隣の工場がセキュリティ被害で操業停止、うちもターゲットになり得るの？

甚大な事業継続リスクに備える“工場セキュリティ”の踏み出し方

ADD VNTR.

Executive summary

01. 経営課題に直結する、セキュリティリスク＝事業継続リスクの方程式

製造DXによって外部ネットワークとの接続が不可欠な工場では、従来のIT同様、セキュリティリスクへの懸念が高まっています。
今やセキュリティリスクは、信用失墜や販売中止、生産停止といった事業継続に対するリスクに直結します。
大企業のみならず、中堅／中小規模の製造業においても、実際の被害が急増している実態を知るべきです。

02. 現状を知ることから！工場セキュリティに向けた4つのステップ

工場セキュリティに向けては、大きく「現状調査」「リスク評価」「対策・監視の検討」「対策・監視の高度化」の4つのステップで進めていくことが重要です。
なかでも、工場内の現状を把握したうえで、その状況に対するリスクをしっかりと評価しない限り、ゴールの達成は困難です。
グローバルに活用されているフレームワークを用いて工場内の現状把握を徹底的に実施し、
その環境においてどんな脅威が潜んでいるのかを分析するリスク評価という、初歩のステップにいち早く着手することが重要です。

03. マクニカが製造DXに不可欠な工場セキュリティに強いワケ

セキュリティ脅威は海外から。グローバルな最新トレンドを踏まえた対策を講じることができるのは技術商社としての強みを持つマクニカだからこそ。
一般的なコンサルタントが示す机上の空論にとどまることなく、その結果をもとに現場に適した豊富なソリューションを組み合わせながら実装していくことが可能です。

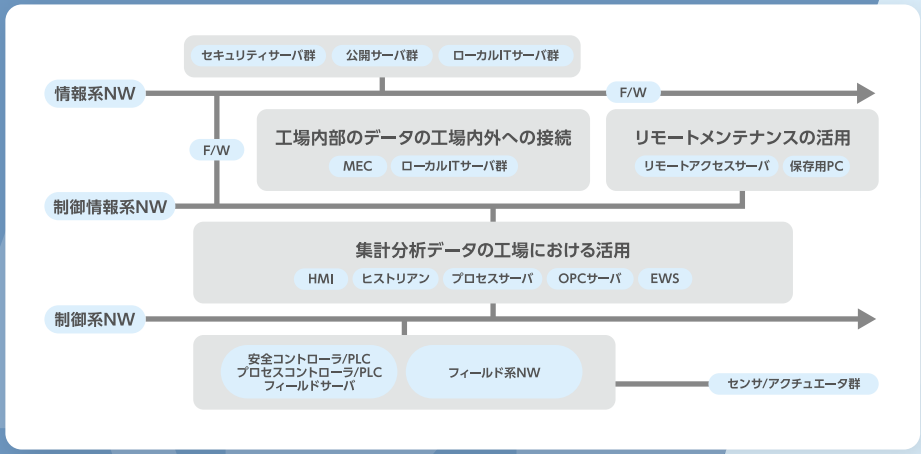
04. 工場セキュリティに向けたマクニカコンサルティング

現状調査では、国際的なフレームワークはもちろん、長年にわたって蓄積された独自の知見を組み合わせ、People（組織・人材）、Process（プロセス）、
System（システム）の観点から20のセキュリティ要件に照らし合わせて、チェックシートによる評価や現場へのインタビューを実施。
現状調査に基づいた工場セキュリティにおける今の課題をいち早く明確化します。

01. 経営課題に直結する、セキュリティリスク＝事業継続リスクの方程式

製造DXで外部との接続が活発に、結果としてセキュリティリスクが顕在化

工場内で発生しているデータを有効に活用し、生産効率の向上やラインの最適化、売上拡大などに向けて、多くの製造業で取り組みが進む製造DX。これまでのような工場内に閉じたネットワークから脱却し、クラウドサービス活用も含めて、外部ネットワークとの接続が必要不可欠です。また、現場で得られたデータは、高度な分析機能を持つ工場外のクラウドサービスにて分析し、自社の工場にフィードバックしていくことになり、外部とデータのやり取りは頻繁に発生することに。さらに外部からのリモートメンテナンスに活用する機会も増えていることでしょう。まに製造DXを推し進めている企業において、工場内システムは大きな転換期を迎えています。その結果、従来のITにおけるセキュリティリスク同様、工場においてもセキュリティリスクは大きなものとなっています。



経営課題に直結する、セキュリティリスク＝事業継続リスクの方程式

しかし、これまで工場において想定されてきた、信用失墜や販売中止、生産停止といった事業継続に対するリスクが、外部からの攻撃をはじめとしたセキュリティリスクと関連づけて認識されていない企業が多く見られます。例えば、外部からの攻撃によって設定情報が変更されてしまい、品質が満たされていないものが市場に出回ることで、信用失墜や販売中止に追い込まれる。また、身代金を要求するランサムウェアなどによってシステムが動かなくなり、結果として生産停止につながる事例も現実的なインシデントとして発生しています。今やセキュリティリスクは、工場を持つ製造業における事業継続リスクといっても過言ではありません。

工場における想定リスクと被害の関係

製造工場を対象にして想定される脅威

- 異常値設定
- システム停止・破壊
- 更なる侵入のための踏み台
- 機密情報窃取
- データ盗難・破壊
- 金銭要求

製造業における事業継続のリスクへ直結

BCPへの影響度が高いリスク

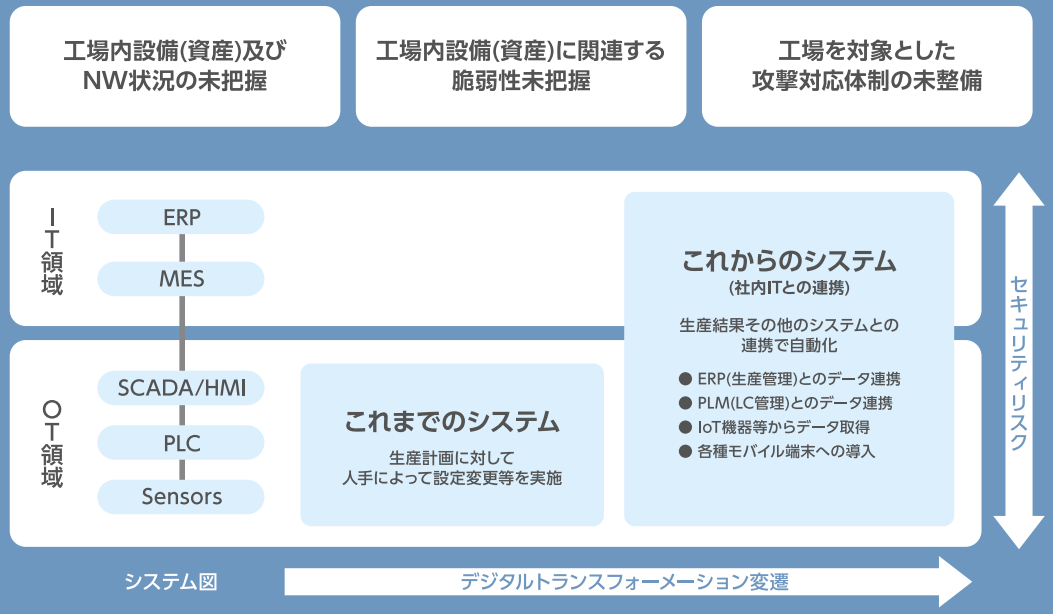
信用失墜
自社製品の欠陥や副作用の他事業投資の失敗、その他財務状況の悪化等により、起こり得るリスク。

販売中止
自社製品の欠陥や副作用、異物混入等により販売中止や製品回収が起こる他、依存度の高い取引先の問題で起こり得るリスク。

生産停止
気候変動や自然災害、また取引先から購入する材料の未入手やシステム停止によって起こり得るリスク。

製造DXで顕在化した、セキュリティリスクの現実

工場におけるセキュリティ対策ですが、製造DXの広がりによって課題が顕在化しています。工場内設備やネットワーク状況が適切に把握されておらず、生産技術部門が独自に設置したIT機器が管理されないまま現場に放置されていることもよく見受けられます。当然ながら、工場内設備にどのようなセキュリティリスクが存在しているか把握されておらず、セキュリティ対策されていない端末や管理外のネットワークが多数存在してしまっているケースもあります。そのリスクが認識されていないがゆえに、万が一サイバー攻撃が発生したときの検知の仕組みやその対応に向けた体制構築などが検討されていないケースが散見されるのです。セキュリティリスクが事業継続リスクにつながることが経営層にも認識されていないため、工場セキュリティにおける責任者が明確でなく、IT関連部門が、自身の主業務に加えて暫定的に工場側のセキュリティを管理せざるを得ないという企業も少なくありません。まさに従来とは異なるシステム領域にまで拡張している製造DXだからこそ、工場セキュリティの課題が浮き彫りになってきているわけです。



システム図

対岸の火事ではない！
企業規模問わず製造業のセキュリティ被害が急増

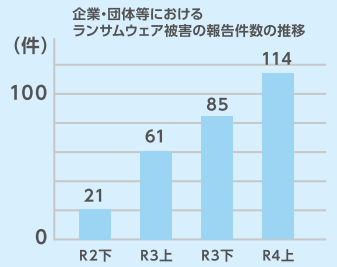
セキュリティインシデントを自社には関係のない、対岸の火事として考えている企業も実は意外と少なくありません。しかし、今や企業規模問わずセキュリティリスクの脅威に晒されており、中堅中小企業にまでのその被害が広がっています。セキュリティリスクが、事業継続に多大な影響を及ぼす時代だということを、しっかりと意識すべきです。

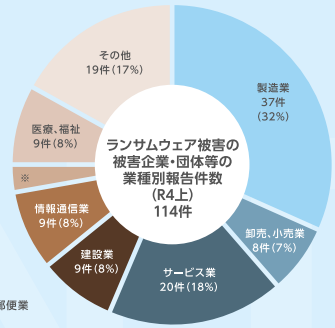
インシデントの半数が中小企業という現実！ランサムウェアの被害実態

2017.6
自動車メーカーの工場(国内)が稼働停止

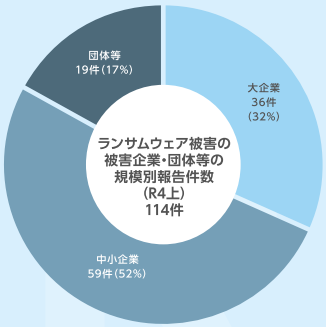
2020.6
自動車メーカーの工場(国内・海外)が稼働停止

2022.6
自動車部品メーカーのサーバー感染により
カーOEM3社の工場が停止





※運輸業、郵便業
3件(3%)



出典:警察庁「令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf
注:図中の割合は小数第1位以下を四捨五入しているため、総計が必ずしも100にならない。

02. 現状を知ることから！工場セキュリティに向けた4つのステップ

サイバーハイジーンとサイバーレジリエンスという2つの視点を念頭に、製造DXに向けた工場セキュリティは、大きく4つのステップで実現していきます。現状調査に向けては、グローバルに活用されているフレームワークを用いて工場内の資産状況を適切に把握したうえで、その環境においてどのような脅威が潜んでいるのかを分析し、それらに対して優先順位をつけていきます。そこでようやく、具体的な対策検討や監視すべき対象の特定などが実施でき、具体的な対策実装に向けて動き出すことができます。その意味でも、まずは工場内での資産や人的リソース、体制などを的確に把握、可視化していき、しっかりとしたリスク評価を行っていくことが重要です。

1 現状調査

対象工場における特定/防御/検知/対応/復旧それぞれにおける現状と課題、改善施策が明確になっている状態。

対策導入　監視体制

セキュリティ活動の現状調査

2 リスク評価

対象スコープ範囲内における保護資産に対するリスク(脅威)とその対応優先順位が確定している状態。

対策導入

脅威の特定と対応優先順位付け

監視体制

既存取得可能なログ等の確認

3 対策・監視検討

リスク評価に基づく対策や、監視項目及び監視運用体制を既存ログから抽出し、監視が開始できている状態。

対策導入

リスクへの対応策の検討と実装

監視体制

監視項目に合う監視体制の実装

4 対策・監視高度化

リスク評価に基づく対策の実装や、実装された対策から得られるログ等を段階を追って監視基盤に集約できている。

対策導入

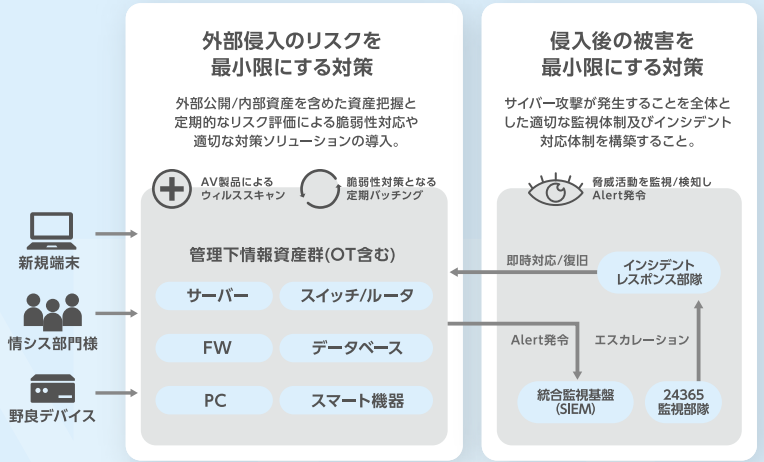
リスクへの対応策の検討と実装

監視体制

都度実装される対策の可視化

工場セキュリティに必要な「サイバーハイジーン」「サイバーレジリエンス」

工場セキュリティの環境整備において、どんなフレームワークに沿って対応を進めていくべきなのでしょうか。工場セキュリティにおける対策フレームワークは、大きくは「特定」「防御」「検知」「対応」「復旧」というフェーズごとに、組織体制や人材の確保から、基準や手順の策定、そして高度な技術を踏まえた仕組みづくりが求められます。これらのフレームワークで重要になるのが、サイバー攻撃を防ぐための予防としてのサイバーハイジーン(衛生管理)とサイバー攻撃を受けることを前提とした対処としてのサイバーレジリエンス(復旧・回復力)という2つの視点です。



03. マクニカが製造DXに不可欠な工場セキュリティに強いワケ

工場セキュリティを実現するために、最良のパートナーとなり得るのがマクニカです。マクニカでは、工場セキュリティを専門に扱う事業を展開しており、コンサルティングを武器に多くの実例から知見を獲得していることが大きな強みです。ITネットワークとつながるOTネットワークだからこそ、ITセキュリティを知見を活かした対策に精通していることもマクニカの特徴です。特にマルウェアをはじめとしたセキュリティ脅威につながる攻撃は、海外で暗躍する組織化されたハッカーなどが手掛るケースがほとんど。だからこそ、グローバルで発生しているインシデントや海外で講じられている対策を参考にしながら、自社の環境に最適な実装が必要です。技術商社であるマクニカは、日本国内のみならず、海外の最新トレンドを踏まえた対策を講じることができ、しかも、標準的なリファレンスにとらわれることなく、リアルな攻撃の最新トレンドをおさえながらベストプラクティスを提供。一般的なコンサルタントが示す机上の空論にとどまることなく、その結果をもとに現場に適した豊富なソリューションを組み合わせながら実装していくことが可能です。

1 商社機能を用いた世界中の知見

製造業のグローバル展開に合わせた、
世界中の標準化知見、
技術知見を所有し、
顧客の目指す姿の実現に寄与する

2 リアルを追求する調査機能

標準化動向のあるべき
論だけはない、リアルに起こっている
攻撃トレンドも考慮した、
ベストプラクティスを
導くことができる

3 商社機能を用いた実現解像度

コンサルティング結果から
机上の空論ではない、
最適な製品/ソリューションを選定し、
導入・運営まで伴走支援

04. 工場セキュリティに向けたマクニカコンサルティング

すぐに取り掛かるべき現状調査やリスク評価ですが、マクニカでは、経済産業省やNIST（米国立標準技術研究所）が示している国際的なフレームワークはもちろん、長年にわたって蓄積された独自の知見を組み合わせ、People（組織・人材）、Process（プロセス）、System（システム）の観点から20のセキュリティ要件に照らし合わせて、チェックシートによる評価や現場へのインタビューを実施。現状調査に基づいた工場セキュリティにおける今の課題を明確化していきます。
具体的には、セキュリティ成熟度やヒートマップに基づく課題サマリや課題詳細、そして改善に向けて取り組むべきロードマップ案などを提示。そこで得られた情報をもとに、対策検討や監視すべき対象の特定などを進め、現場にあった対策や監視の高度化に向けた具体的な実装までを支援します。

FOCUS DOMAINS

- サイバー・フィジカル・セキュリティ対策フレームワーク（CRSF）
- 工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン
- NIST Cyber Security Framework
- IEC 62443-2
- 弊社知見 MACNICA

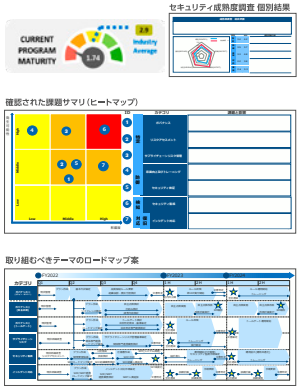
KEY DELIVERABLES

People（組織・人材） / Process（プロセス） / System（システム）

20のセキュリティ要件

1	資産管理	11	製品・システム保守
2	ビジネス環境	12	製品の保護技術
3	ガバナンス	13	異変とイベント
4	リスク評価	14	セキュリティモニタリング
5	リスク管理戦略	15	検知プロセス
6	サプライチェーンリスク管理	16	インシデント対応計画
7	ID管理、認証及びアクセス制御	17	インシデント情報の伝達
8	意識向上及びトレーニング	18	インシデント分析
9	データセキュリティ	19	被害の撲滅
10	情報保護プロセス・手順	20	プロセス・計画改善

ENGAGEMENT OVERVIEW



安心安全な製造DXのセキュリティを実現するコンサルタント

製造業におけるDXは、既存の業務を改革し大きな利益をもたらしうるとして期待されています。しかし、その一方でサイバー攻撃の増加も、大企業だけでなく中堅/中小企業を対象に認められているのも事実です。これまで閉鎖空間である工場内ネットワークも、このDXによってIT化され攻撃の対象となっています。またその適切な対策が何であるかを検討するためには、自社の工場を対象としてセキュリティリスクを把握することが最も近道です。マクニカは、自社のセキュリティリスクの特定から最適な対策の検討と実装、運用まで幅広く支援を行い、製造業におけるDXを支えるケイパビリティを持ちながらも、そのDXによって得られる利益を、損害に変えないセキュリティを追求し続けます。

飯田 洋平
Yohei Iida

マクニカDXコンサルティング統括部
セキュリティコンサルティング部　部長

IoTセキュリティ事業の立上げ後、制御システムを開発・販売する製造業を中心に、製品や工場を対象としたセキュリティリスク可視化と対策と運用建付けを多数従事。現在は、CPSセキュリティの統括組織のセンター長補佐を務める。
【専門分野】制御システムコンサルティング、IEC62443、OTセキュリティ、リスクアセスメント、OTセキュア開発プロセス、セキュリティ中期計画策定　等

まずはお気軽にご相談ください。メールからのお問い合わせはこちら　add-venture@macnica.co.jp