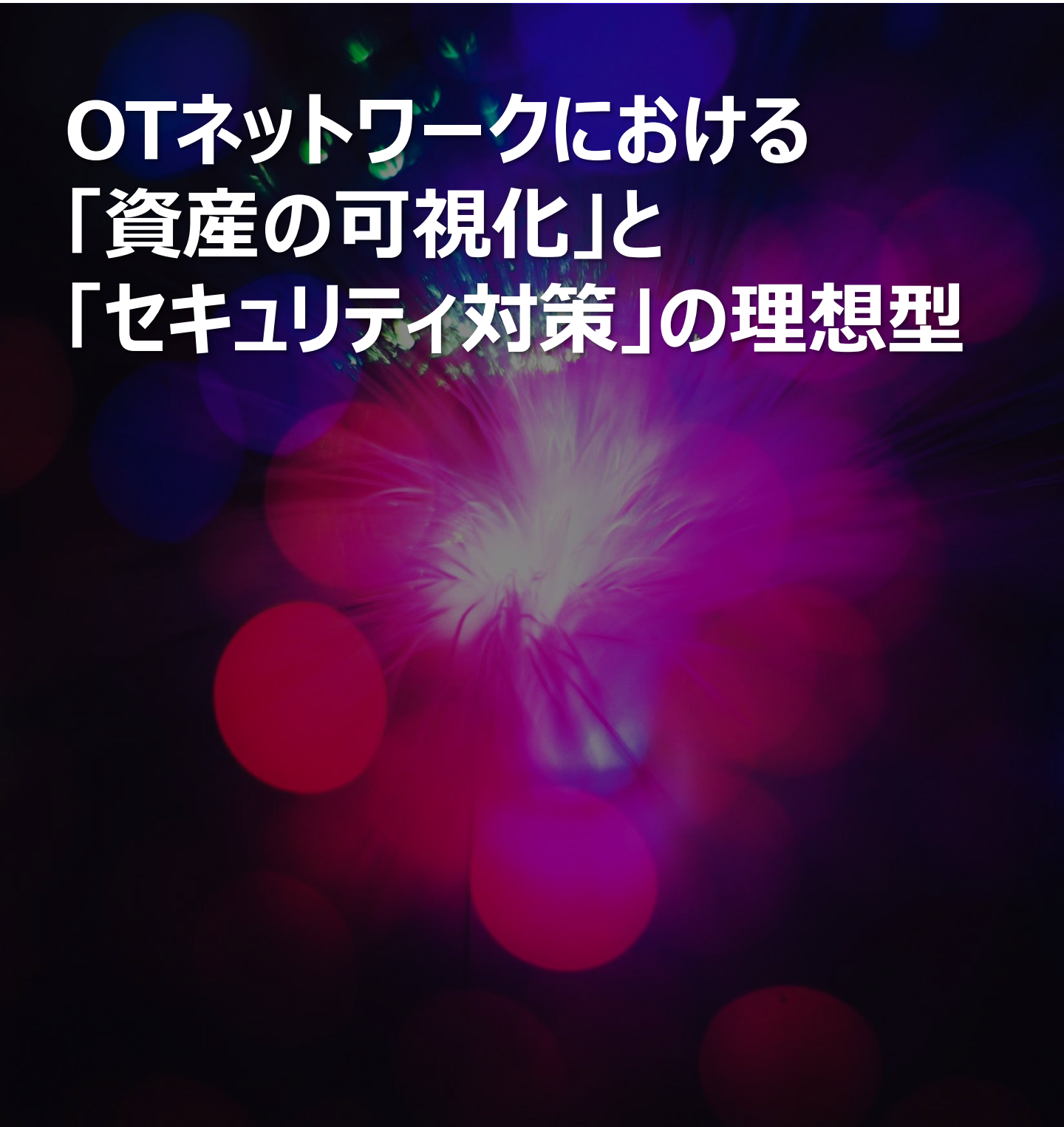
SCADAfence

障害や事故で、決して止めてはいけない
Operational Technology



OTネットワークにおける「資産の可視化」と「セキュリティ対策」の理想型

SCADAfence

もくじ

近年、工場やプラントを支える工場インフラが外部インターネットに繋がるようになってきている中、マルウェアを始めとするサイバー攻撃を受ける事例が増えてきています。そして、この背景にあるのは「技術的な原因」ではなく、『この設備やパソコンは外部に接続していないから被害にあうことはないだろう…』という油断や見当違いにあることが指摘されています。デジタルトランスフォーメーション（DX）やイノベーションが急速な進展を見せる昨今、どのような工場・プラント設備もサイバー攻撃に遭遇する可能性があるのです。

本書では、DXが加速する現代において、工場インフラがどのような姿にあるべきか、そのポイントと実現までの流れをご紹介したものです。セキュアな工場インフラを実現し、障害や事故を未然に防ぐネットワーク環境を構築したいと考える全ての方に、ぜひ一度お読みいただきたい内容となっています。

ITと比べて「20年遅れ」の工場セキュリティ

Chapter

1

攻撃者のターゲットは セキュリティ対策の進んでいないものづくり現場へ

デジタルトランスフォーメーションの波が急速な広がりを見せている今、あらゆる企業においてシステム、データ、ネットワークの統合・再構築が進んでいます。この流れは**製造業を支えるOT(Operational Technology)**領域にまで及んでおり、これまではバラバラだった各要素が繋がり合うことで、従来は存在し得なかった新たな価値が生み出されています。例えば、運用プロセスの可視化や業務効率の向上がイメージしやすいのではないでしょうか。しかし、様々なメリットが生み出されている一方で、新たな脅威が生まれている点を見逃してはなりません。

例えば、2017年には、仏・自動車大手「ルノー」の工場がサイバー攻撃を受けて、操業が一時中断される事態に陥りました。この事件は多くの製造各社に衝撃を与えると同時に、「工場は外部ネットワークから遮断されているから安全」という発想から脱却することの必要性を私たちに提示しました。

工場がサイバーセキュリティーの新たなターゲットに

被害を受けた工場で感染が確認されたのは、パソコンのデータと引き換えに身代金を要求する形態のウイルス「ワナクライ」。これは、いわゆる「ランサムウェア」と呼ばれるウイルスの一種で、工場の他にも、病院や通信会社、政府機関も被害を受けたとされています。

このウイルスの感染原因は明らかにされていませんが、はっきりしていることは、**一見スタンドアロン（孤立した）と思われているシステムやパソコンも、何らかのタイミングでウイルスに感染・発症する可能性がある**ということです。事実、近年は製造業の制御システムを狙ったサイバー攻撃が増加しており、何らかの対策を講じなければ、どの工場も操業停止などの被害を被る恐れがあります。

重大事故に直結しかねないOTへのサイバー被害

そもそも、OTの中核にあたる制御システムは、情報システム(IT)とは異なる特性がある点を理解することが大切です。ITでは「情報漏洩の防止」が最大のテーマに掲げられる一方で、制御システムを始めとするOTでは、「システムの継続的な安定稼働」が命題となっており、これが危ぶまれれば人命や重大事故すら引き起こしかねません。この前提を踏まえて、製造業各社はDX時代のサイバーセキュリティーリスクのあり方を捉え直す必要があり、事業継続に向けた対策を本格的に講じることが求められています。

OTネットワークにどのような資産がつながっているか把握できている企業は少ない

デジタルトランスフォーメーションが加速する現代、OT環境にはどのようなセキュリティ対策が求められているのでしょうか。まず、第一段階として実施すべきは、『工場と資産の可視化（把握）』です。何故ならば、資産の可視化を行うことで、今後のDXの流れの中での施策対象を明確にするだけではなく、もしもOTシステムが何らかの脅威にさらされたとき、これら対策の有無によって「障害検知に要する時間」が大きく変わるからです。

障害検知に要する時間 MTTD（Meantime to Detect）

セキュリティ対策を**「していた」**場合 → **24**時間以内

セキュリティ対策を**「していなかった」**場合 → 平均 **272**日間

出典：https://gereports.jp/ot-security

セキュリティ対策をしていなかった場合には、障害検知までの時間がかかることはもちろん、その対応策の実施や復旧にも多大な時間を要することが予想されます。では、このような時間の差は一体どこから生まれるのでしょうか？その最大のポイントが、工場インフラネットワークに接続された「資産の可視化」と「セキュリティ対策の実施体系」にあります。

次章では、これらを実現するために求められる基礎知識と、具体的な方法論をご紹介します。

OTネットワークにおける「資産の可視化」と「セキュリティ対策」の理想型

Chapter

2

「可視化」と「異常検知」を実現する理想的なOT×ITの形とは

工場インフラネットワークの構成を考えるにあたっては、まず初めに、IT指向からOT指向へと発想を切り替える必要があります。この理由として、ネットワークに接続された制御システム全般が「稼働停止できない」という特性を持っていることが挙げられます。

ITとOTの特性の違い

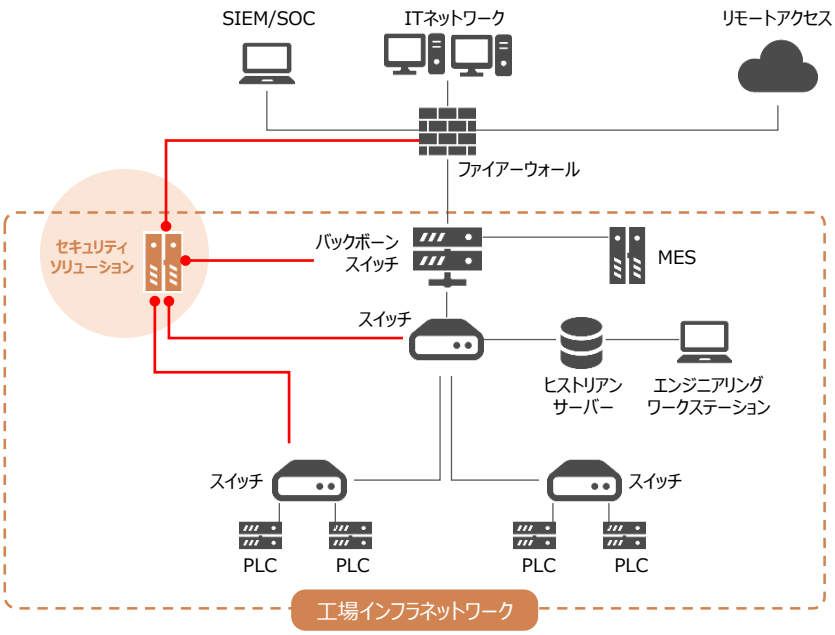
	優先順位	保護対象	求められる水準
制御システム（OT）	システムの継続的な安全稼働	モノ（設備・製品）サービス（連続稼働）	24時間365日の安定稼働（再起動は困難）
情報システム（IT）	情報の適切な管理情報漏洩の防止	情報	再起動は許容範囲となるケースが多い

参考：https://www.ipa.go.jp/files/000058489.pdf

この前提を踏まえて設計すべきOT×ITのアーキテクチャが右図になります。ここでのポイントは、常時、もしくは一時的に工場インフラに接続された膨大な機器が監視対象から漏れてしまうことがないように配慮した構成とすることです。工場セキュリティを運用する現場では「この設備がネットワークに接続しているとは知らなかった」という認識の相違や、「メンテナンス時に一時的にネットワークに接続してから、そのまま接続している状態になっていた」というケースが生じています。
だからこそ、そのような事態を予め想定したアーキテクチャは必須といえるでしょう。

工場セキュリティを考える上では、ネットワーク経由の脅威のみならず、あらゆる「人」が直接重要機器を操作・メンテナンスするケースも考慮する必要があります。だからこそ、右図のように、ネットワークの中核から末端まで、ハードウェア／サービス両面にわたる包括的な対策が必要です。

OT×ITのアーキテクチャ概念図



https://gereports.jp/ot-security

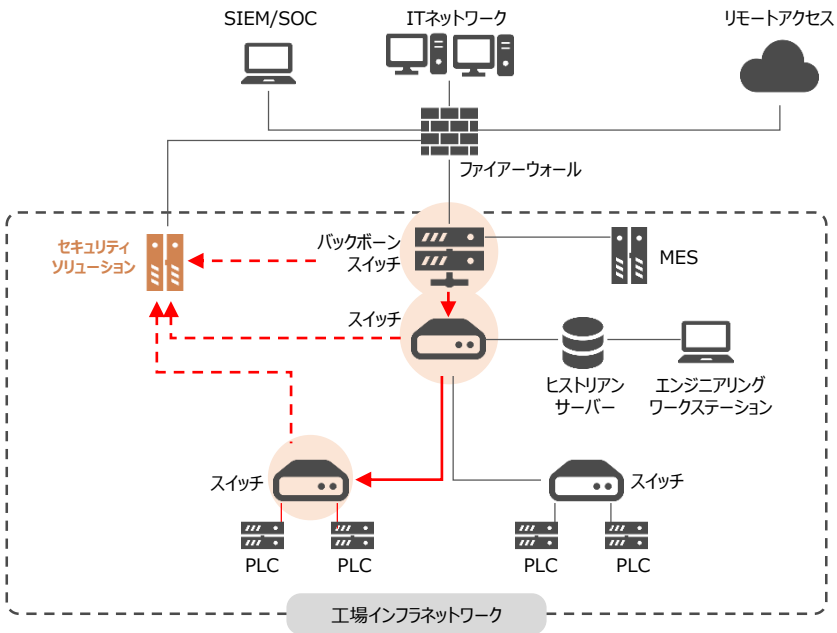
既存のOTネットワークに一切影響を与えず導入することが実現のポイント

工場セキュリティを考えるうえで欠かせないもう一つの観点は、「可用性への配慮」です。前述のように、OTの領域では、「動いている設備を止めないこと」が最重要事項になるため、既存の機器や設備に何らかの影響を与えうる新たなソフトウェアの導入は好まれません。だからこそ、「いかに既存設備の稼働に与えるリスクを最小化するか」という点の議論は避けては通れないのです。

既存設備への影響を抑えるためには、「①非侵入型」「②パッシブ型」という２つの条件を満たす必要があります。「①非侵入型」は、個々の設備・ソフトウェアとの競合を防ぐために最適な監視形態です。加えて、「②パッシブ（受け身）型」の監視形態を取ることで、パフォーマンスの低下を防ぐことができます。

技術的な観点を加えるならば、近年は、下図のように「スイッチ」のミラーリングポートを利用し、産業機器全体の挙動をリアルタイムで監視する手法が最適とされています。この手法を用いることで、業務への悪影響を排除し、個別の製品への設定作業もなくすことができます。

非侵入型・パッシブ型の構成がポイント



セキュアなOT環境を実現する標準的なワークフロー

セキュリティ被害からOT環境を守りつつ、OT環境全体の可用性を維持するためには、セキュリティソリューションの運用を始めるまでの過程でも多くの配慮が求められます。工場インフラの全体像を把握し、休むことなく稼働を続ける既存設備への悪影響を排除するためには、次の標準的なフローをベースに議論を進める必要があります。

OT環境構築までのフロー

Step 1

パッシブ型でシームレスなシステム構築

機器の挙動を網羅的に監視する「パッシブ型」の監視を前提に、アーキテクチャ設計を行い、OT資産の可視化を行います。

Step 2

ネットワークディスカバリーによる運用状況の把握

工場インフラの全体像を把握し、産業特性に応じたトラフィックパターンを検出させた上で、各種リスク、脆弱性を分析します。合わせて、資産のリスト化、運用状況を検証する基準値の定義も行います。

Step 3

継続的な監視の実施

万が一、悪意のあるアクティビティが検出された際には、管理者は早期に適切な対応を講じる必要があります。ここではサイバー攻撃の他、人為的なミスなどによる障害を事前に検知し、可用性を維持するための予知保全を行う環境を構築する必要があります。

Step 4

既存の管理システムとの統合

既存のファイアウォールやログ蓄積デバイス連携・統合し、内部アラートの効率化・高度化を行い、効果の最大化を目指します。このためには、初期段階から業界標準に基づいたアーキテクチャ設計を実施することが必要です。

セキュリティソリューションを自社で構築する場合、専用のソリューションを導入する場合、いずれのケースでも、上記のフローはおおよそ共通しています。まずは工場セキュリティの特性を踏まえた上で、自社の組織体制に応じて最適なフローを検討しましょう。

取得し可視化するデータの活用用途を明確にしておこう

ここまででご紹介した工場セキュリティの整備は、一見すると、セキュリティ対策の領域にとどまったものに見えるかもしれません。しかし、市場の変化に合わせてOT環境の改善が求められ続ける現代では、もう一つの用途も重要視されています。それは、「生産プロセスの最適化」と「コスト削減」です。

製造現場の生産性向上が急務となっている中でも、既存設備のパッチ適用など、細かなメンテナンスは欠かせません。そして、このプロセスがおろそかになれば、機器の急な稼働停止など予定外のトラブルに見舞われるため、これらの情報管理（資産管理、変更管理等）は作業スタッフの大きな負担になっています。だからこそ、OTセキュアを考える上では、セキュリティ対策のみならず「OT資産の見える化」が生産プロセス全体の価値向上に寄与するのです。ネットワーク全体と個々の設備に関するデータをフルに活用すれば、自社の製造現場が持つ新たなポテンシャルを見出すことも難しくはありません。

データを活用し、ヒューマンエラーの防止・回避にも

OT資産に関するデータの活用は、日本国内でも様々な可能性が見出されています。例えば、大手不動産デベロッパーの三井不動産では、複合施設の運用管理業務にOTセキュリティソリューションを導入し、ビル管理体制・管理方法の見直しを進めています。同社の担当者が「ビル内にネットワーク接続される機器が増え続ける中では、これまでのような『目視』と『紙（台帳）』に頼った運用管理では維持できなくなる」という認識を示していることからも、人的リソースに頼った管理が限界を迎えつつあるといえるでしょう。同時に、アセットモニタリング（資産監視）やネットワーク接続機器の不具合検出といった検証も進めており、不具合発見後のオペレーションの改善も検討しているとのことです。このように各種ソリューションやそこから得られたデータを活用してヒューマンエラーを防止・回避するなど、OT環境の見直しは様々な展開可能性を秘めています。

では、ここまでにご紹介してきた工場インフラネットワークの理想形には、どのような実現方法が考えられるのでしょうか？次章では、ネットワーク上の資産の可視化、およびセキュリティ対策に特化したプラットフォームをご紹介します。

SCADAfence
プラットフォームのご紹介

Chapter

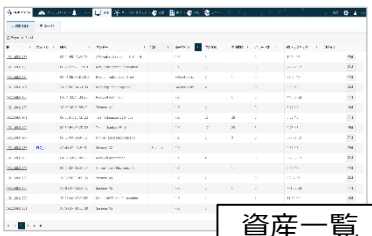
3

サイバーセキュリティ先進国イスラエル発の「SCADAfenceプラットフォーム」

SCADAfenceプラットフォームは、イスラエル軍サイバーセキュリティ開発部門の出身者が設立し、産業セキュリティに特化した「SCADAfence社」が提供するソリューションです。工場・ビル内に対するサイバー攻撃の監視・検知に特化しており、広大な工場インフラの可視化・常時監視が可能。多様化する製造工程についても、それらの振る舞いを学習し、不審な通信を検知した際にはアラート通知を行うことで、セキュアなOT環境を実現します。

Feature1

VISUALIZE：守るべき資産の可視化

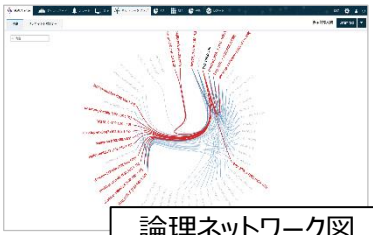


資産一覧

- 制御システムや生産設備など「守るべき資産」を自動でリスト化し、リアルタイムでの通信状況も可視化が可能
- ネットワーク論理構成図も自動生成できる
- パッシブ型のため、工場ネットワーク環境を変更せずに導入可

Feature2

ANALYZE：通信内容の学習・解析・保存



論理ネットワーク図

- 論理ネットワーク構成情報により、それぞれの生産設備の通信状況のリアルタイムかつ正しい理解が可能
- 独自の機械学習アルゴリズムにより、工場ネットワークならではの多様化する製造工程を含めた振る舞いを学習、モデル化

Feature3

RESPOND：異常検知と復旧・改善

検知したアラート一覧

- 外部からの攻撃だけでなく、内部での誤操作、予期しない設備の構成変更など障害や事故につながる可能性のある動きを発見、通知
- APIによる他システムとの連携により、特定から対応までの自動制御や、セキュリティサービスプロバイダーによる運用支援の利用もできる

機能と特徴

SCADAfenceプラットフォームは、大規模で複合的な産業用ネットワークの「規模」と「多様性」の両面をサポートする、極めてユニークなソリューションです。従来の産業ネットワークは予め決められた処理を繰り返す傾向にある一方で、大規模な産業ネットワークは「膨大なトラフィック」「ノイズの大きいアクティビティ」「動的で、多様な通信パターン」といった特徴を持っています。これらに対応すべく、SCADAfenceでは以下のような幅広い機能を備えています。

可視化と資産管理

自動で資産検出とネットワークマッピングを行い、資産インベントリをデジタル化することで、従来は手作業で取得していたスプレッドシートを最新のリアルタイム情報に置き換えることができます

リスクプロファイリング

産業ネットワークが潜在的なリスクにさらされている箇所とその攻撃シナリオを特定します。また、攻撃可能面を減らし、ネットワークの回復性を高めるために事前に行えるリスク緩和措置の把握が可能です

継続的な監視

ネットワークのアーキテクチャを継続的に監視して、セキュリティの状況を正確に把握し、リアルタイムのイベントを把握します。重要な事業資産を完全かつ継続的にコントロールできます

悪意のある脅威の検出

運用の継続性を脅かすマルウェアやランサムウェアなどの脅威を早期に検出して損害が被る前に効果的に対処することで、計画外のダウンタイムを防ぐことができます

操作ミスによる脅威の検出

日常的に発生して、運用環境に重大な損害を与えかねない悪意のない問題に対して洞察を得ることができます。業務停止を招きかねない人為的過失、設定ミス、機器の誤作動などのインシデントを検出します

フォレンジックとインシデント対応

報告されたインシデントに関する情報をすべて受け取り、根本的な原因を理解します。高度なフォレンジックツールを使用してアラートの原因を解明し、推奨事項を修正することでインシデントに対応できます

企業管理システムとの統合

SOCやSIEMなど既存の企業管理システムとの統合をサポートしています。社内管理またはMSSPによる管理に関係なく、OTで発生したインシデントの効果的な管理や、ITセキュリティのワークフローへの統合が可能です

セキュリティとポリシーの強制

サードパーティ製のインシデント管理プロダクトやファイアウォールと統合された高度なイベント管理・報告ツールにより、インシデント処理の効率化、文書化を実現してIT/OTセキュリティ（工場セキュリティ）の管理を総合的に改善します

ものづくり現場ならではのニーズに対応

SCADAfenceプラットフォームの優位性は、大規模で複合的な産業ネットワークを監視することを目的として、様々なニーズに対応可能な知見と、多種多様な先端機能を備えていることにあります。DXが加速する現代において変化が著しい工場インフラにも柔軟に対応し、高度なセキュリティと運用健全性をもたらします。

1 数万に及ぶ資産の監視

SCADAfenceプラットフォームでは、数万に及ぶ資産とセッションの情報を監視できます。搭載されたネットワークマップは、膨大な資産を簡単に表示することを目的に設計されているため、各資産の関連情報や詳細情報を段階的に掘り下げることができます。モデル番号、ファームウェアバージョン、潜在的なリスクなど資産に関するさまざまな情報の自動検出が可能です

2 ディープ・パケット・インスペクションに対する知見の蓄積

SCADAfenceプラットフォームでは、IT/OTプロトコルの両方に対してDPIの実施を可能としています。当社リサーチ部門ではさまざまなバージョンで産業用プロトコルの最新情報を維持して、ベンダーに合わせたカスタマイズへの対応に取り組んでいます。最先端のプラントや運用ネットワークの設計、構築の専門家チームからなる世界クラスの産業ラボを備え、さまざまなタイプのPLC、HMI、ベンダー独自のエンジニアリングソフトウェア、プロトコル・コンバーター、I/Oモジュールなどの機器を運用しています

3 動的なベースラインテクノロジーの採用

SCADAfenceプラットフォームはユーザー特有のネットワーク動作を学習し、その動作基準から逸脱した動作を検出します。ハードコーディングで設定されたパラメータの場合、厳しすぎて誤検知を誘発したり、緩すぎて違法行為を許したりするなど運用中のネットワーク特性に適さないことがありますが、SCADAfenceのシステムは自動的に動作基準を学習し、ノイズのレベルやイベントの種類などネットワーク動作のパラメータの設定が可能。ホストや動作タイプなど、ネットワークのイベントごとに調整を行うきめ細かな学習機能に加えて、ユーザーのフィードバックに基づいた調整も行います

SCADAfence

SCADAfence Ltd.

〒103-0023

東京都中央区日本橋本町3-3-3

Clipニホンバシ

03-4588-5432

https://www.scadafence.com/ja/

info-jp@scadafence.com