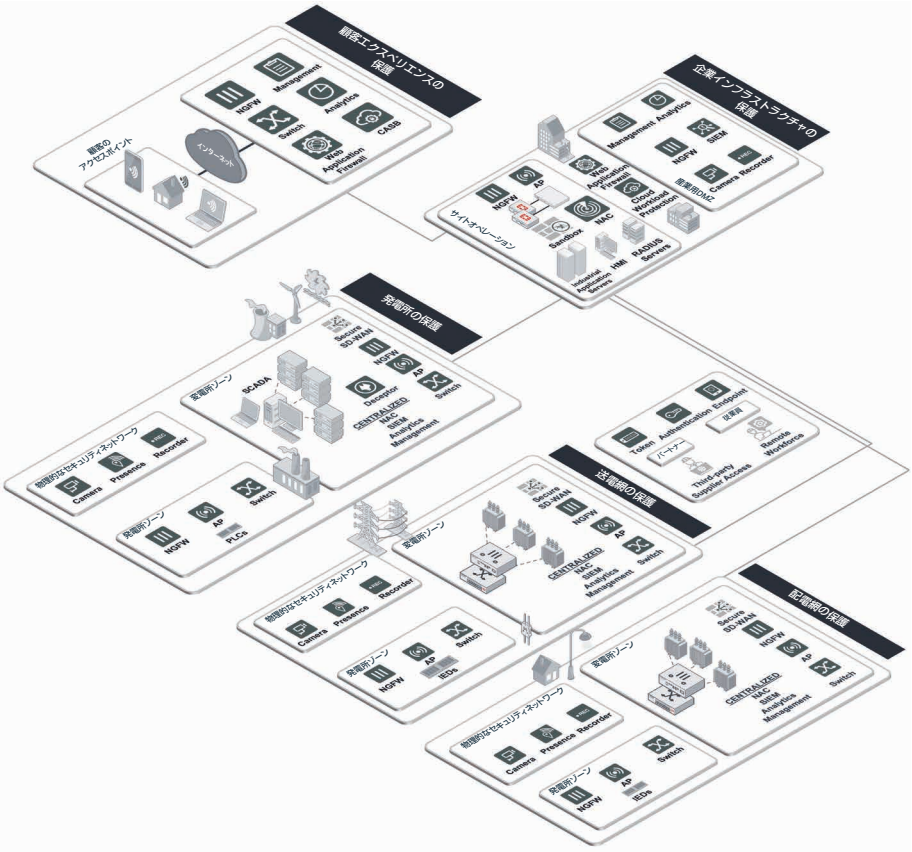


図 1. サイバー攻撃や内部の脅威から電力 / 公益事業分野を保護するには、幅広い攻撃対象領域を包括的に保護するセキュリティアプローチが必要です。

電力 / 公益事業分野のネットワークをサイバー攻撃から保護する取り組みは、太陽光発電や風力発電といった新たなタイプの電力が登場したことでますます複雑になっています。ネットワーク全体の一元的な可視化およびリスク管理ができないため、セキュリティのワークフローやコンプライアンスレポート作成を手作業で管理しなければならず、運用効率は低下してしまいます。このような非効率なオペレーションによって、脅威の検知や対応の遅れに加え、(オペレーションの) ムダを招き OpEx (運用コスト) の増加をもたらします。

OT 組織のおよそ 4 分の 3 (74%) が、過去 12 ヵ月の間にセキュリティ侵害を経験しています。これは、生産性の低下、売上喪失、ブランドの信頼性低下、知的財産の侵害、物理的な安全性の低下を引き起こしています [3]。

電力 / 公益事業分野のサイバーセキュリティのユースケース

企業 IT インフラストラクチャ

電力 / 公益事業分野のインフラストラクチャは、分散したプラントや施設の運用に不可欠な IT ネットワークサービスで構成されています。企業ネットワークインフラストラクチャは、ERP (エンタープライズリソースプランニング)、財務、人事といった重要なビジネスアプリケーションをサポートします。また、施設、運用、サプライヤー、顧客に関する機密データを保管する場でもあります。このようなデータには、サイバー攻撃に対して特に脆弱なセンサーや IoT (モノのインターネット) デバイスから送信される情報も含まれています。

このように分散したネットワーク資産の保護を目的に、フォーティネット セキュリティ ファブリックは幅広いモデルの FortiGate NGFW (次世代ファイアウォール) を活用して高度な脅威保護を提供します。優れたパフォーマンスを特徴とする NGFW は、企業データセンターや WAN (ワイドエリアネットワーク) エッジ、さらにはさまざまな現場サイトに導入できます。また、FortiGate NGFW の仮想アプライアンスは、企業が使用するあらゆるパブリッククラウドやプライベートクラウドに導入することが可能です。いずれの FortiGate NGFW も、ネットワークスピードとほぼ同じ速度でトラフィック (暗号化パケットも含む) インスペクションを実行し、アプリケーションとインタフェースを既知の脅威やゼロデイ脅威から保護します。さらに、SD-WAN (ソフトウェア制御によるワイドエリアネットワーキング) などの重要なネットワーク機能を安全に実行することも可能です。

FortiSwitch セキュアアクセススイッチを使用することで、こういったネットワーク保護機能を FortiAP 無線アクセスポイントまで拡張することができます。インターネットや企業ネットワークへの接続を提供するアクセスポイントは、侵入阻止対策の最前線としても機能します。FortiGate NGFW で複数の SSID (サービスセット識別子) を設定すれば、複数のユーザーグループ (従業員、顧客、契約社員など) 各々に異なるサービスや権限を提供することが可能になります。FortiAP アクセスポイントを介してユーザーがネットワークにログインすると、適切なファイアウォールポリシーと認証メカニズムが自動的に適用されます。また、FortiSIEM のセキュリティ情報およびイベント管理機能は、攻撃へのレスポンスと修復を自動実行してセキュリティ侵害を未然に防ぎます。高度な脅威検知を実現する FortiSandbox は、未知の脅威への対策とデータ喪失の防止に役立ちます。

スタッフ不足に悩むセキュリティチームであっても、一元管理 / ワークフロー自動化を実現する FortiManager を導入することで FortiGate NGFW の導入環境全体を 1 つのダッシュボードから管理できます。社内のステークホルダーやコンプライアンス監査向けのレポート作成においては、FortiAnalyzer を活用できます。このログ作成 / レポーティングを一元化するソリューションを活用することで必要なレポートを短時間で作成可能となり、スタッフはネットワーク管理やセキュリティ管理に集中できるようになります。

クラウドインフラストラクチャとサービスを使用する環境では、FortiCASB クラウドアクセスセキュリティブローカー (CASB)、FortiWeb Web アプリケーションファイアウォール (WAF)、FortiCWP クラウドワークロード保護 (CWP) が能力を発揮し、複数のクラウドを隔てるサイロの解消と一元的なポリシー管理を可能にします。FortiCASB は、SaaS (サービスとしてのソフトウェア) のアクティビティと構成をすべて監視します。FortiCWP は、コンプライアンスややインシデントのレポーティングをはじめ、複数のクラウドリソース上で行われるアクティビティと構成を監視します。FortiWeb は、既知と未知の脆弱性を狙ったサイバー攻撃からビジネスクリティカルな Web アプリケーションを保護します。

セキュリティチームは、ネットワークアクセス制御を実現する FortiNAC を活用してネットワーク上のデバイスを容易に可視化し、ユーザーデバイスに適切なアクセス権を設定できるようになります。また、FortiAuthenticator によるユーザーアイデンティティ管理、FortiToken を使った二要素認証の適用も可能です。企業ネットワークでは、セキュリティイベントおよびオンプレミスで発生する物理的なアクティビティを関連付けて管理しなければならないケースが多々あります。このニーズに対応するため、フォーティネット セキュリティ ファブリックは FortiCamera および FortiRecorder によるネットワークビデオセキュリティを活用し、企業内施設の重要な出入り口や境界周辺を監視することができます。

発電所の保護

発電所を狙ったサイバー攻撃はサービス中断の原因となり、重大な物理的および経済的な被害につながりかねません。管理者は、このような設備のネットワークでも企業オフィスと同様にフォーティネット セキュリティ ファブリック ソリューションを活用できますが、OT が圧倒的多数であるという点が異なります。OT には無数の脆弱なヘッドレスデバイス、そして巧妙な攻撃者の標的となる重要なインフラストラクチャ機器が含まれます。また、発電所の周辺や施設内では契約社員や非正規社員も働いています。

このような環境ではいくつかのセキュリティ要件を満たす必要がありますが、そのようなニーズに応えるのがフォーティネット セキュリティ ファブリックです。

北東部の州にある公益企業では、システムへの侵入やセキュリティ侵害を試みるアクセスが毎日 100 万件も発生しています [4]。

さまざまな OT および IT デバイスにセキュリティ ドリブンの接続を提供：FortiGate NGFW は、OT ネットワーク内でインテント ベースト セグメンテーションを実現し、OT ネットワーク上のアプリケーションとプロトコルを可視化します。FortiGate 内で有効化されたセキュア SD-WAN は、ビジネストラフィックに優先順位を付けることでネットワーク接続のパフォーマンスを高めます。FortiSwitch セキュアアクセススイッチと FortiAP アクセスポイントは、前述の保護機能をネットワークインフラストラクチャの他の領域まで拡張します。

承認済ユーザーの業務を妨げないネットワークアクセス制御：ネットワークアクセスを制御するには、認証と承認の最適なオーケストレ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、ユーザーアイデンティティ管理（FortiAuthenticator）、二要素認証（FortiToken）、そしてネットワークアクセス制御（FortiNAC）によるトップクラスの機能をシームレスに統合します。特に、ネットワークアクセス制御は OT デバイスの監査で重要な役割を果たし、脆弱な機器のアップグレードや入替えに関する生産的な意思決定に役立ちます。

発電所全体でユーザーのアクティビティと位置を監視：発電所のセキュリティ担当者は、FortiPresence の Wi-Fi プレゼンス分析機能を活用してネットワーク上のスマートフォンなどのモバイルデバイスを追跡し、その移動状況を分析することが可能です。また、FortiCamera および FortiRecorder によるネットワークベースのビデオセキュリティは、顔認識機能を活用して制限区域に立ち入ろうとする従業員や契約社員、ベンダーに関して管理者に警告します。

発電所で発生するセキュリティイベントに対する迅速かつ適切なレスポンス：FortiSIEM は、レスポンスと修復を自動化してセキュリティ侵害の検知機能を改善します。FortiSandbox の高度な脅威検知機能との連携によって、未知の脅威対策が可能になります。また、FortiDeceptor の自動ディセプションテクノロジーは、自らをおとりに偽装してネットワーク内外の脅威を検知し、修復します。FortiManager は管理を一元化し、FortiAnalzyer は自動レポーティング機能によって侵害防止対策を強化します。

供給網の保護

公益事業の供給インフラストラクチャには、高電圧線、ガスや上下水管などがあり、その制御を行う変電所などの分局施設にはスタッフが常駐しているとは限りません。このため、物理的な不正行為に対して脆弱です。また、このような分局施設の Wi-Fi アクセスポイントと企業オフィスへの WAN 接続はサイバー犯罪者の侵入経路となり、供給網への攻撃や企業ネットワークへの侵入の被害が発生する可能性があります。

供給網を保護するフォーティネットのセキュリティソリューションは、4 つの領域を中心として機能します。

高可用性の確保：FortiGate は、アクティブ / パッシブな HA（高可用性）構成に対応しています。ネットワークの停止や作為的な NGFW の無効化イベントが発生した場合に、シームレスなフェイルオーバーを行います。FortiGate NGFW でセキュア SD-WAN が有効になると、使用可能なすべての WAN リンクの活用が自動的に最適化されると同時に、リンクを横断するトラフィックのインスペクションが実行されます。さらに、FortiSwitch はセキュアなアクセススイッチを FortiAP 無線アクセスポイントまで拡張します。

インシデントに対する適時のレスポンス：FortiSIEM のセキュリティ情報 / イベント管理機能は包括的なインシデント管理プログラムの一部として動作し、統合ソリューションとして脅威の可視化、関連付け、自動対応、修復を行います。FortiManager はすべてのフォーティネットソリューションを一元管理し、FortiAnalyzer は強力な自動化とログ管理機能によってセキュリティ侵害対策を講じます。

監視を一元化：FortiCamera と FortiRecorder は、発電所内の重要な場所を視覚的に監視することでインフラストラクチャを確実に保護します。また、FortiPresence 分析ソフトウェアは、変電所などの分局施設の Wi-Fi ネットワークに接続されたデバイスを追跡し、建物や特定区域への不正侵入を検知します。さらに、デバイスユーザーの訪問を時間、頻度、場所のパターンによって分析し、設備のセキュリティをさらに強化します。

外部サービスまたは従業員によるリモートアクセスの制御：ユーザーの認証と管理（FortiAuthenticator）、二要素認証のサポート（FortiToken）、ネットワークアクセス制御（FortiNAC）が可能になります。また、FortiClient は幅広いネットワークにアクセスするエンドポイントデバイスを可視化し、制御します。

供給網

近代的な配給システムの中核には、スマートメーター、上下水管、変電所など分局施設による複雑な構造が存在します。配給ネットワークに関連する攻撃対象領域には、公益事業のサービス領域にあるほぼすべての建物で稼働している産業用モノのインターネット（IIoT）デバイスや、無人状態が大半の多数の分局施設が含まれています。ネットワーク接続された IoT デバイスを標的にした攻撃を完全に阻止することは不可能であるため、感染デバイスからネットワークの他の領域への被害拡大を阻止することが重要です。

無人の分局施設については、WAN 接続の耐障害性と TCO（総所有コスト）が課題となります。この課題解決で能力を発揮するのが FortiGate セキュア SD-WAN で、それほど重要度の高くないものに比べてビジネスクリティカルなトラフィックとアプリケーションを優先して処理します。また、パス識別型インテリジェンスとリンクの修正機能はアプリケーションパフォーマンスを最大限に引き出し、フェイルバックメカニズムを提供します。FortiGate セキュア SD-WAN の統合型セキュリティは、保護領域をネットワークエッジまで拡張します。

フォーティネットのセキュリティは、セキュア SD-WAN にとどまりません。FortiGate NGFW による効果的なネットワークセグメンテーション、FortiNAC ネットワークアクセス制御（NAC）、FortiSwitch セキュアアクセススイッチを組み合わせることで、脆弱性と悪意のある脅威のリスクを最小限に抑えることができます。そして、可視化と迅速なレスポンスを可能にする FortiSIEM、FortiManager、FortiAnalyzer ソリューションは、2 番目の防御階層となります。第 3 の防御階層は、ネットワーク資産の物理的な保護機能で構成されます。FortiCamera と FortiRecorder 監視ソリューション、そして FortiPresence プレゼンス分析が変電所をはじめとする分局施設の建物や機器を監視します。さらに、FortiAuthenticator によるユーザー認証 / 管理、FortiToken の二要素認証は、セキュアなネットワークアクセスをサードパーティやリモートワーカーまで拡張します。

ネットワークへの侵入が過去 12 ヵ月発生していない組織は、6 件以上の侵入を経験している組織に比べ、ネットワークセグメンテーションを使って攻撃者の移動を制限している割合が 51% 高くなっています [5]。

OT 組織の 78% では、自社の OT 環境のサイバーセキュリティに関する一元的な可視化が不完全です [6]。

顧客エクスペリエンスの保護

サービスの利用者は、モバイルアプリケーション経由の通信、自動支払、リアルタイムの使用量情報などのエクスペリエンスを通じた、電力会社 / 公益事業者への容易で即座の自動アクセスを求めています。プロバイダーは、同様の電子的なチャネルを介して利用者とのコミュニケーションを行い、システム障害や物理的な安全が損なわれる状況が発生した場合に情報のリアルタイム配信や更新を行います。電力 / 公益事業者の Web サイトが DDoS（分散型サービス拒否）攻撃を受けると、利用者は正確な情報をタイムリーに入手できなくなり、生命の危険にさらされる恐れもあります。また、公益事業のデータやアプリケーションをアクセス不能にするランサムウェアは、事業オペレーションを停止に追い込む可能性があります。

このようなリスクを最小限に食い止めるために、電力会社 / 公益事業者は FortiGate NGFW、FortiWeb Web アプリケーションファイアウォール、FortiCASB クラウドアクセスセキュリティブローカーで提供されている完全な脅威保護機能を活用できます。これらのソリューションが企業のデータセンターとクラウドの両方に展開されている場合には、FortiManager の一元管理コンソールからの自動構成や一貫したセキュリティポリシーの適用、そして FortiAnalyzer による自動化とログ管理が可能です。

フォーティネットが提供する電力 / 公益事業者向けの差別化要因

フォーティネットは、電力 / 公益事業者向けに実績ある独自の機能を提供しています。主要な差別化要因には下記があります。

広範な可視化

フォーティネットのソリューションは、IT / OT 環境全体を包括的に可視化し、セキュリティを統合します。OT 環境については、すべての FortiGate NGFW に実装されている ICS サービスが OT システムで使用される通信プロトコルとのインタフェースを提供します。これにより、ネットワーク環境全体でコンテキスト識別を実現し、信頼（トラスト）の維持と水平 / 垂直方向トラフィックの監視を行います。

一元管理

電力 / 公益事業者のネットワークには、ICS、IIoT デバイス（センサーや測定機器など）、監視デバイス（IP 対応カメラなど）といった幅広いエンドポイントが接続されています。フォーティネットのソリューションは、ネットワークおよびセキュリティインフラストラクチャを統合すると同時に、サイロを解消して一元的な可視化と制御を実現します。

優れた耐久性を備えたアプライアンス

フォーティネットのセキュリティソリューションは、極度の高温や低温、電気的干渉にさらされる過酷な環境であっても安定したオペレーションが可能です。優れた耐久性を誇る FortiGate NGFW と FortiSwitch スイッチは、あらゆる導入環境でも重要なインフラストラクチャを保護します。

内部脅威の防止

FortiInsight は、UEBA（ユーザー / エンティティ振る舞い分析）を利用して内部関係者の悪意や怠慢による脅威およびデータ流出を防止します。また、インテント ベースト セグメンテーションを活用して重要なシステムを隔離し、ネットワーク内の脅威保護を実行します。FortiDeceptor は、悪意のあるユーザーアカウントや侵害されたユーザーアカウントを特定し、対処します。

ICS / SCADA システムを所有する組織の 89% でセキュリティ侵害が発生しています [8]。

プロアクティブな脅威インテリジェンス

重要なインフラストラクチャの保護には、ICS に特化した脅威インテリジェンスが必要です。フォーティネットは、この分野で過去 15 年におよぶ独自の経験と知識を培ってきました。この実用的なインテリジェンス、そして FortiGuard Labs が追跡を続ける OT 固有の脅威情報に基づいて、OT に特化したセキュリティ脅威レポートが実現しており、最初のレポートは 2019 年初旬に公開されています [7]。

業界の専門知識

フォーティネットのチームには、OT システムの保護に関して長年の経験を持つ業界のエキスパートが参加しています。その豊富な経験は業界をリードするテクノロジーの設計にも反映されており、詳細な実用的インテリジェンスと分析を通じて電力 / 公益事業者のサイバーセキュリティ責任者をサポートしています。

堅牢なパートナーエコシステム

フォーティネットは、トップクラスのセキュリティソリューション提供に注力すると同時に、オープンソースを活用したネットワーク / セキュリティテクノロジープロバイダーとの連携に取り組んでいます。フォーティネットは、OT サイバーセキュリティに特化した大規模なパートナーエコシステムと同時に、オープン API（アプリケーションプログラミングインタフェース）エコシステム、およびフォーティネットのファブリック・レディ パートナーが提供するソリューション向けの組込み型ファブリック・レディ API の活用を通じたサードパーティソリューションの統合を実現しています。

終わりに

国家が資金援助するハッカーや金銭目的のサイバー犯罪者、そしてアマチュアのハッカーたちは、国家レベルの混乱を引き起こす重要なインフラストラクチャを狙い、大規模な影響を与えようとしています。電力 / 公益事業者のセキュリティリーダーがこのような悪意のある攻撃を阻止するには、幅広い機能の統合と自動化を特徴とするセキュリティテクノロジーに基づく綿密な防御戦略を講じなければなりません。

フォーティネット セキュリティ ファブリックは、このような戦略を実行するための強力な基盤を提供し、個々のセキュリティ要素の統合、ポリシー管理、セキュリティワークフロー、脅威インテリジェンスの共有を実現します。その結果、スタッフ不足に悩む IT チームであっても、電力 / 公益事業者に不可欠な IT / OT セキュリティの幅広いニーズに応えることが可能になります。フォーティネット セキュリティ ファブリックを導入することで、複数のポイントソリューションや他のプラットフォームソリューションに比べ、最小限のスタッフトレーニングと低コストで確実な IT / OT セキュリティを実現することが可能になります。

[1]「48% of power and utility CEOs think cybersecurity attack is inevitable: KPMG」、Catherine Morehouse 氏、Utility Dive、2018 年 11 月 16 日（英語）：https://www.utilitydive.com/news/48-of-power-and-utility-ceos-think-cybersecurity-attack-is-inevitable-kpm/542412/

[2]「Managing cyber risk in the electronic power sector: Emerging threats to supply chain and industrial control systems」Steve Livingston 氏他、Deloitte、2019 年 1 月 31 日（英語）：https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/cyber-risk-electric-power-sector.html

[3]「Shortcomings of Traditional Security and Digital OT: Key Takeaways for Network Operations Analysts」、フォーティネット、2019 年 4 月 12 日（英語）：https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/02_Collateral/eBooks/eb-network-operations-analyst.pdf

[4]「Improving the Cybersecurity of the Electric Distribution Grid: Identifying Obstacles and Presenting Best Practices for Enhanced Grid Security」、Mark James 氏他、Institute for Energy and the Environment、Vermont Law School、2019 年 4 月（英語）：https://www.vermontlaw.edu/sites/default/files/2019-04/VLS_IEE_Electricity_Distribution_Grid_Cybersecurity_Phase_1 Report[1].pdf

[5]「State of Operational Technology and Cybersecurity Report」、フォーティネット、2019 年 3 月 15 日（英語）：https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-state-of-operational-technology.pdf

[6] 同上

[7] 同上

[8]「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

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-Protecting-Powere-Utilities-202002-R1