今すぐ実践できる工場セキュリティハンドブック
リスク対策編　第 1.0 版

2024 年 3 月

JNSA 日本ネットワークセキュリティ協会

西日本支部

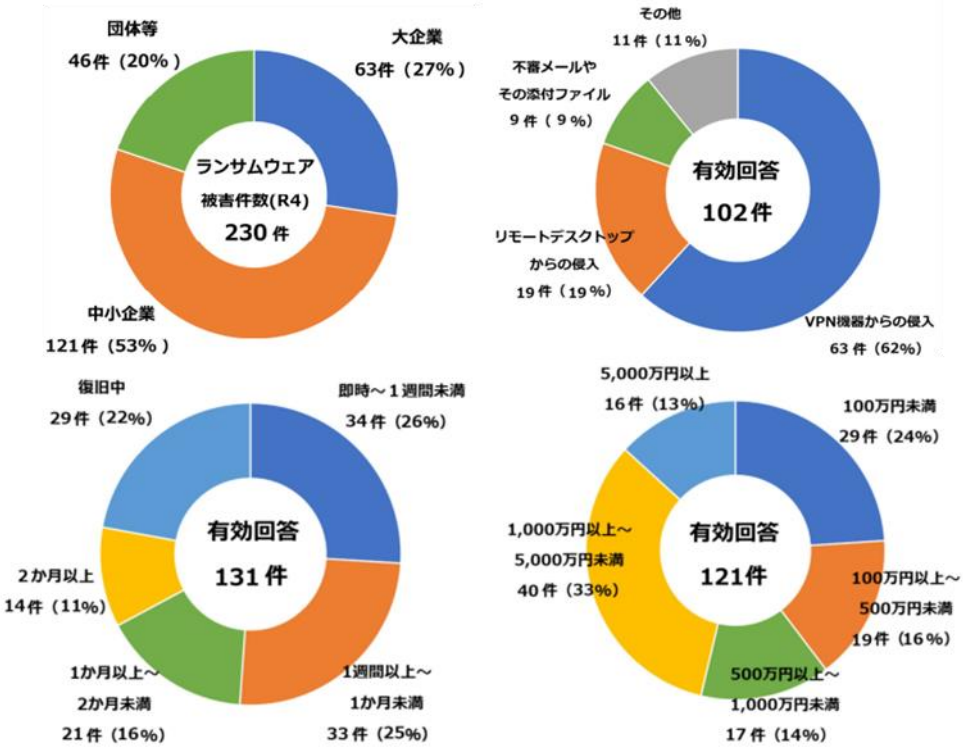
今すぐ実践できる工場セキュリティ対策のポイント検討 WG

目次

工場セキュリティハンドブック・リスク対策編

１．はじめに

ここ数年、ランサムウェアなどによって工場の稼働が停止する事件・事故が増えてきました。これは、これまで比較的、外の環境（例えばオフィス環境やインターネット環境）とは接点を持たず、閉じた環境で稼働していた製造現場が、昨今の IoT 活用や DX の推進などをきっかけに、外部環境と接点を持ち始めたことに関係していると思われます。「うちの工場はインターネットや事務所のネットワークから切り離されているから大丈夫」と思われる事業者も多いようですが、よく調べてみると既にインターネットとつながっていたというケースもあります。また、VPN 接続などで安全に保守事業者と接続しているはずが、ここを攻撃されて侵入される事例やネットワークは外部と繋がっていなくても、保守のために持ち込まれた PC からランサムウェアに感染する事例なども発生しています。



警察庁広報資料令和5年3月16日
「令和4年におけるサイバー空間をめぐる脅威の情勢等について」より引用

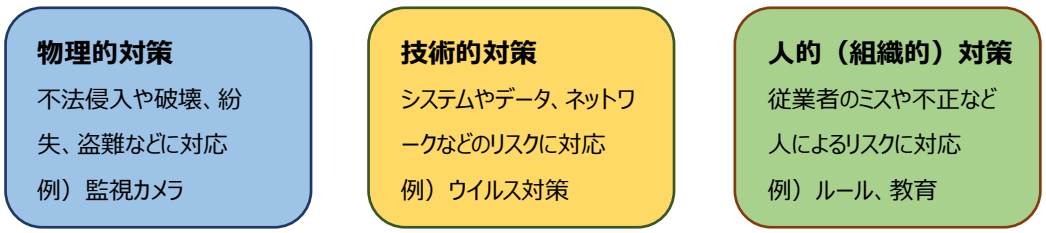
最近、特に注目されているのが「サプライチェーンのセキュリティ」です。製品の企画・開発、原料調達、製造、在庫管理、物流、販売までの一連のプロセスには多くの企業が関係します。このサプライチェーンの中でセキュリティ対策が脆弱な企業を最初の標的とし、そこを踏み台として本命の企業が攻撃されるような事例が発生しています。また、本命の企業が攻撃されなくても、サプライチェーンの一端を担う企業の事業が停止することで一連のプロセス全体が停止してしまう場合もあります。

国内の中小製造業ではセキュリティに対する投資は低調であり、対策はあまり進んでいないのが現状です。資金の問題、人材の問題、スキル・ノウハウの問題など様々な課題を抱えている中でセキュリティリスクは年々大きくなっています。この工場セキュリティハンドブック・リスク対策編は、今すぐにでも取り組める対策から少し高度な対策まで、できるだけ平易な解説と具体的な事例を取り上げ、中小製造業がセキュリティの脅威から自らを守り、事業が継続できるようになるためのセキュリティリスク対策実践方法をまとめたものです。

1．1　ハンドブック･リスク対策編活用の目的

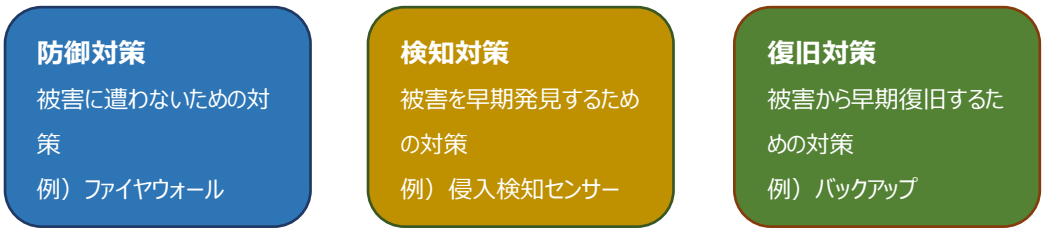
セキュリティリスク対策には、残念ながら万能薬はありません。実際の現場の状況に合わせた対策の選定が必要になります。自社の製造現場における現状を正しく把握するためには、脅威の存在と客観的なリスク評価が必要です。リスクアセスメントについては、「工場セキュリティハンドブック･リスクアセスメント編」を参考にして下さい。

セキュリティリスク対策には、大きく分けて 3 つに分類されます。



セキュリティリスク対策には、どれかひとつの分類で対応すればいいのではなく、組み合わせることが重要です。例えば、基幹システムを守るためには、すべての分類の対策が必要になります。

また、何のための対策かによっても種類が分けられます。



セキュリティ脅威の被害に遭わないためにはできるだけ防御できることが最善ですが、すべてを完全に防御することはできません。また、過度な防御対策は大きな費用がかかるだけでなく、社内システムやデータの活用を損なう場合もあります。工場セキュリティリスク対策で重要なことはバランスです。本ハンドブックは、自社の状況に合わせて、バランスよく対策を実践するための参考書として活用されることを目的としています。

1．2　対象事業者

設計から出荷までの製品製造工程の中で、コンピュータおよび電子技術を利用し、計算や情報の処理および組み立てや加工、検査などを自動的に行う設備を導入している中小製造業（製造される物の分野は問いません）が対象となります。

1．3　セキュリティリスク対策実施者

本ハンドブックを参考にしたセキュリティリスク対策は、経営者および情報システム責任者、製造現場責任者が推進し、製造現場責任者、工場システム担当者、情報システム担当者、もしくはこれに準ずる担当者が実施することを想定しています。（対策によっては外部の専門家に依頼する必要があるものもあります）

１．４ セキュリティリスク対策対象

本ハンドブックがセキュリティリスク対策の対象とする領域は、コンピュータおよび電子技術を利用し、計算や情報の処理および組み立てや加工、検査などを自動的に行う設備とこれらをつなぐネットワーク、ならびに装置やネットワークが設置された場所とします。

１．５ セキュリティリスク対策後の対応

本ハンドブックを参考にセキュリティリスク対策を実施した後の対応を支援するために、以下の続編を予定しています。併せてご活用下さい。

●工場セキュリティハンドブック・サイバーBCP 策定編（工場セキュリティに着目した BCP 策定のヒント）

2．工場セキュリティリスク対策

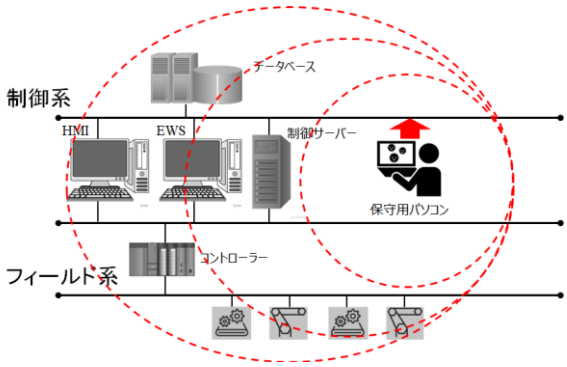
製造現場におけるセキュリティリスク対策とはどのようなものなのか、セキュリティリスク対策を決めるためにはどのような点に注意が必要なのか、セキュリティアセスメント結果とセキュリティリスク対策はどのようにつながるのかなどについて解説します。

2．1　製造現場におけるセキュリティリスク

リスクとは「損害を受ける可能性」であり、これを現実のものにする引き金が「脅威」、この脅威を受けてしまう弱点が「脆弱性」です。従って、脆弱性がなければ、リスクは現実のものにはならないということです。では、実際の製造現場には、どのような脆弱性と脅威があるのでしょうか？まずは脅威の入口となり得るものの例を下記に列挙します。

＜USB メモリー＞ ＜パソコン＞ ＜スマホ･タブレット＞ ＜IoT 機器･センサー＞ ＜複合機＞ ＜ハンディターミナル＞ ＜OA ネットワーク＞ ＜インターネット＞ ＜Wi-Fi＞ ＜機器保守用回線＞ ＜クラウド＞ ＜電子部品･原材料＞ ＜新規導入機器＞

これらの入口に脆弱性があった場合、どのようなリスクが考えられるのか、一例を示します。



保守用パソコンがマルウェアに感染していることを知らずに製造現場 LAN に接続してしまうと、ネットワークの通信速度に比例してマルウェアが工場内の装置に広がります。マルウェアに感染した装置は正常に動作せず、工場全体が止まってしまいます。

【解説】マルウェア
マルウェア（malware）とは、不正かつ有害に動作させる意図で作成された、悪意のあるソフトウェアや悪質なコードの総称。コンピュータウイルスが代表例。感染拡大には様々な方法が使われる。

（詳細は「工場セキュリティハンドブック・リスクアセスメント編」を参考にして下さい）

2．2　セキュリティリスク対策の位置づけ

これまで、製造現場では生産を継続させるために災害などに備えたリスク対策や緊急時の対応方法などが事前に準備されてきましたが、セキュリティリスクに対してはあまり意識されていませんでした。しかし、現在においては、災害と同等かそれ以上にセキュリティの脅威は高まっており、生産を止めないためには、セキュリティリスク対策が不可欠となってきました。セキュリティの脅威は目に見えない状態で侵入してきます。しかも、同時に多数の機器が被害を受け、気が付いた時には既に手遅れの状態となってしまうこともあり

ます。また、停止した機器を代替えの機器と交換するなどの対応をしても、再度、攻撃の影響を受けてしまうなど、復旧も極めて困難になるケースもあります。

何らかの事業を営んでいる上で、その規模の大小を問わずセキュリティ被害に遭わない保証はありません。セキュリティリスクは経営に直結する課題であることを理解し、適切な対策を行う必要があります。

２．３ セキュリティリスク対策の実施

セキュリティリスク対策を実施する前にセキュリティリスクアセスメントを実施して、どこに弱点があるのかが把握できていることを前提とします。セキュリティリスク対策の観点は以下の通りです。

① この弱点をなくすこと
② 弱点を攻められないように防ぐこと
③ 防げないなら攻撃を受けていることを素早く検知し、更なる攻撃を防ぐこと
④ これもできなければ速やかに復旧させること

「工場セキュリティハンドブック・リスクアセスメント編」を活用したセキュリティリスクアセスメントでは、概ね上記のような順番で現状が把握できるようになっています。

セキュリティリスク対策においては、ひとつの脅威の入口に対して、ひとつの対策を行えば大丈夫ということではありません。完全な防御は困難なため、①の対策ができない場合は、②～④を組み合わせる必要があります。

また、対策を選択する際には、確実に運用が継続できるかどうかがポイントになります。割り当てが可能なリソース（人やお金など）を考慮し、無理のない対策を確実に運用することがもっとも重要です。

次の章では、具体的なセキュリティリスク対策の例を解説します。

3　工場セキュリティリスク対策の実践

本ハンドブックで紹介するセキュリティリスク対策は、工場に内在するリスクを網羅的に扱うものではなく、今すぐにでも取り組まなければならない緊急性の高いセキュリティリスクの対策に重点が置かれています。また、それぞれの対策では、分類や種類、運用のポイントなどが簡潔に整理されており、対策選定の参考になるように工夫されています。

3．1　セキュリティリスク対策の対象となる脅威シナリオ

緊急性が高いと考えられるリスクを引き起こす脅威は、製造業における過去の情報セキュリティ事故事例や、本ハンドブック検討メンバーの知見から 13 の入口として定義されています。表 1 は、本ハンドブックにおけるセキュリティリスク対策の対象となる脅威シナリオの一覧です。

No	脅威の入口	脅威が引き起こす可能性のある事象	懸念されるリスク
1	USBメモリー	USBメモリーから制御システムや製造装置にマルウェアの感染が広がる	工場停止
2	持込パソコン	持込パソコンから制御システムや製造装置にマルウェアの感染が広がる	工場停止
3	スマホ・タブレット	スマホ・タブレットに感染したマルウェアが利用者の意図しない動作をさせる	情報漏洩
4	IoT機器・センサー	IoT機器・センサーが第三者に遠隔操作される	工場停止
5	複合機	複合機が第三者に遠隔操作される	情報漏洩
6	ハンディターミナル	ハンディターミナルに感染したマルウェアがプログラムやデータを改竄する	情報改竄
7	OAネットワーク	OAネットワークからマルウェアの感染が広がる	工場停止
8	インターネット	インターネットからマルウェアの感染が広がる	工場停止
9	Wi-Fi（無線AP）	Wi-Fi通信が傍受されたり、通信が妨害される	情報漏洩
10	保守用ネットワーク	保守用ネットワークからマルウェアの感染が広がる	工場停止
11	クラウドサービス	認証情報が不正に利用される	情報漏洩
12	部品・原材料	組み込んだ部品のセキュリティ不具合が悪用される	品質低下
13	新規購入機器	新規購入した機器から制御システムや製造装置にマルウェアの感染が広がる	工場停止

表 1　脅威シナリオ一覧

3．2　セキュリティリスク対策集

それぞれの脅威シナリオに対して実施したセキュリティリスクアセスメントの結果を踏まえて、別紙「工場セキュリティリスク対策ハンドブック・リスク対策集」から適切な対策を選択して下さい。

４．付録

４．１　用語集

【製造装置】
工場内で稼働している製造に関わるすべての装置

【製造現場 LAN】
工場内に設置された Ethernet ベースの有線ネットワークおよび Wi-Fi ベースの無線ネットワーク
工場ネットワーク、OT ネットワークとも呼ばれる

【機密性(Confidentiality）】
許可されていない個人、グループ、組織、システムに対して、情報を使用不可又は非公開にする特性

【完全性(Integrity）】
情報資産の正確さ及び完全さを保護する特性

【可用性(Availability）】
許可された個人、グループ、組織、システムが要求したときに、アクセス及び使用が可能である特性

【脅威(Threat）】
情報資産（装置などのハードウェアも含む）の機密性、完全性、可用性に危害を与える原因となる事象で、人為的(意図的、作為的)なものと環境的(地震、落雷など)なものに分類される

【脆弱性(Vulnerability）】
脅威によって利用されるおそれのある弱点

【リスク】
情報セキュリティにおけるリスクとは、情報システムとそのデータやその他の様々な情報資産に損害や悪影響を与える可能性のこと。

リスクの大きさ　＝　資産の価値　×　脅威の程度　×　脆弱性の程度

で表されることが多い。

【リスクアセスメント】
情報セキュリティに関係するリスクを洗い出し、これを分析してその大きさなどを評価すること。リスクに対する対処を含めてリスクマネジメントと呼ぶ。

【マルウェア（malware）】
不正かつ有害に動作させる意図で作成された、悪意のあるソフトウェアや悪質なコードの総称。コンピュータウイルスやワーム、トロイの木馬などが含まれる。特にワームは単独で感染を広げ、悪質なものが多い。

【ランサムウェア】
身代金（Ransom）とソフトウェアを組み合わせた造語。暗号化などによってファイルを利用不可能な状態にし、そのファイルを元に戻すことと引き換えに金銭を要求するマルウェアのこと。最近では、窃取した情報の公開を身代金取引に使うケースもある。

【ファイアウォール】
ネットワークの通信において、その通信を許可するか拒否するかを判断する機能をもつもの。専用のハードウェアや PC 上のアプリケーションなどがある。

【セキュリティパッチ】
情報システムの脆弱性（欠陥）を修正するためのプログラムのこと。新たに脆弱性が発見されると、そのシステムの提供ベンダーからインターネット等で配布される。

【Wi-Fi（無線 AP）】
国際標準規格である IEEE 802.11 規格を使用したデバイス間で相互接続ができる無線 LAN に認められた名称。無線 AP は、この規格に準拠した装置で、無線通信を中継したり有線通信の機器に接続したりするもの。AP は「アクセスポイント」の略

【デジタル証明書】
インターネットの世界で持ち主の情報を正しく証明するためのデータで、現実世界における身分証明書（パスポート、印鑑証明書、運転免許証など）に相当する。デジタル証明書は、認証局と呼ばれる信頼できる第三者機関が発行する。

【MAC アドレス】
ネットワーク機器やネットワークアダプター（LAN カードなど）に割り当てられるユニークな識別番号のこと。世界中で MAC アドレスは重複しない。一般的に 12 けたの 16 進数で表され、前半の 6 桁がその製品のメーカー固有の数値になっている。

WG メンバー

青木　茂　（協力者）
秋山　健一（日本電気株式会社）
大財　健治（ケー・コンサルタント）
岡本　登　（WG リーダー／富士通株式会社）
金子　啓子（JNSA 顧問）
河島　君知（エヌ・ティ・ティ・データ先端技術株式会社）
木村　哲也（兼松エレクトロニクス株式会社）
小柴　宏記（ジーブレイン株式会社）
近藤　伸明（株式会社神戸デジタル・ラボ）
塩田　廣美（協力者）
嶋倉　文裕（富士通株式会社）
田中　駿悟（フューチャー株式会社）
谷川　貴幸（フューチャー株式会社）
西川　和予（プライムコンサルティング）
西本　敦司（アイネット・システムズ株式会社）
古川　佳和（大阪商工会議所）
松谷　和博（株式会社ソリトンシステムズ）
元持　哲郎（アイネット・システムズ株式会社）
吉崎　大輔（アクセンチュア株式会社）
米澤　美奈（西日本支部長／株式会社ソリトンシステムズ）

敬称略・五十音順