「工場セキュリティハンドブックのご紹介と演習との相乗効果について」

日本ネットワークセキュリティ協会（JNSA）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」

WGリーダー　岡本　登

2023年2月1日

多くの工場が抱える課題

判断が個人まかせ

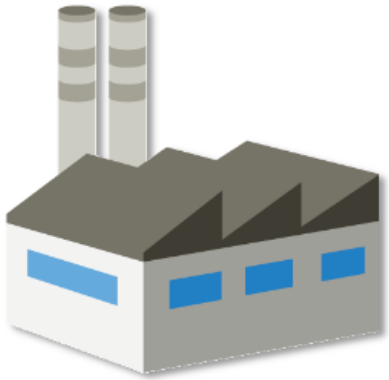
セキュリティルールが明確ではない

ネットワークの流量・内容を監視していない

異常がわからない

全体が把握できない

工場全体のネットワーク担当がいない



ネットワークへの不正接続が検知できない

外部から攻撃される

原因調査ができない

正確なネットワーク図面や装置一覧がない

ネットワークがセグメント化されていない

被害が広範囲に及ぶ

復旧が手探りになる

BCPにサイバーリスクが考慮されていない

マルウェア対策機能や脆弱性対処パッチが適用できない

マルウェアに感染する

現場で活用できるものを作る

機器故障・火災・自然災害に対する対策は取り組んでいるが、セキュリティ脅威で工場が止まった経験がない（想像できない）

中小企業の工場が止まれば日本のものづくりは止まる（サプライチェーン）

【課題】情報部門との環境差、厳しい経営、工場の人材

セキュリティに詳しくない方でも、自社工場のセキュリティリスクが把握でき、どのような状況にあるのかを客観的に理解し、対策ができる**参考書のようなものを作りたい、現場に届けたい**というWGの理念

工場セキュリティハンドブック

リスクアセスメント編

セキュリティリスクアセスメントを自らの手で実施できる参考書
2022.6 初版公開

リスク対策編

自社の環境に合ったセキュリティ対策が選択・実行できる参考書
2023.春 初版公開予定

サイバーBCP策定編

従来の災害対応BCPにセキュリティ観点を加えるための参考書
2023.夏 初版公開予定

リスクアセスメント・ハンドブックの概要

- 情報セキュリティの脅威による**危険性や有害性を特定**し、対策を行うための第一歩として活用できる参考書として作成しました。

- 中小企業において、製造現場で従事する方々が、容易にセキュリティ対策に取り組んでいただけるように、できるだけ**平易な解説と具体的な事例**をもとに実践方法をまとめました。

- 本ハンドブックでは、**リスクベースアプローチ**を主体として、情報セキュリティにあまり詳しくなくても実践できるような方法を採用しました。

13の脅威の入口（リスクシナリオ）

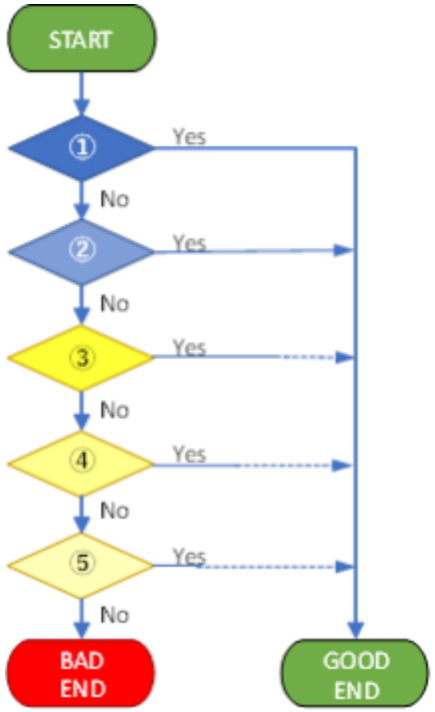
No	脅威の入口	脅威が引き起こす可能性のある事象	懸念されるリスク
1	USBメモリー	USBメモリーから制御システムや製造装置にマルウェアの感染が広がる	工場停止
2	持込パソコン	持込パソコンから制御システムや製造装置にマルウェアの感染が広がる	工場停止
3	スマホ・タブレット	スマホ・タブレットに感染したマルウェアが利用者の意図しない動作をさせる	情報漏洩
4	IoT機器・センサー	IoT機器・センサーが第三者に遠隔操作される	工場停止
5	複合機	複合機が第三者に遠隔操作される	情報漏洩
6	ハンディターミナル	ハンディターミナルに感染したマルウェアがプログラムやデータを改竄する	情報改竄
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	WiFi（無線AP）	WiFI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

※全ての脅威を網羅するものではありませんが、世の中で発生している事故の原因はほとんど含まれていると考えています。

独自のアセスメント手法

リスクシナリオ：持込パソコン

製造装置保守のために製造現場LANに保守用PCを接続したところ、当該製造現場の装置（もしくはその他の製造現場の装置）の動作が異常となった。



現状の対策状況	対策の効果等
①マルウェアチェック済の許可されたPC以外は接続しないルールを確実に運用している	安全な状態でPCが利用できる
②製造装置にマルウェア対策を導入している	マルウェアに感染したPCが持ち込まれても、製造装置側でマルウェア感染が防げる
③PCが製造現場LANに接続されたことがすぐに検知できる	無断でPCが接続されても、すぐに取り外すことができる。ただし、既にマルウェアが拡散してしまった可能性がある
④製造現場LANの通信内容をモニタリングしている	マルウェアの感染拡大の動きを検知して、蔓延する前に対処することができる
⑤製造装置の動作不良の原因調査にはセキュリティ観点も加えている	装置ログや通信ログを分析して、何らかのマルウェアが原因であることが判明すれば、適切な応急・復旧処置ができる

- **現状をシンプルに評価できる**
- **対策の効果が理解できる**
- **リスク対応レベルがイメージできる**

結果の把握（例）

脅威の入口	現状	留意点
USBメモリー	①	
持込みパソコン	BAD	実態が把握できていない
スマホ・タブレット	②	
IoT機器・センサー	①	
複合機	①	
ハンディターミナル	④	古い機種の入れ替え検討が必要
OAネットワーク	BAD	接続されているかどうかを詳細に調査する必要あり
インターネット	①	
WiFi（無線AP）	③	管理者が明確になっていないものがある
保守用回線	BAD	ベンダー任せで詳細が不明
クラウドサービス	①	
部品・原材料	①	
新規購入機器	③	ベンダー任せで詳細が不明

ハンドブックとTTX(机上演習)との相乗効果

【工場緊急時生産管理体制TTX】

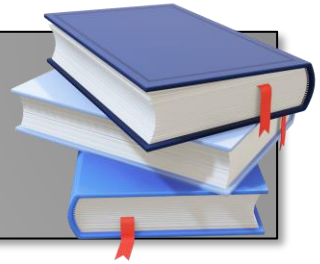
TTXは、サイバー攻撃を引き金事象の一つとして捉え、その影響が生産管理にまで及んだ際、**工場生産を継続するためにはどのような対応をすべきなのかを演習の模擬体験を通じて考える**ものです。単にITシステムの運用を維持するための対応ではありません。

課題議論を
フィードバック

課題解決への
有効利用

【工場セキュリティハンドブック】

工場セキュリティハンドブックは、中小製造業の現場の皆さんが**自らの手で情報セキュリティリスクを把握し対策を考え、これを運用する**ための参考書を目指しています。従って、その領域はITシステムとこれに関連する運用が中心となります。



最後に

「JNSA　リスクアセスメントハンドブック」で検索！


JNSA