



第7回工場SWG

中小製造業のセキュリティ状況と JNSA西日本支部の取り組みのご紹介

JNSA西日本支部
工場セキュリティWGリーダー
岡本 登（富士通株式会社）

2024年2月8日

自己紹介とワーキンググループの概要

●岡本 登

JNSA西日本支部で活動（所属：富士通株式会社）

2000年頃からセキュリティソリューションに従事。2018年から工場セキュリティ対策を研究
現在、お客様のセキュリティアドバイザーとして活動中

●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ワーキンググループ

活動期間：2020年10月～現在

メンバー：西日本を中心に約20名

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

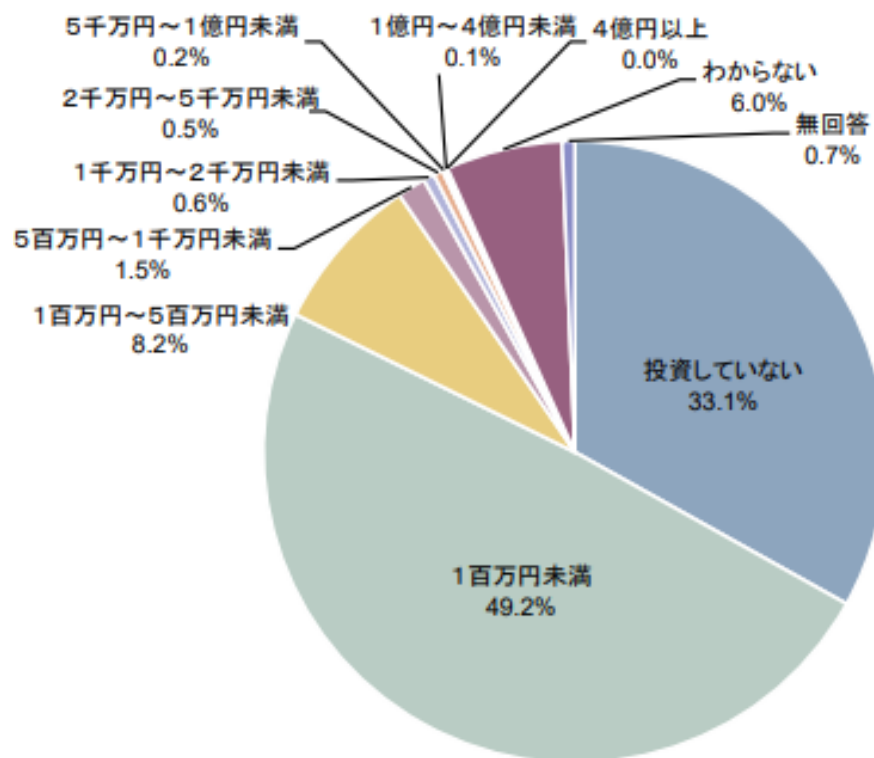
成果物：リスクアセスメント、対策、BCPに関するハンドブック

中小製造業のセキュリティ事情

中小企業の実態①

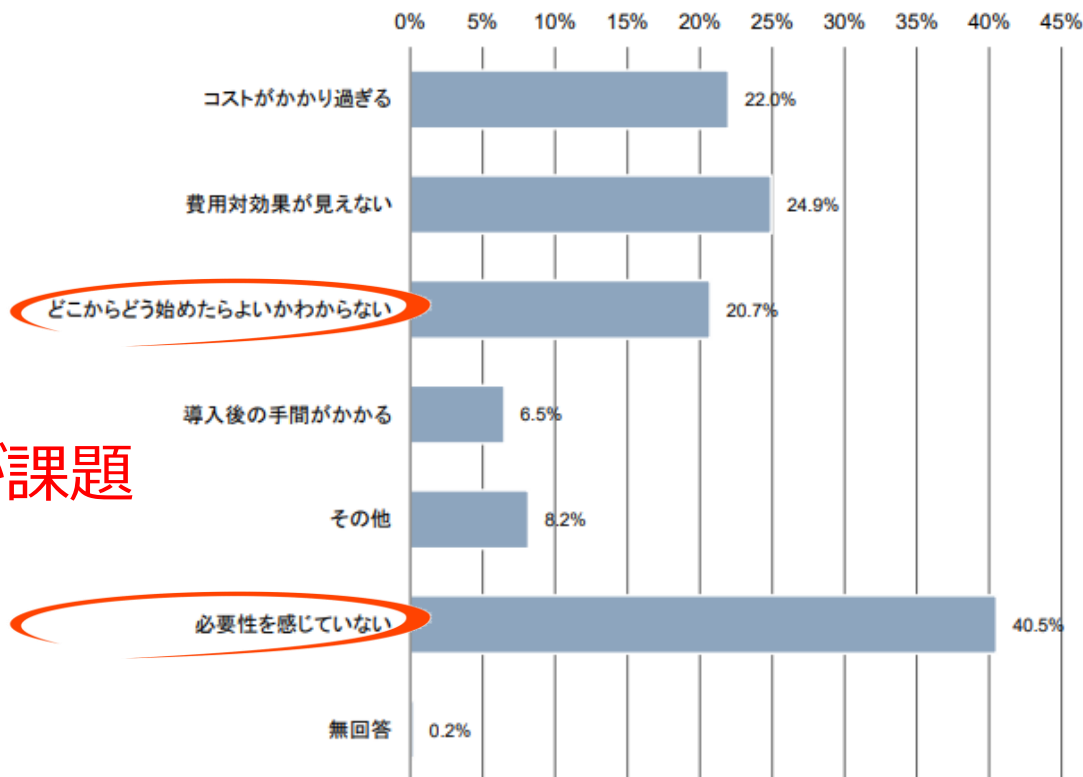
直近過去3期の情報セキュリティ対策投資額

n=3,802



情報セキュリティ対策投資を行わなかった理由

n=1,259



ここが課題

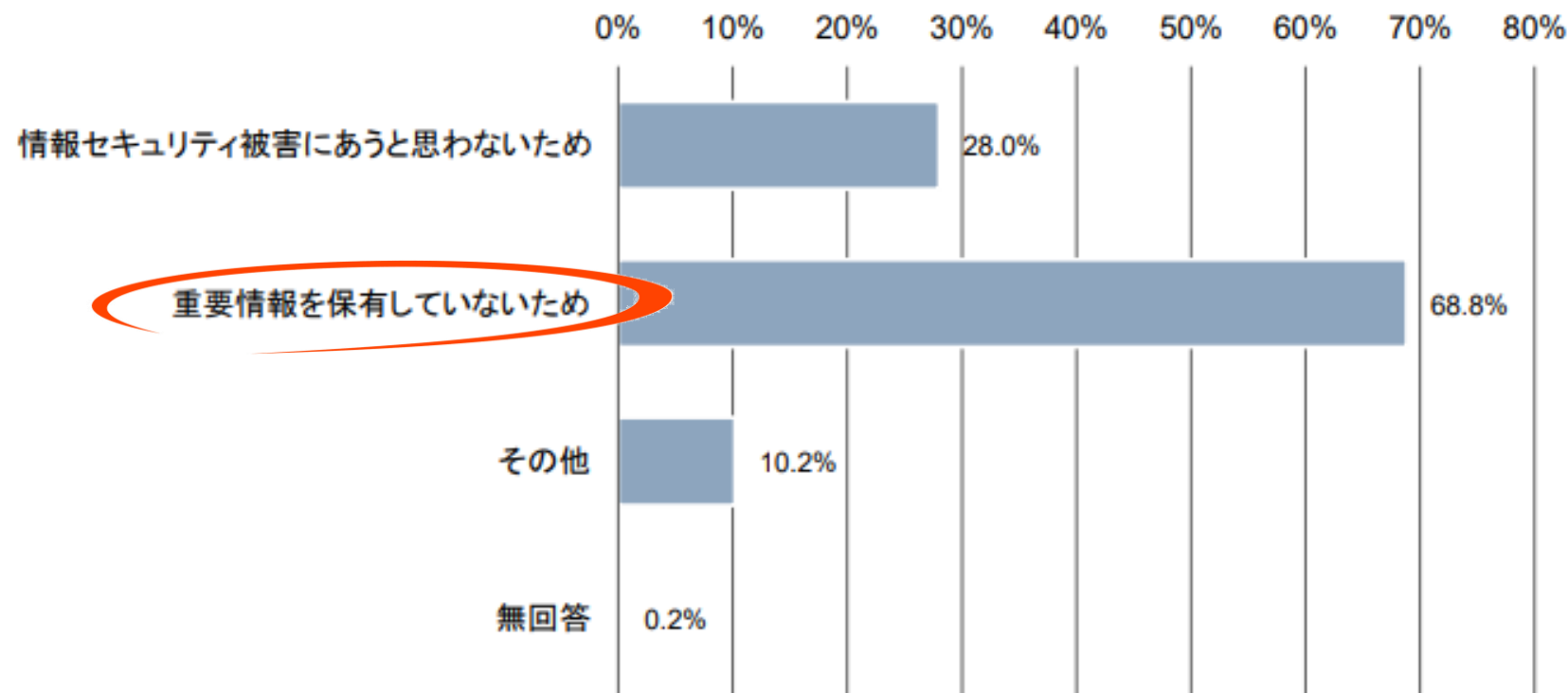
- ・製造現場にはセキュリティの専門家がいるわけではない
- ・迫っている脅威、リスクの大きさに気づいていない

IPA「2021年度中小企業における
情報セキュリティ対策に関する実態調査」より抜粋
有効回答数4,074（製造業11.8%）

中小企業の実態②

情報セキュリティ対策の必要性を感じない理由

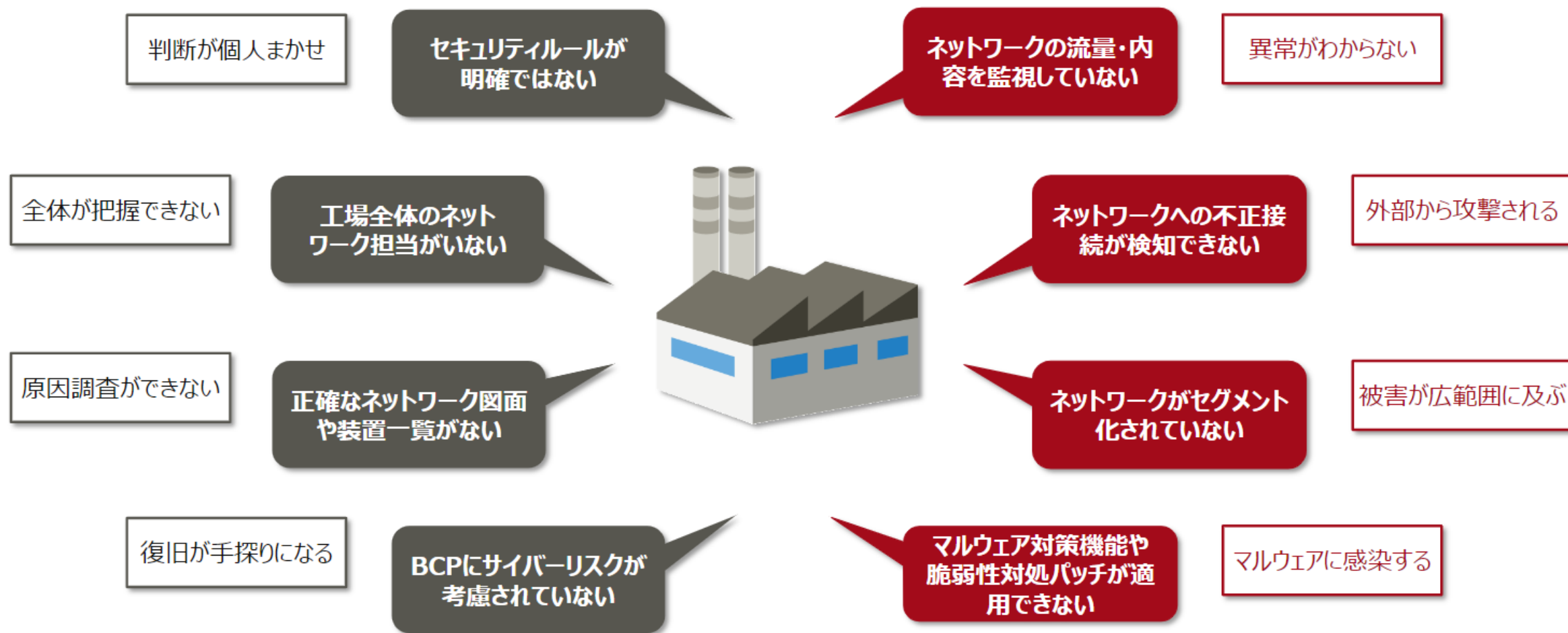
n=1,259



IPA「2021年度中小企業における
情報セキュリティ対策に関する実態調査」より抜粋
有効回答数4,074（製造業11.8%）

**情報セキュリティリスクは機密性（情報漏洩）だけではない
特に製造業は可用性（生産を止めない）が重要。止まっても大丈夫な工場はない！**

多くの中小工場が抱える課題



具体的な事例①

●マルウェアを飼っている工場

2008年に「コンフィッカー」というワームが爆発的に蔓延。しかし、工場内では目立った被害が出ないために、いまだに感染したままの機器が稼働している工場がある。

- 工場では機器の稼働年数が情報系と比べて長い
工場内にもWindowsOSで動作している機器が多数あるが、その認識はない
工場内にはマルウェアを検知する手段がない

●LANカード2枚刺しパソコンでネットワーク分離

生産情報の連携などのために、OTとOAをネットワークでつなぐ必要が出てきたが、ネットワークスイッチ（HUB）やNIC2枚刺しPCでつなぐケースが多く見られる。

- 中小製造業のネットワーク構築は、地場の電気工事事業者などが手掛けることが多い。
セキュリティ知識やノウハウのある人材が社内にはいない。

具体的な事例②

●セキュリティのイメージ

リスクアセスメントハンドブックの作成中に現場のご意見を伺いたく、実際の工場を訪問した際、「セキュリティ」と聞いて思い浮かぶことをお訊ねしたら、「セコムさんとかですかね」という回答だった。

→ 敢えて「情報セキュリティ」とは言わなかったが、やはり、あまり関心がないことが伺われる。

●セキュリティ侵害を受ける可能性

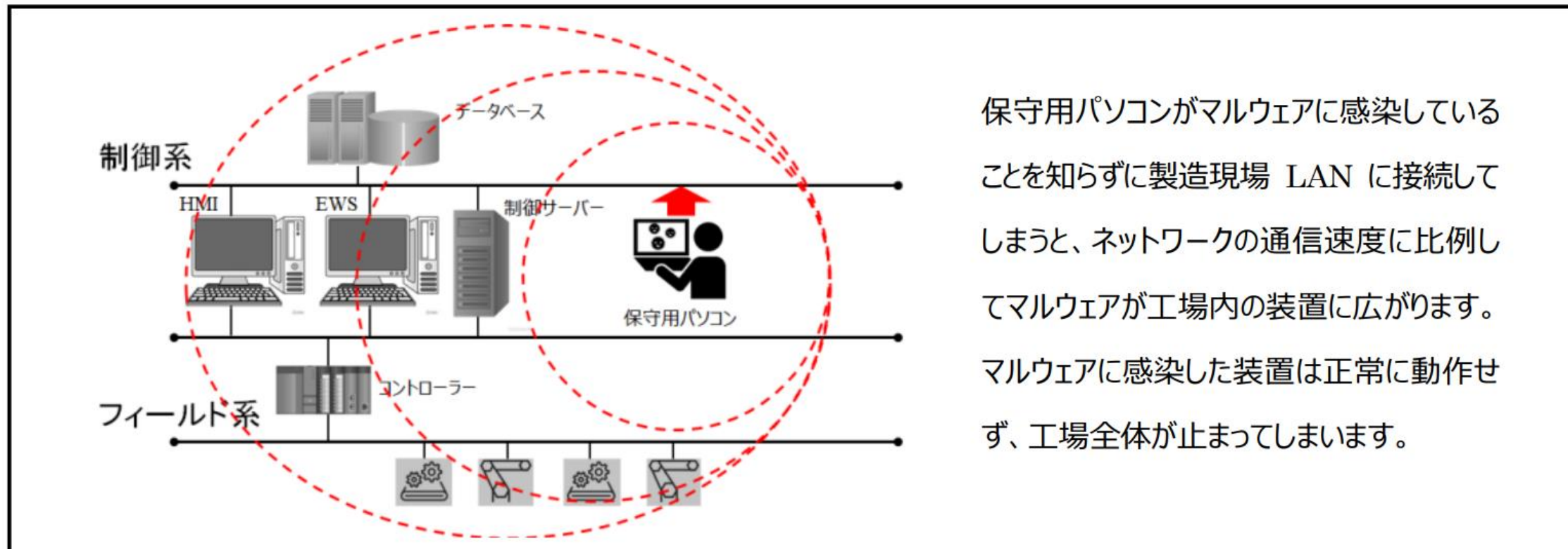
同様に、実際の工場でUSBメモリーを例にアセスメントの方法を説明したところ、「USBメモリーは使っているが、これがリスクになるとは知らなかった」というお話を聞いた。

→ 加えて、工場はインターネットにつながっていないとのことだが、事務所とはつながっていて、事務所はインターネットにアクセスできる環境だった。

ハンドブックを活用した対策の紹介

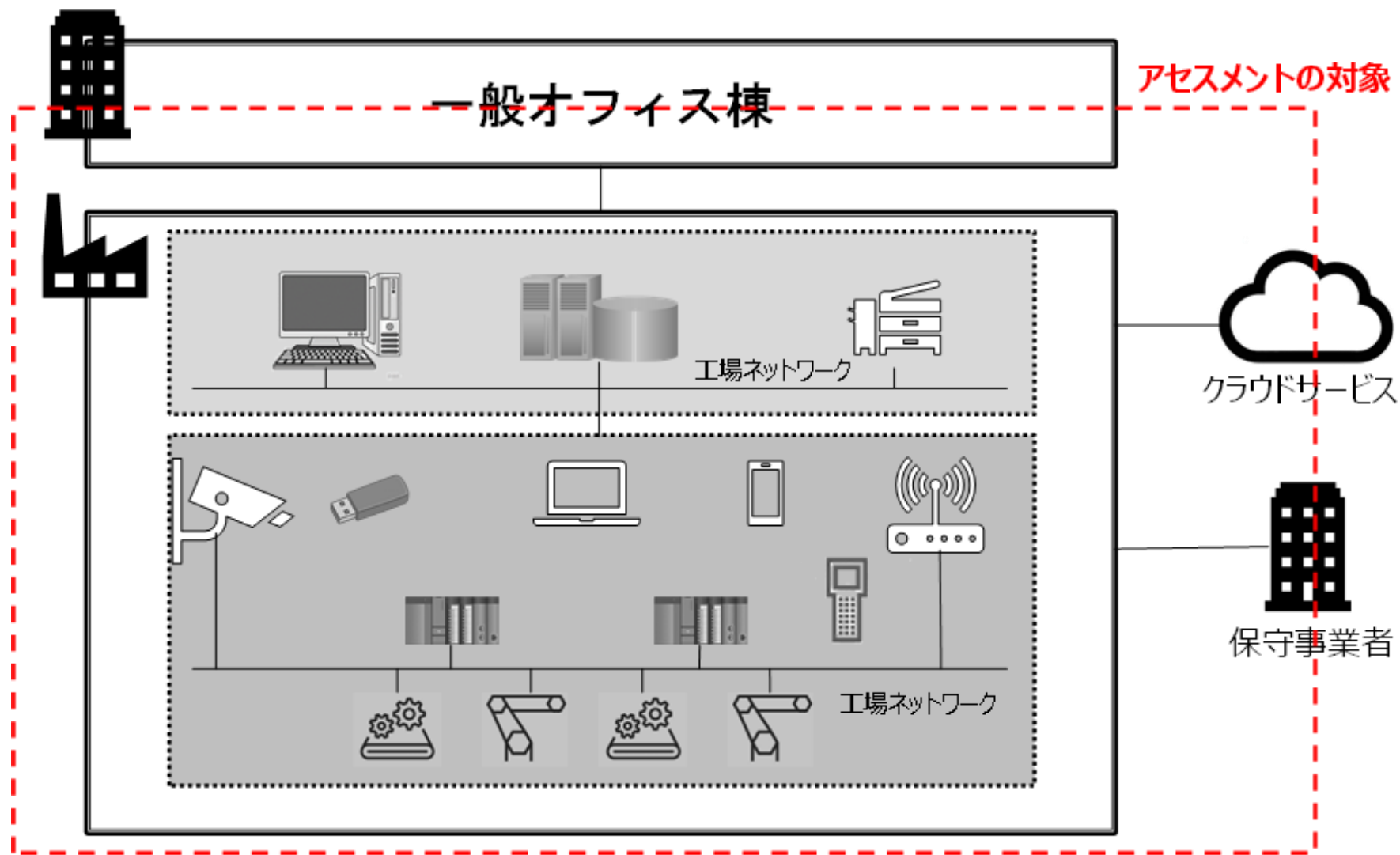
～目指すのは中小企業が自らの手でできること～

1st STEP リスクアセスメント



どこに弱点（脆弱性）があるかが分からなければ、有効な対策を行うことはできません。
どの弱点からどんな脅威が侵入してくる可能性があるのか、その脅威は、工場にどのようなダメージを与えるのかをしっかりと見極めることが重要です。

リスクアセスメントの対象



13の脅威の入口

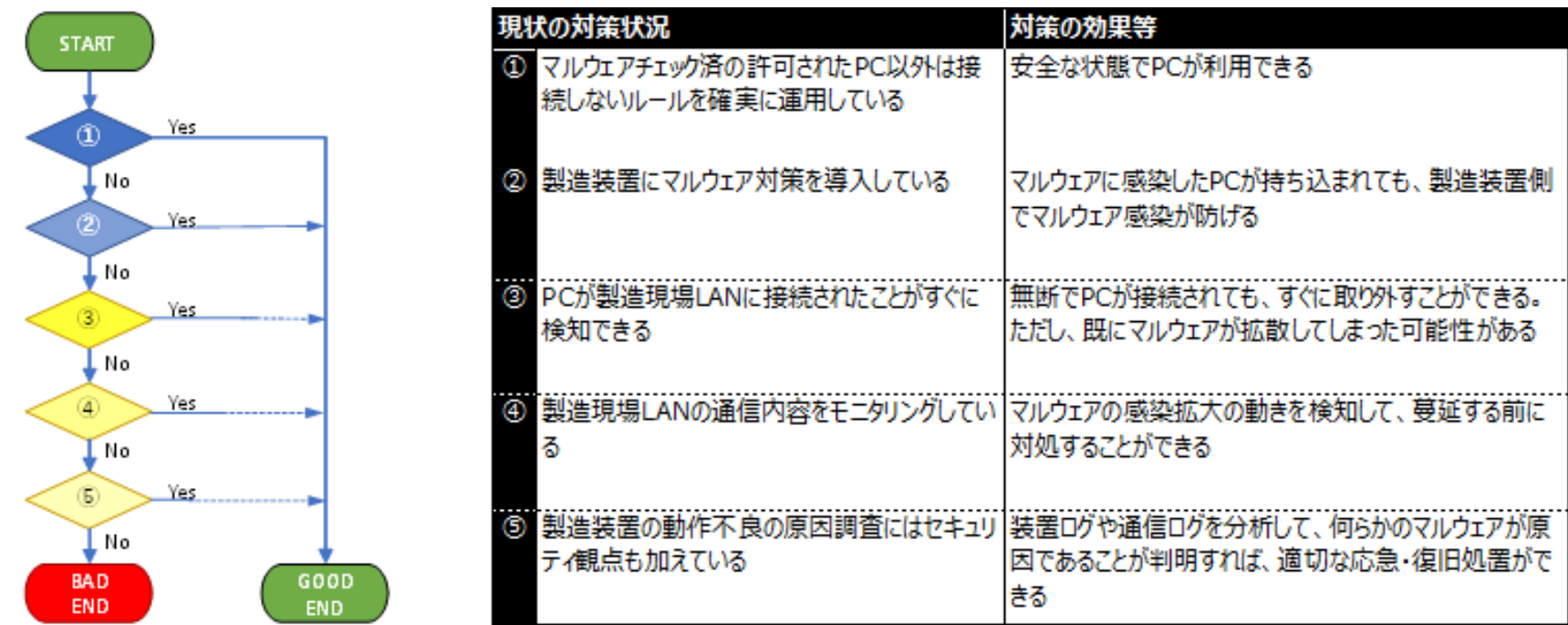
No	脅威の入口	脅威が引き起こす可能性のある事象	懸念されるリスク
1	USBメモリ	USBメモリから制御システムや製造装置にマルウェアの感染が広がる	工場停止
2	持込パソコン	持込パソコンから制御システムや製造装置にマルウェアの感染が広がる	工場停止
3	スマホ・タブレット	スマホ・タブレットに感染したマルウェアが利用者の意図しない動作をさせる	情報漏洩
4	IoT機器・センサー	IoT機器・センサーが第三者に遠隔操作される	工場停止
5	複合機	複合機が第三者に遠隔操作される	情報漏洩
6	ハンディターミナル	ハンディターミナルに感染したマルウェアがプログラムやデータを改竄する	情報改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

ハンドブック・リスクアセスメント編

このハンドブックでは、一般的なリスクアセスメントとは異なるユニークな手法で現場の皆様が簡単に実施できるように書かれています。

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。



アセスメント結果の例

脅威の入口	アセスメント結果	課題
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	古い機種の入替え検討が必要
OAネットワーク	BAD	接続の有無、方法などの詳細な調査が必要
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（VPN接続方法など）
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（チェック体制など）

2nd STEP リスク対策

リスク対策にはいくつかの段階があります

- ①弱点をなくす ➡ セキュリティパッチを適用する、システムをアップデートする
- ②弱点を攻められないように守る ➡ ファイアウォールなどを導入する
- ③攻められたらすぐに見つけて抑える ➡ ウイルスチェックを行う
- ④やられたらすぐに元に戻す ➡ バックアップを作る

対策方法には3つの種類があります

物理的対策

不法侵入や破壊、紛失、盗難などに対応
例) 監視カメラ

技術的対策

システムやデータ、ネットワークなどのリスクに対応
例) ウイルス対策

人的（組織的）対策

従業員のミスや不正など人によるリスクに対応
例) ルール、教育

残念ながら万能な対策はない！

アセスメントの結果や環境に合わせて対策を選ぶことが重要

多層的防衛の視点で整理

高度な共通対策（E-01～03）

各脅威ごとの対策（01-01～13-02）

USBメモリー
(01-01～03)

持込パソコン
(02-01～04)

スマホ・タブレット
(03-01～02)

IoT機器・センサー
(04-01～03)

複合機
(05-01～05)

ハンディターミナル
(06-01～05)

OAネットワーク
(07-01～04)

インターネット
(08-01～04)

Wi-Fi（無線AP）
(09-01～02)

保守用ネットワーク
(10-01～02)

クラウドサービス
(11-01)

部品・原材料
(12-01～03)

新規購入機器
(13-01～02)

基礎的な共通対策（C-01～05）

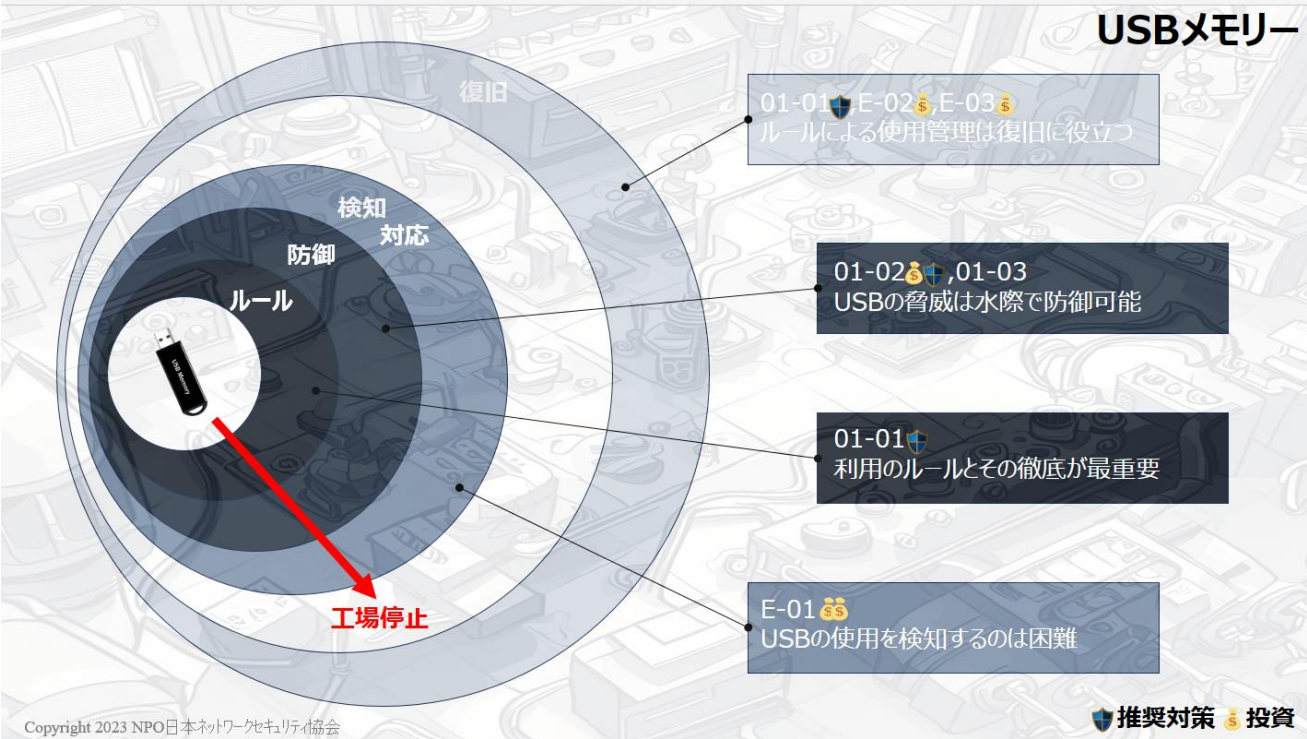
代表的なフレームワークも参考に



→ すり抜けた攻撃を見逃さない

→ 被害範囲を特定して対処

ハンドブック・リスク対策編（近日公開）



対策No.01-02	関連する脅威の入口：USBメモリー
具体的な内容：ウイルスチェック機能付きUSBメモリーの導入	
●対策内容	
対策No.01-01	関連する脅威の入口：USBメモリー
具体的な内容：USBメモリー使用ルールの策定と管理の徹底	
●対策内容	
工場内で使用を許可するUSBメモリーとその取り扱い方法をルールとして明文化し周知徹底する。	
記載内容の具体例	
-使用を許可するUSBメモリーの指定（社給USBメモリーのみなど）	
-使用目的、使用対象機器	
-管理方法（USB台帳管理）	
-管理責任者、識別番号、保管場所、ウイルスチェックデータ更新日※1	
-使用記録（USB作業記録）	
-作業日、作業者、使用USB識別番号、使用機器、ウイルスチェック※2、不要ファイル削除	
●運用のポイント	
USBメモリーの識別番号表示（シール等）は目立つものにして管理外のものが入り込まないように注意すること。	
対策の種類： ☒ 被害に遭わないための対策 ☐ 被害を早期発見するための対策 ☒ 被害から早期復旧するための対策	
対策の分類： ☐ 物理的対策 ☒ 人的対策 ☐ 技術的対策	
備考：※1 対策No.01-02を行う場合 ※2 対策No.01-03を行う場合	

対策カード

リスク対策集として、13の入口ごとに複数の対策カードが用意されています。
対策カードには対策段階や対策の種類以外にも必要な費用情報などが記載されています。

3rd STEP BCP策定

2023年12月1日に大阪で「NSF in KANSAI 2023」を開催
工場内でのセキュリティ事故を想定したワークショップを実施



どのような行動をとればいいのか、事前に決めておくことが重要であると実感

ハンドブック 3 部作



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 (<https://www.jnsa.org/result/west/2022/index.html>)

リスク対策編

◀ 近日公開予定

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.秋 初版公開予定

サイバーBCP策定編

3rd STEP

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

2024.夏 初版公開予定



JNSA