成果物発表
「リスクアセスメントハンドブック」のご紹介

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

2022年5月13日

ワーキンググループの概要

- 名称　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
- 期間　2020年10月～2023年3月
- メンバー数　24名（随時参加受付中）／リーダー：岡本　登
- 目的　現場実態を考慮したセキュリティ対策の考え方や新たなサイバー対応BCP策定に必要な観点などを整理し、中堅・中小製造現場のセキュリティ向上を支援する
- WG開催　基本的に月１回の集合＆オンライン検討会
- 予定成果物　リスクアセスメント、対策、BCPの関するハンドブック

WGメンバーの紹介

メンバー：青木　茂　（協力者）
秋山　健一（日本電気株式会社）
家富　和寿（NECプラットフォーム株式会社）
井上　陽一（JNSAフェロー）
今西　幸一（株式会社インターネットイニシアティブ）
沖　裕之　（株式会社ソリトンシステムズ）
大財　健治（協力者／ケー・コンサルタント）
岡本　登　（富士通株式会社）
金子　啓子（JNSA顧問）
兼子　竜也（ニュートラル株式会社）
河島　君知（エヌ・ティ・ティ・データ先端技術株式会社）
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）
田野　久敏（ONWARD SECURITY JAPAN 株式会社）
西川　和予（協力者／プライムコンサルティング）
橋本　護　（株式会社さくらケーシーエス）
古川　佳和（大阪商工会議所）
峯浦　梨紗（富士通株式会社）
元持　哲郎（JNSA西日本支部長／アイネット・システムズ株式会社）
山口　直樹（富士通株式会社）
吉崎　大輔（日本電気株式会社）
米澤　美奈（株式会社ソリトンシステムズ）

5月13日現在
敬称略・五十音順

工場を取り巻く現状

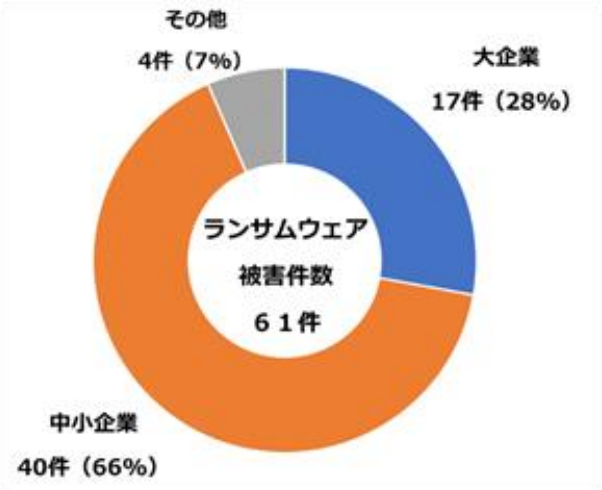
最近の情報セキュリティ脅威

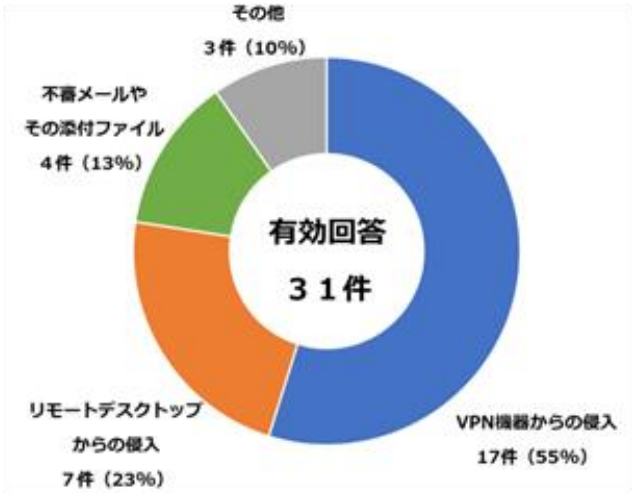
「個人」向け脅威	順位	「組織」向け脅威
フィッシングによる個人情報等の詐取	1	ランサムウェアによる被害
ネット上の誹謗・中傷・デマ	2	標的型攻撃による機密情報の窃取
メールや SMS 等を使った 脅迫・詐欺の手口による金銭要求	3	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	4	テレワーク等の ニューノーマルな働き方を狙った攻撃
スマホ決済の不正利用	5	内部不正による情報漏えい
偽警告によるインターネット詐欺	6	脆弱性対策情報の公開に伴う悪用増加
不正アプリによる スマートフォン利用者への被害	7	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）
インターネット上のサービスからの 個人情報の窃取	8	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	9	予期せぬ IT 基盤の障害に伴う業務停止
インターネット上のサービスへの 不正ログイン	10	不注意による情報漏えい等の被害

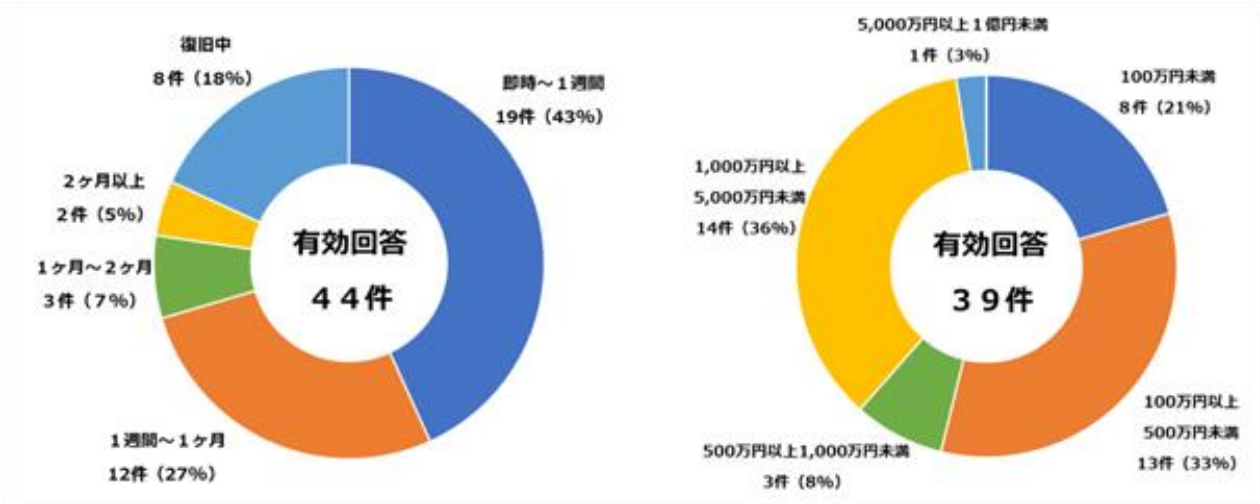
国内外で工場の操業が停止する事故が数多く発生しています

IPA「情報セキュリティ10大脅威2022」より引用

実際の被害状況

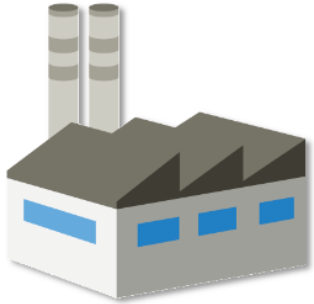






警察庁広報資料令和3年9月9日
「令和３年上半期におけるサイバー空間をめぐる脅威の情勢等について」より引用

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

WG活動の狙い

危機感を共有する

WGスタート時の状況

OA系の情報セキュリティに詳しい方でも、工場のセキュリティはよく分からない

情報共有・勉強会から

WGメンバーで事例や経験談を持ち寄り、勉強会から始め、製造業におけるセキュリティ課題や危機感を共有

製造現場の方はもっと分からない。WGメンバーのそれぞれの立場において**日常の活動の中で製造業の方と接する機会に危機感を共有**できると、世の中の関心はもっと高まるはず。

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）

↓

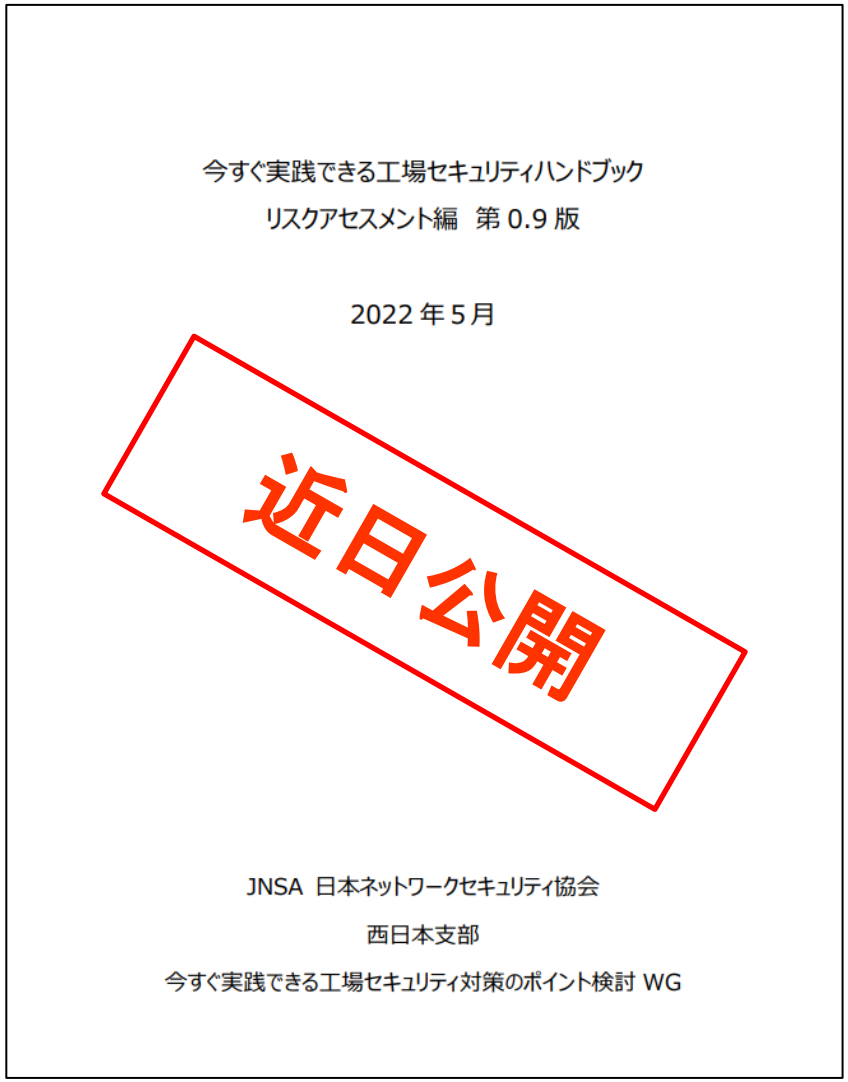
情報部門との環境差、厳しい経営、工場の人材

↓

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）という目的

ハンドブック・リスクアセスメント編

ハンドブック目次


今すぐ実践できる工場セキュリティハンドブック

リスクアセスメント編　第 0.9 版

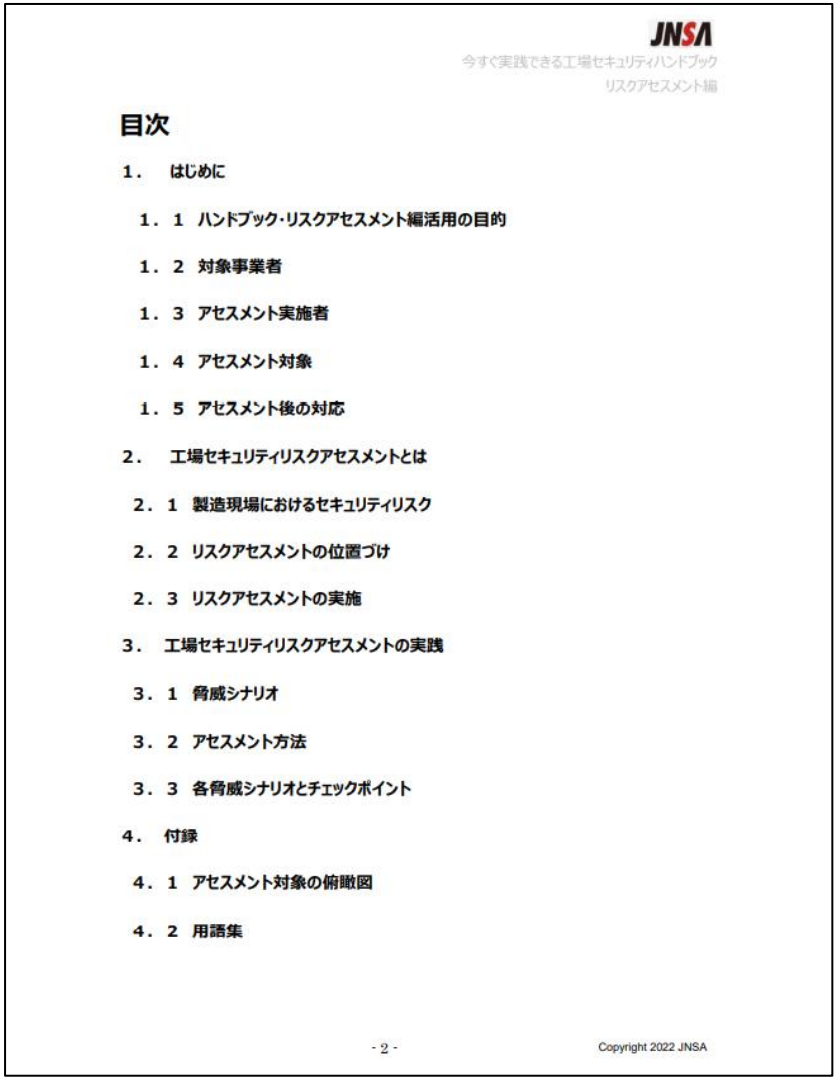
2022 年 5 月

近日公開

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

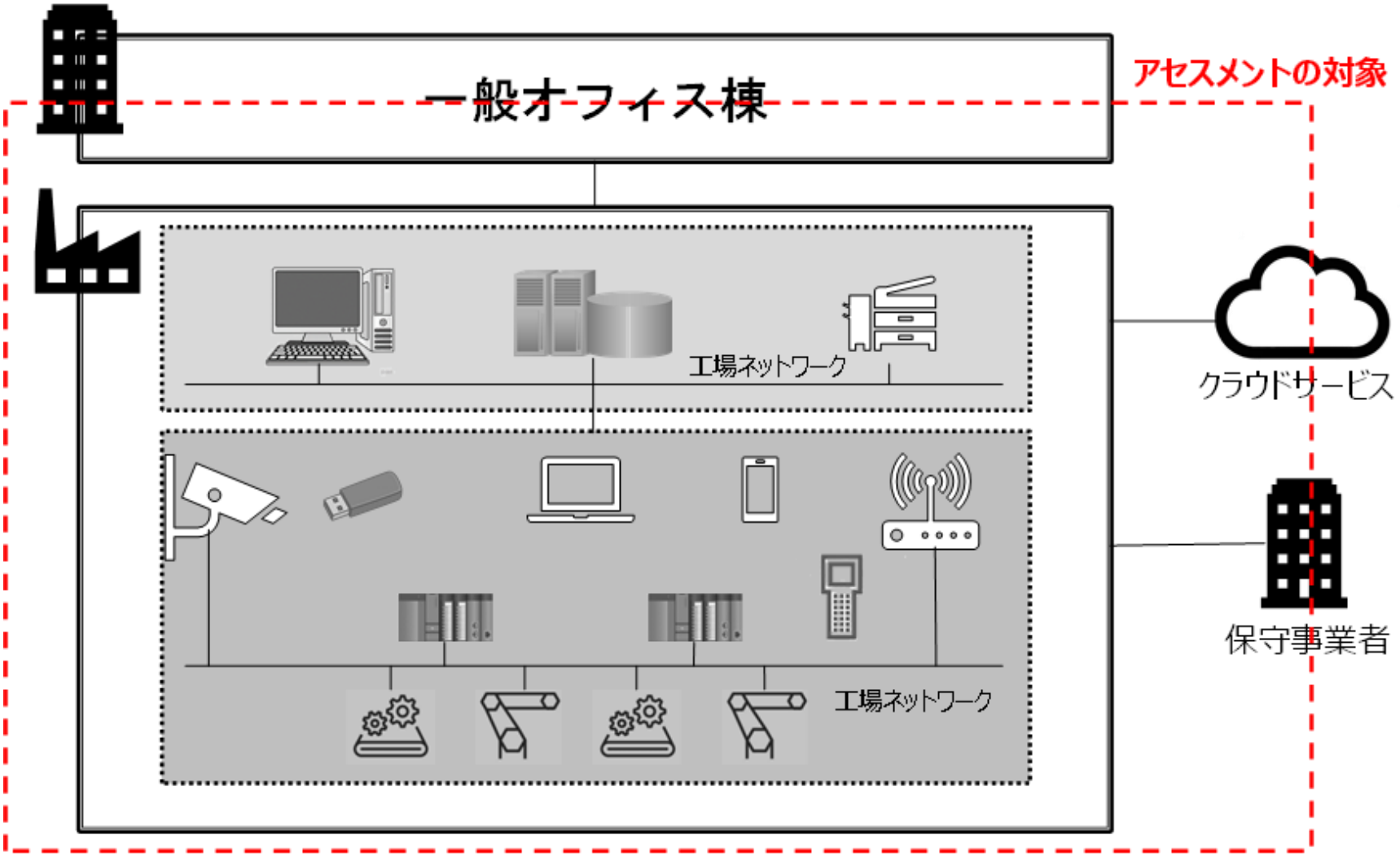
ハンドブック・リスクアセスメント編の概要

- 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。

アセスメントの対象



13の脅威の入口

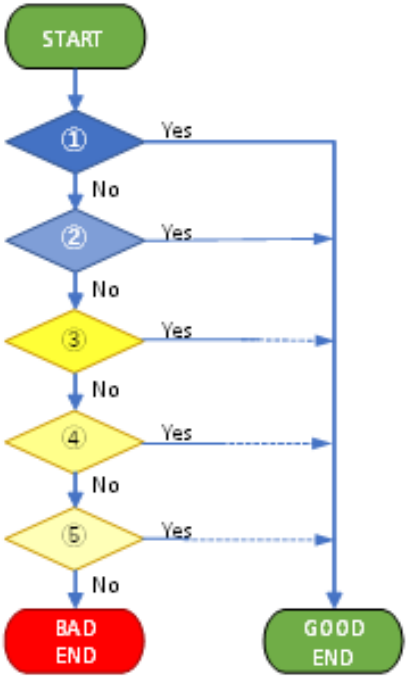
No	脅威の入口	脅威が引き起こす可能性のある事象	懸念されるリスク
1	USBメモリー	USBメモリーから制御システムや製造装置にマルウェアの感染が広がる	工場停止
2	持込パソコン	持込パソコンから制御システムや製造装置にマルウェアの感染が広がる	工場停止
3	スマホ・タブレット	スマホ・タブレットに感染したマルウェアが利用者の意図しない動作をさせる	情報漏洩
4	IoT機器・センサー	IoT機器・センサーが第三者に遠隔操作される	工場停止
5	複合機	複合機が第三者に遠隔操作される	情報漏洩
6	ハンディターミナル	ハンディターミナルに感染したマルウェアがプログラムやデータを改竄する	情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

リスクアセスメント方法

- リスクシナリオに対して現状をシンプルに評価できること
- なぜその対策に効果があるのかが理解できること
- 現状の対リスク耐性のレベルがイメージできること

製造装置の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
③	PC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

今後の予定

ハンドブック３部作

リスクアセスメント編

今回はここ

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
2022.5 初版公開予定

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
2022.9 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
2023.3 初版公開予定


JNSA