SCADAfence

情報システム責任者と生産技術責任者
双方の異なるKPIを達成する方法

# IoT時代の製造業における資産管理とリスクマネジメントのベストプラクティス

# もくじ

IoTの進化が急速に進む今、製造業の現場では大きな変化が起こっています。機械設備がネットワークに接続されたことで、サイバー攻撃の脅威が急速に増しているのです。事実、国内外の工場では外部からの悪意ある攻撃により生産設備が稼働停止したり、設備不良により不良品が製造・出荷されたりする事態も発生しています。IT／ものづくり現場のネットワークの統合が進む今、果たしてどのようなアプローチが求められているのでしょうか？

本書は、情報システム責任者と生産技術責任者の方々が、外部からの脅威に対応しつつ「生産性向上」という命題に向き合うために有効なベストプラクティスをご紹介するものです。生産性向上とリスクマネジメントという異なるテーマへの対応を求められる情報システム責任者・生産技術責任者の方々には、ぜひご一読いただきたい内容を収録しています。

# 機器のIoT化に伴い進む IT／ものづくり現場のネットワーク統合

Chapter

1

# IT／ものづくり現場のネットワーク統合に伴い発生するサイバーセキュリティリスク

今、製造業界では、IoTを始めとするテクノロジーを駆使した「スマートファクトリー (つながる工場)」が大きなトレンドとして広まりを見せています。このコンセプトが実現することで、各種指標の見える化による生産効率向上、設備稼働状況の傾向分析を基にした障害検知・予防保全など、さまざまな価値の創出が期待されています。その一方で、工場内の各設備がOT（Operational Technology）設備と接続し、それらがITネットワークにも接続されることで、新たな脅威が表出化しています。近年、国内外の工場に操業停止等の被害をもたらしている「サイバー攻撃」です。

## サイバー攻撃の被害は設備故障にとどまらない

OT設備と工場設備を狙ったサイバー攻撃は、ITネットワークに対するものとは目的が異なります。後者が情報を盗むために行われていることに対して、前者（ものづくり現場への攻撃）は工場設備や生産している製品そのもの、延いては生産活動への悪影響を狙ったものといえます。

例えば、ドイツの製鉄所では、eメールを介して攻撃者が情報（IT）ネットワークに侵入。さらに、OT設備に接続されていた生産設備の制御システムに侵入したことで、溶鉱炉の不具合を発生させて設備へ損傷をもたらすなど、深刻な被害を与えています。他にも、米国の自動車工場では、制御システムにウイルスが侵入したことで、ネットワークで繋がっていた計13工場にウイルス感染が拡大。組み立てラインで生産に携わっていた50,000人の作業が中断したことで操業停止に陥り、1,400万ドルの被害が発生しました。

## 少しの油断が「リコール発生」に繋がる恐れも

操業停止以外にも、深刻な被害をもたらした事例が国内に存在します。日本国内のある工場では、現場に持ち込まれたUSBメモリを介して、最終工程の品質検査装置にウイルスが感染。この影響で、本来は不良品として判定されるべき製品がそのまま出荷され、リコールを行う事態にまで発展しました。

このように、テクノロジーの活用によって新たな価値を生み出すためには、同時に降りかかってくる新たな脅威と向き合うことが求められます。

# IT部門とものづくり部門の連携が求められている

製造業の現場がサイバー攻撃に対応するためには、どのような対策が求められるのでしょうか？ここで忘れてはいけない視点は、いまや**ものづくりの領域はIT（情報システム）と切っても切れない関係性にある**、ということです。かつて、工場の生産設備はネットワークとは切り離され、隔離された状態での運用が当然でした。そのため、ものづくり分野では、「ソフトウェアライフサイクル管理」といった考え方は浸透しておらず、それらのメンテナンスもITとは異なるルールの元で行われているケースがほとんどだったのです。しかし、消費者ニーズが目まぐるしく移り変わり、オペレーションの高度化・デジタル化が必須要件となった今、ものづくりの領域にもITと同等のソフトウェアマネジメントやリスク管理が求められています。そして、これら業務の担い手として重要な役割を果たすのが、かねてよりサイバーセキュリティへの対策を行ってきた「情報システム部門」となります。

## 情報システム部門の一貫した取り組みが成否を決める

IT領域で行わているセキュリティ対策は、自社のものづくり現場下ではどの程度行われているでしょうか？例えば、次のようなポイントについて、現状のセキュリティ対策を確認してみましょう。

**セキュリティ対策で行う業務例**

- ソフトウエアライセンスの管理
- ソフトウエアの構成管理
- 開発／運用プロセスの標準化
- リリース管理
- バージョン管理
- パッチ適用管理

現在は更新頻度が少ない工場設備のソフトウェアも、生産設備のデジタル化・IoT化が進む中では、比較にならないほどアップデートを行う機会が増えていくはずです。だからこそ個別最適に陥ってしまうような管理手法ではなく、IT／ものづくり現場の全体最適を目的とした管理体制が求められます。

加えて、ものづくり領域でもITと同じように、専門ベンダーからのソリューションの調達、導入・運用管理など、セキュリティ対策と並行した各種業務が発生します。だからこそ、資産管理とセキュリティ対策の双方の視点が必要とされるでしょう。

次章では、これらの視点を実践に移すために押さえておきたい、ベストプラクティスをご紹介します。

# IoT時代の製造業における資産管理とリスクマネジメントのベストプラクティス

Chapter

2

# 「稼働の継続性」が重要視される製造業

まず初めに、ものづくり現場のネットワーク・システム構成を考えるにあたっては、IT領域とは優先順位が異なる点を理解しなければなりません。特に重要な点は「稼働の継続性」が100%に近いレベルで求められるということです。

IT領域では「情報」を扱う一方で、ものづくり領域では「モノ」を扱う上、前後の工程が定められた時間内に繋がり合って初めて意味を成します。何故ならば、モノの温度・形状・状態が少し違うだけで異なる結果をもたらす現場が極めて多いためです。加えて、24時間365日の安定稼働が絶対条件となる現場も多く、IT領域で見かけることのある「サーバーの再起動」といった行為が許されないケースも珍しくありません。

このような各領域の違いを整理すると、次のように表現できます。

**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）<br>サービス（連続稼働） | 24時間365日の安定稼働<br>（再起動は困難） |
| **情報システム（IT）** | 情報の適切な管理<br>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

このような優先順位の違いを前提として、IoTを活用し、生産ラインの見える化を行っていくわけですが、基本となるアプローチは『データの可視化』です。データを可視化することで、一定の指標を設けた上で「目標とするラインに達しているのか、達していないのか」という評価を行えるようになります。

# 製造業のKPIを担う 生産技術部門と情報システム部門

工場のIoT化が進み、各種データの可視化が実現すると、運用状況の改善を重ねるために各部門で一定の指標（KPI）を持つことが必要になります。そして、IoTに工場のインフラとしての機能が求められる時代には、例え部門が違えど、組織内で「同一の指標」を持つことが求められます。

しかし、ここで一つ問題が生じます。ものづくり現場の運用に携わる「生産技術部門」とITの運用を担う「情報システム部門」とでは、抱えているミッションも考え方も、延いては日常的に用いる言語体系すらも大きく異なるのです。事実、IoT化を推進する国内各社でも、あらゆる面における思考・優先順位の違いが障壁となり、多くの苦労を強いられています。

## 両部門を隔てる「分厚い壁」

生産技術部門と情報システム部門との間にある壁は、次のような背景から生まれています。

・ものづくり現場とITとでは、そもそも「文化」が異なるため、コミュニケーションが取りづらい
・工場セキュリティは「予算」の獲得が難しく、ITとは取り組みの優先順位に差異が生まれてしまう
・モノづくり現場は直接的に利益を生み出す部門として位置付けられており、情報システム部門よりも発言力が強い傾向にある
・ものづくり部門が複数存在する企業では、それらの部門間でも業務プロセスが異なるため、統一のセキュリティポリシーでは運用が困難

これらの状況からわかるように、両部門は日常的に運用している指標も異なります。

| | |
|---|---|
| 生産技術部門のKPI | 稼働率、運用効率の向上 |
| 情報システム部門のKPI | セキュリティ、リスクマネジメント |

視点を統一するための新たなKPIを設ける必要があります。

**ここで着目したいのが「生産性向上」という指標です。**

# 生産性向上とセキュリティ対策 双方の取り組みが同時に求められている

## 両者を結び付ける「生産性向上」というKPI

もしも、「生産性向上」という指標を元に、生産技術部門と情報システム部門が運用を始めたとすればどうでしょうか？生産技術部門は生産を最大化させるために、IoTを搭載した設備機器の最適な活用方法を模索し、情報システム部門は、製造現場が生産性を最大化させるために最適な環境を整えることに注力することができます。

このように、まずは異なる部門間のベクトルを統一し、それらを定量的に運用可能なKPIに落とし込むことで、現場のパフォーマンスは更なる向上を目指すことができます。

ものづくり現場のIT化が進む中では、両部門が一体となり、部分的な改善アプローチでは実現が難しかった「更なる生産性向上」が求められます。一方で、ものづくり現場へのサイバー攻撃も日々多様化しており、操業停止のみならず、IT環境への攻撃と似たような手口（例：生産情報の改ざん、レシピ等の重要データの搾取）が増えています。

このような状況下で、製造業の生産性向上ために求められる取り組みをまとめると以下のようになります。

## IoT時代の製造業における生産性向上の取り組み


### ①OT資産管理

生産性向上のためには、生産プロセスの最適化やコスト削減、ヒューマンエラーの予防といった観点が必要なことはいうまでもありません。しかし、こうした取り組みを実施するためにはものづくり現場全体を「可視化」し、正常に稼働率しているかを把握するといった「OT資産の管理」をする必要があります。

### ②リスクマネジメント

そして生産性を最大化させるためには、これらの観点に基づいたセキュリティ対策も日々改善を続けていく必要があるのです。生産性向上に向けた取り組み（OT資産管理）とセキュリティ対策は、決して別々の取り組みではなく、相互に関係し合うものとして取り組む姿勢が欠かせません。

# 生産性向上に欠かせない「OT資産管理」

OT設備に接続した設備機器が増え続ける中、生産性向上の鍵を握る取り組みの一つに「OT資産管理」があります。一見、資産管理というと管理的な側面が大きいように思えますが、これはどのような意味を持つのでしょうか？

## 機器の管理体制を見直し、オペレーションを最適化

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工場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ことがわかります。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、管理やメンテナンス体制、異常時のオペレーションを最適化することで、現場の生産性はより一層高められる可能性を秘めています。

# 生産性向上に欠かせない「リスクマネジメント」（1）

## 製造業におけるリスクマネジメントとは

前述の通り、ものづくり現場へのサイバー攻撃も日々多様化しており、操業停止のみならず、IT環境への攻撃と似たような手口（例：生産情報の改ざん、レシピ等の重要データの搾取）が増えています。生産性向上を図るためにこしたリスクに対する対策は欠かせません。

改めてこのような状況下で製造業に求められるリスクマネジメントを整理すると、次のようになります。

**Safety 安全性**

・装置の誤作動による人身事故
・装置の物理的故障、破損

**Availability 可用性**

・システム異常による生産停止
・システム異常による減産

**Integrity 完全性**

・改ざんによる不良品発生
・生産データの改ざん

**Confidentiality 機密性**

・レシピや生産情報の漏えい
・営業秘密の漏えい

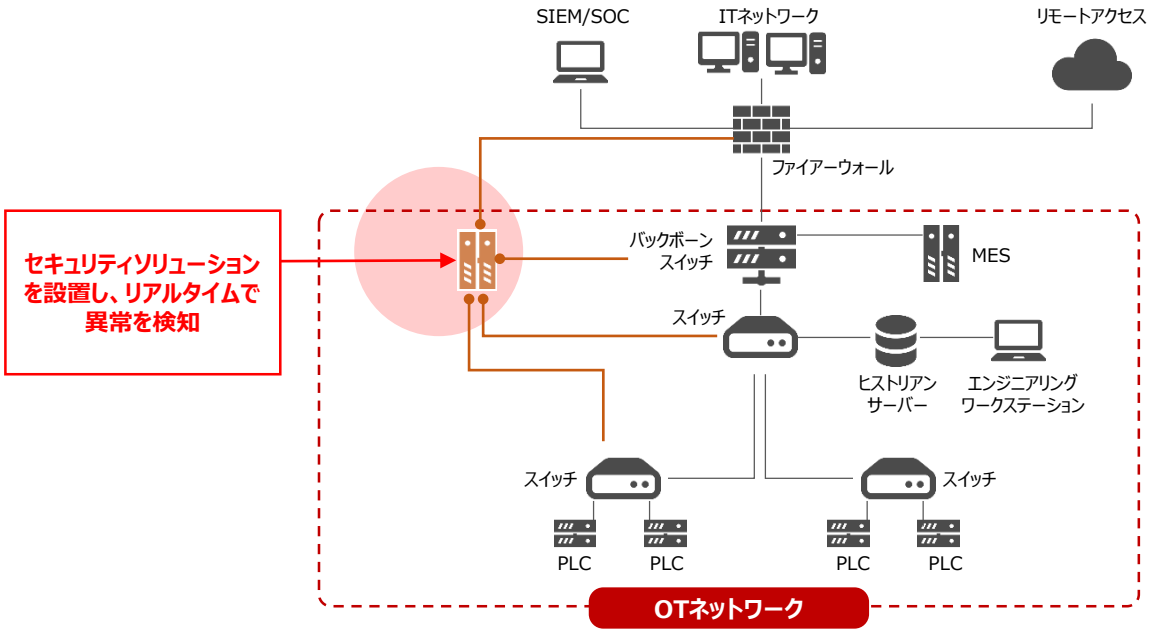
# 生産性向上に欠かせない「リスクマネジメント」（2）

## リスクマネジメントに必要な「リアルタイム分析・異常検知」

最後にご紹介するのは、ものづくり現場の生命線ともいえる「稼働の継続性」を担保する上で欠かせない、『リアルタイム分析・異常検知』に関する観点です。

製造機械やビル設備などは「止めてはいけない」という大前提に基づいているため、サイバー攻撃を受けたり、ウイルスが侵入したりといった脅威に対して事後対応していたのでは、目的を果たすことはできません。もしも復旧までに数時間、数日かかるようであれば、その分だけ損失が拡大し、事業全体に致命的なダメージを与えます。そのような事態を防ぐためにも、ものづくり設備のリアルタイム監視は次のような構成で行うことが理想とされています。

**リアルタイム分析・異常検知のイメージ**




このような異常検知の仕組みを構築し、精緻化していくためには「どこで異常な動作が起こったのか？」「正常時とは異なる命令を発したのは、どの装置か？」といった原因と結果を明らかにするための環境整備が欠かせません。そして、**この環境整備の根底を支えるのが『ネットワークの可視化』**です。上記の図で示したようなネットワーク構造を可視化する「ネットワーク論理構成図」は、常に最新の形を工場内で共有し、異常の早期発見と原因究明に生かすことが望まれます。

# まとめ：双方のKPIを実現する理想的なOT×ITの形とは

今回ご紹介した各種ベストプラクティスの背景には、全体を通じて共通したメッセージが存在します。それは、IoT時代の製造業には部門間を隔てる境目曖昧になり、かつて当然とされていた「分業体制に基づいた組織カルチャー」だけでは生産性の最大化はままならないということです。

ものづくり設備がITネットワークと繋がり、新たな脅威にさらされながらも「生産性向上」という命題と向き合っていくためには、もはや単独の部門だけでは太刀打ちできません。組織一体となって望ましい環境整備を行うためにも、まずは、次のサイクルを念頭に置きながら「生産技術部門」と「情報システム部門」の間での課題共有・指標の統一を行っていきましょう。


そして、上記の「Step3. 環境整備」では、ものづくり現場とIT環境双方のネットワークを可視化し、統合的に管理するためのプラットフォームが欠かせません。次章では、このテーマを実現するために最適な、OT×ITセキュリティ／資産管理プラットフォームサービスをご紹介します。

# SCADA fence
# プラットフォームのご紹介

Chapter

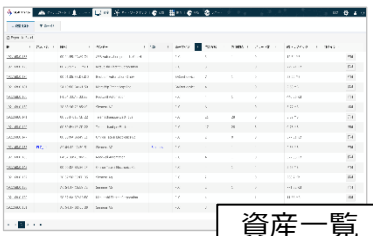
3

# 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

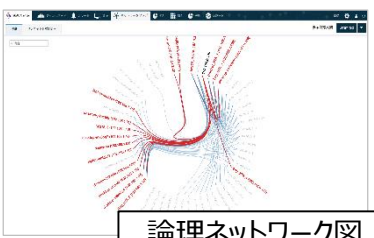


資産一覧

- 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

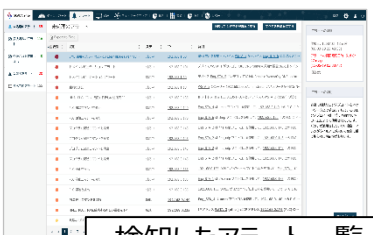


論理ネットワーク図

- 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**