SOLUTION BRIEF

FortiNAC によるセキュリティ強化

概要

オペレーショナルテクノロジー（OT）システムのセキュリティは、重要度の高い製造インフラストラクチャにおいて、重大な懸案事項の 1 つです。何十年も前に登場した ICS（産業用制御システム）とその SCADA（監視制御 / データ収集）サブセットシステムは、IT システムとの接続が進み、巧妙な脅威が次々に登場している今、格好の標的になっています。フォーティネットは、OT 環境を保護するさまざまなソリューションを提供しており、NAC（ネットワークアクセス制御）もその 1 つです。FortiNAC は、スタンドアロンまたはフォーティネット セキュリティ ファブリックの一部として実装することができ、OT ネットワーク全体の可視化と制御を可能にします。

相互接続が SCADA と ICS リスクを高める

かつての OT 環境、つまり ICS システムと SCADA システムは、パブリックネットワークやインターネットからは隔絶されていたため、安全性が保たれていました。また、実質的に攻撃が存在しなかったため、PLC（プログラマブルロジックコントローラ）といったセキュリティテクノロジーを導入する理由もなかったのです。ところが、OT と IT（情報テクノロジー）を隔てる壁がなくなると、事態は一変しました。最近の調査から、ほとんどの組織が IT システムと OT システムを接続していることが明らかになっています。これは、制御システムにハッカーが侵入する危険があることを意味します [1]。

2015 年 12 月、ウクライナで送電網がダウンし、8 万人の世帯が停電しました。この SCADA を狙った多面的な攻撃をきっかけに、SDADA システムが攻撃の標的になり得ることが急速に認識されるようになりました [2]。その背景には、多くの SCADA システムがインターネットやクラウドに接続されるようになったことがあります。このようなネットワーク環境の変化は、ほとんどがデジタルトランスフォーメーションによるものです。さらに、OT システムには、接続機能を搭載したスマート環境制御（照明、消火、空調システムなど）のようなコンポーネントが組み込まれています。かつて、OT システムでは有効なセキュリティ対策は講じられてこなかったため、このような接続の 1 つ 1 つが新たな侵入経路になってきているのです。

OT システムのセキュリティ管理は難題です。特に、エネルギー供給企業や分散した製造施設など、重要度の高いインフラストラクチャを運用する組織にとって、これは大きな課題となっています。システムのインターネット接続は大きなメリットであると同時に、OT 管理チームがこれまで経験したことのない新たなリスクをもたらします。インターネット接続された ICS システム、SCADA システム、PLC が複雑なネットワークを構成する現在、一元管理とセキュリティ制御の強化が求められています。組織は、ネットワークを厳格に管理し、OT ネットワークに接続するあらゆるユーザーとモノを確実に把握しなければなりません。

IoT のセキュリティという課題

OT システムは、極めて広範な攻撃対象領域をもっています。最近 Forrester Consulting が実施した調査によると、SCADA または ICS を使用している組織の 60% 近くが、過去 1 年間にシステムへの侵入を経験しています。また、「IT / OT のコンバージェンスが原因でセキュリティの課題が発生した」と回答した企業は、97% にのぼります [3]。

SCADA と ICS の違いを理解する

ICS は SCADA システムを介して管理されることが多く、オペレーターは GUI（グラフィカルユーザーインタフェース）を使用して、システムステータスの確認、アラートの受信、プロセス管理の調整入力などを行います。

ICS 市場は、2021 年までに 810 億ドルに成長すると予測されています。

SCADA 市場は毎年 6.6% 成長し、2022 年までに 134 億 3,000 万ドルに達すると見込まれています [4]。

ICS / SCADA システムはこれまで隔絶されていたことから、ほとんどの IT サイバーセキュリティ設計では考慮されてきませんでした。さらに、レガシーシステムの多くは、パッチ適用やアップデートに対応していません。このようにセキュリティ保護されていないエンドポイントは、格好の攻撃対象となります。なぜなら、こういったシステムは攻撃者が高価値のネットワークデータにアクセスできる経路となるだけでなく、重要度の高い国家的なインフラストラクチャ（電気、石油、ガス、水、輸送など）の一部だからです。

IT と OT が統合される領域に存在する脆弱性は、主に次の 3 つに分類されます。

1. 可視性の欠如：

包括的かつ一元的にデバイスを可視化する機能がないと、OT ネットワークは攻撃に対して脆弱になります。ネットワーク接続デバイス（IoT や個人所有の BYOD など）が広く普及した結果、ラテラルな攻撃に弱いアクセスポイントが増加し、エンドポイントのセキュリティ脆弱性が増大しています。セキュリティチームには、ネットワークの末端までを網羅するあらゆる場所でネットワークに接続しようとするデバイスすべてを可視化する機能が必須です。

ICS センサー、空調システム、コントローラのスマート化や接続が進んでいますが、これが OT システム攻撃の新たな侵入経路になっています。特に、IoT デバイスにはセキュリティ標準がなく、保護されていないデバイスが数多く存在します。また、既存のファイアウォールをはじめとするセキュリティ機能は、ほとんどがユーザーベースでアクセスの可否を判断しますが、IoT デバイスにはユーザーが関連付けられていないため、認証は不可能です。

2. 制御性の欠如：

フラットでオープンな内部ネットワークは、ハッカー、悪意のあるユーザー、自動化されたマルウェアの標的になりやすく、機密性の高いデータや IP を簡単に盗み出すことができます。したがって、ネットワークに接続するユーザーやデバイス毎にアクセスポリシーを適用する機能が必要です。ロールベースの動的なネットワークアクセス制御は、論理的にネットワークセグメントを作成することで、アプリケーションのグループ化、データのリンク、特定のグループに限定したアクセス制限を実行し、企業内のセキュリティを強化します。

ユーザーとデバイスの制御は、コンプライアンスの維持において特に重要なポイントです。現在、多くの業界規制やプライバシー法によって厳格なネットワークアクセス制御やデータ保護が義務付けられています。一例を挙げると、GDPR（一般データ保護規制）、HIPPA（Health Information Portability and Accountability Act）、SEC（米国証券取引委員会）、SOX 法（Sarbanes-Oxley）、PCI DSS（Payment Card Industry Data Security Standard）などがあります。コンプライアンス違反が発生した組織には、数百万ドルもの罰金が科せられる可能性もあります。

3. 迅速な状況確認能力の欠如：

個々の接続デバイスが攻撃されようとしている場合、全社規模で防御態勢を整えるには、脅威情報を自動的に共有する機能が必須です。ところが、セキュリティチームが毎日受信し、仕分けなければならないセキュリティアラートは、何千件にものぼることがあります。セキュリティ管理者は、特定の IP アドレスで不審な操作が行われているという通知を受け取ると、何時間もかけて調査を行い、不審なデバイスやその他の関連情報を手作業で追跡することで、それが攻撃か異常なのかを判断しています。

FortiNAC で攻撃を阻止

ICS / SCADA、さらには IoT や BYOD をはじめとするエンドポイントのセキュリティ保護という課題を解決するには、高度な機能を備えた NAC をセキュリティアーキテクチャ全体に組み込む必要があります。FortiNAC は、スタンドアロンまたはフォーティネット セキュリティ ファブリックの一部として実装することができ、脆弱なエンドポイントへのネットワークアクセスを保護します。

FortiNAC は、他のフォーティネットソリューションと連携することで、パッチが適用されていない脆弱なエンドポイントを検知し、SCADA を狙う脅威から幅広い分散ネットワークを保護します。重要度の低いエンドポイントについては、パッチが適用されるまでの間、ネットワークから瞬時に自動切断できます。このようなエンドポイントは、中央のダッシュボードを使用して、ネットワーク接続状態へと自動的に復帰することが可能です。FortiNAC は、特にインターネット接続が進む産業界において不正なエンティティによる OT ネットワーク接続を阻止することができ、脆弱な ICS / SCADA システムの保護において重要な役割を担います。FortiNAC の主な機能としては、ネットワークセキュリティを強化する可視化、制御、脅威の自動通知が挙げられます。

1. あらゆるエンドポイントデバイスを完全に可視化

Forrester が実施した前述の調査によると、組織の 82% が「OT / IT ネットワークに接続されているデバイスを完全には特定できていない」と回答しています [5]。見えない脅威からネットワークを保護することは不可能であるため、組織全体を完全にリアルタイムで可視化することが、エンドポイントデバイス保護の最初のステップとなります。FortiNAC は、ネットワーク接続されたすべてのエンドポイントのプロファイリングを行い、物理的な所在地点やデバイスのタイプを識別します。

2. 比類のない機能で脆弱なデバイスを制御

FortiNAC は、SCADA / ICS システムの管理業務をサポートします。ネットワーク接続やインフラストラクチャの別のコンポーネントとの通信を開始しようとする新しいデバイスを管理することで、ネットワークが完全に制御された状態を維持します。不審なリクエストを検知すると、誤ったトラフィックのないネットワーク接続が管理者により承認されるまでそのリクエストを保留します。

これにより、重要なシステムのサービス中断を回避できます。また、FortiNAC では、どのユーザーにネットワークアクセスを許可し、どの程度のアクセス権限を割り当てるかを指定する条件やポリシーを設定し、適用することも可能です。ポリシーの構成変更も可能で、幅広いベンダーのスイッチや無線製品を対象にセグメンテーションポリシーを実装できます。この動的な制御により、マルチベンダー環境においてセキュリティ ファブリックが保護できる領域が広がります。FortiNAC の自動ルールは、セキュリティ ファブリックにおける他のコンポーネント（FortiGate、FortiSwitch、FortiAP など）で設定されている隔離機能をトリガーします。その対象には、サードパーティソリューションをはじめとするあらゆるファブリック レディの要素が含まれます。

このような制御機能には Web ベースの管理ダッシュボードからアクセスでき、ダッシュボードは高度なカスタマイズや容易な活用が可能です。不審なユーザーや脆弱なデバイスを特定し、幅広い隔離アクションを実行することで、潜在的な脅威を確実に隔離します。その結果、隔離に要する時間は、数日からわずか数秒へと短縮されています。また、ますます厳格になる業界の規制、重要なデータや IP の保護にも対応し、コンプライアンス状態を維持します。

3. 脅威の自動通知

不審なイベントを検知すると、FortiNAC は SOC（セキュリティオペレーションセンター）に脅威通知を自動送信します。フォーティネット セキュリティ ファブリックの一部である FortiNAC は、幅広いセキュリティアーキテクチャとシームレスに統合します。脅威インテリジェンスのリアルタイム送受信でアラートの信頼性を高めると同時に、セキュリティに対する認識を全社規模で高めます。この高度な自動通知機能は、ネットワーク接続されたセキュリティアーキテクチャの中核とも言うべき重要な要素です。

FortiNAC のオーケストレーションでは、すべてのセキュリティデータが集約されます。優先度に基づいた脅威のトリアージを自動実行し、SOC へとアラートを自動送信します。また、イベントに関するリアルタイムのコンテキスト情報は、セキュリティアナリストが問題の発生場所や脅威への対応を実行する際に役立ちます。これにより、隔離に必要な時間を数日から数秒へと短縮できるだけでなく、ますます厳格になる法規制やセキュリティ標準へのコンプライアンスを支援します。

柔軟性と拡張性を兼ね備えたアクセス制御プラットフォーム

フォーティネットは、FortiNAC の他にも OT 環境向けに包括的なソリューションを展開しています。フォーティネットのポートフォリオは、次のような中核機能を備えています。

事例：大手石油ガス会社：FortiNAC で重要なインフラストラクチャをセキュリティ保護

重要なインフラストラクチャの運用とエネルギー事業を行う組織は、絶えず変化する市場のニーズに合わせて進化を続けています。一方で、コンプライアンスが実現されていないエンドポイントを悪用しようとする脅威にサービスを中断されないように、システムのセキュリティ強化を図らなければなりません。そのためには、ネットワークの可視化、制御、そしてレスポンスを完全に実行することが極めて重要です。ところが、広く分散した ICS 環境を運用することが多いエネルギー供給企業にとって、セキュリティ保護は難題です。地理的に広く分散したシステムを IT スタッフが手作業で保守とアップデートを行う方法は、現実的ではありません。

北米の 200 拠点で 5,000 のエンドポイントを使用している大手石油ガス会社は、分散したエンドポイントとレガシー機器へのネットワークアクセス管理に、FortiNAC を活用しています。

物理的に離れた拠点を確実に制御できる FortiNAC により、困難の伴うハードウェアのインストールや複雑なレガシー機器のアップグレードが回避されています。

フォーティネットのソリューションは一元管理と帯域幅の節約を特徴としており、リモートサイトにアプライアンスをインストールすることなく、帯域幅の制約という懸案事項を解決することができました。この企業は、広く分散したリモートスイッチからあらゆる場所のエンドポイントやユーザーまで、すべての接続の最新インベントリに基づいてネットワーク全体を可視化しています。

- 通信のセグメンテーションと保護
- 有線 / 無線アクセスの保護
- ユーザー、デバイス、アプリケーション、プロトコルに対するロールベースのアクセス制御の適用
- 脆弱性やパッチ管理手順の確立
- 資産の特定とプロファイリング
- マルウェアとゼロデイ脅威の特定とブロック

フォーティネット セキュリティ ファブリックの一部として、FortiNAC はセキュリティオートメーション / オーケストレーションプラットフォームを提供しています。ハードウェアアプライアンス、仮想アプライアンス、クラウドサービスとして実装でき、あらゆるネットワーク環境に固有のニーズを満たす柔軟性の高い NAC ソリューションを提供します。FortiNAC は、拡張性のニーズを念頭に設計されているため配備先各々にサーバーを設置する必要がなく、TCO の削減にも貢献します。既存のディレクトリ、ネットワーク、セキュリティのインフラストラクチャを活用する FortiNAC は、これまでの投資を保護すると同時にシステム運用の中断を最小限に抑制可能な優れた NAC ソリューションです。

一元管理機能、そして課題となっているレガシーシステムの全面的なアップグレードを行わずに封鎖する機能を備えた FortiNAC は、未承認のデバイスやユーザーに対する脆弱性が高まり続ける OT ネットワークの保護に理想的なソリューションです。

事例：GIBSON ENERGY 社

Gibson Energy 社は、石油や石油精製品の輸送、備蓄、混合、処理、販売に特化した企業です。カナダのカルガリーに本拠を置く Gibson Energy 社は、油田廃棄物や水の管理サービスも提供しています。

中堅のエネルギー企業であるこの企業は、何千ものデバイスを現場で利用しています。つい最近まで、そのようなデバイスは手作業での管理、あるいはまったく管理されていない状況にありました。ところが、IoT デバイスの導入によって IT ネットワークへの接続が行われるようになったことで、運用体制を強化するためにさらなる可視化と制御が必要になりました。

Gibson 社の運用チームは、この課題を解決するために FortiNAC を選択しました。チームでは、カスタマイズ可能な Web ベースのダッシュボードから、脆弱なデバイスの監視と管理をリアルタイムでリモート実行しています。ネットワーク接続やインフラストラクチャの別のコンポーネントとの通信を開始しようとする新たなデバイスを検知すると、FortiNAC は管理者が承認するまでその接続を保留します。これまで手作業で保守を行ってきた Gibson 社は、FortiNAC の導入によって数千時間もの労働時間を節減しています。

Gibson Energy 社の情報サービス担当バイスプレジデント、Richard Hannah（リチャード・ハンナ）氏は、次のように述べています。「重要なリソースの管理と制御に携わる我々は、ファイアウォールをはじめとするセキュリティツールへのアクセスをきめ細かく制御し、統合されたセキュリティ態勢を確立し維持する必要があります。フォーティネットは、このニーズに理想的なソリューションを提供してくれました」

1「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、2021 年 9 月 3 日：
https://www.fortinet.com/content/dam/fortinet/assets/white-papers/ja_jp/report-ot-forrester.pdf

2「Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid」、Wired、2016 年 3 月 3 日（英語）：
https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

3「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、2021 年 9 月 3 日：
https://www.fortinet.com/content/dam/fortinet/assets/white-papers/ja_jp/report-ot-forrester.pdf

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、2021 年 9 月 3 日：
https://www.fortinet.com/content/dam/fortinet/assets/white-papers/ja_jp/report-ot-forrester.pdf

5「IoT Security Fail: 82 Percent of Companies Can't Identify All Network-Connected Devices」、eSecurity Planetm、2017 年 11 月 8 日（英語）：
https://www.esecurityplanet.com/network-security/iot-security-fail-82-percent-of-companies-cant-identify-all-network-connected-devices.html

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