日本のサイバーセキュリティを「連携」「学び」「創造」

中小製造業における現実的な情報セキュリティ対策
～目に見える・手が届く運用とは～

2025年08月27日

特定非営利活動法人日本ネットワークセキュリティ協会[略称：JNSA]　西日本支部

支部長 米澤 美奈 (株式会社 ソリトンシステムズ：所属)

アジェンダ

1. はじめに

(1) 自己紹介
(2) 今、1番、言いたいこと

2. 中小製造業の現状

(1) 自分たちが「日本の要」って思ってない
(2) でも、やらないとあかんやろ？
(3) 多くの中小工場が抱える課題

3. 自分でできること、助けを求めること

(1) まず、できる事ってなんだろう
(2) 専門家と呼ばれる人たち
(3) 意外と、すっと入ってくる気もする

4. まとめ

1. はじめに

(1) 西日本支部紹介

●JNSA西日本支部

- 支部メンバー：約50名
- 現ワーキング：約30名　「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」

※ コロナの影響で、WebMeeting形式が普及。関西エリアにとどまらず、東京・山口等
遠隔地からの参加者も集まっている。
※ 現ワーキングメンバーが、月1回(オンサイト/オンラインのハイブリッド実施)
※ 参加者、絶賛募集中
そろそろ、次のテーマを考えてるところ・・・

2014年04月01日
出社してから退社するまで中小企業の情報セキュリティ対策実践手引き
（出社してから退社するまでのリスク対策WG）

2016年03月29日
情報セキュリティポリシーサンプル改版（1.0版）
（中小企業向け情報セキュリティポリシーサンプル作成WG）

2020年11月20日
中小企業において目指すSecurity By Design
（中小企業のためのSecurity by Design WG）

2022年05月31日
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
（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）

2024年3月22日
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
（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）

2025年5月13日
今すぐ実践できる工場セキュリティハンドブック・IT-BCP編
（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）

活動方針に即した、
「西日本のネットワーク社会における
セキュリティレベルの維持・向上」のため。
中小企業が多い「関西」ならではの成果物。

<報告書・成果物>
https://www.jnsa.org/result/west/

(2)今、1番、言いたいこと

中小製造業のセキュリティ

このままでは、あかんやろ！

製造現場を見学させてもらった

●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、「警備会社さんとかですか？」という回答だった。

→ 敢えて「情報セキュリティ」とは言わないで聞いたが、やはり、関心がないことが伺われる。

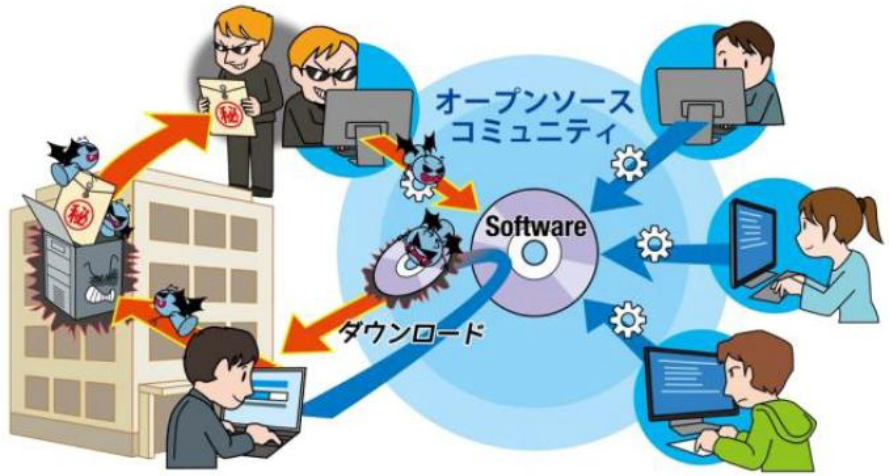
●セキュリティ侵害を受ける可能性

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メモリって 危ないんですか？」との反応。

→ 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。

日本中、ゴリゴリ やられてんのに・・・

2位 サプライチェーンや委託先を狙った攻撃



商品やサービスの企画、開発から、調達、製造、在庫管理、物流、販売までの一連のプロセス、および この商流に関わる組織群をサプライチェーンと呼ぶ。「繋がり」を悪用した攻撃は、自組織の対策のみで防ぐのが難しいため、取引先や委託先も含めたセキュリティ対策が必要な脅威といえる。

攻撃者は、直接攻撃が難しい強固なセキュリティ対策を持つ標的組織に対して、まずサプライチェーンの脆弱な部分を攻撃する。 その後、その脆弱な部分を経由して、間接的および段階的に標的組織を狙う。

IPA
情報セキュリティ10大脅威 2025 より抜粋

国内製造業の**９８．９%**を占める中小企業（資本金３億円以下）が日本のものづくりを支えている

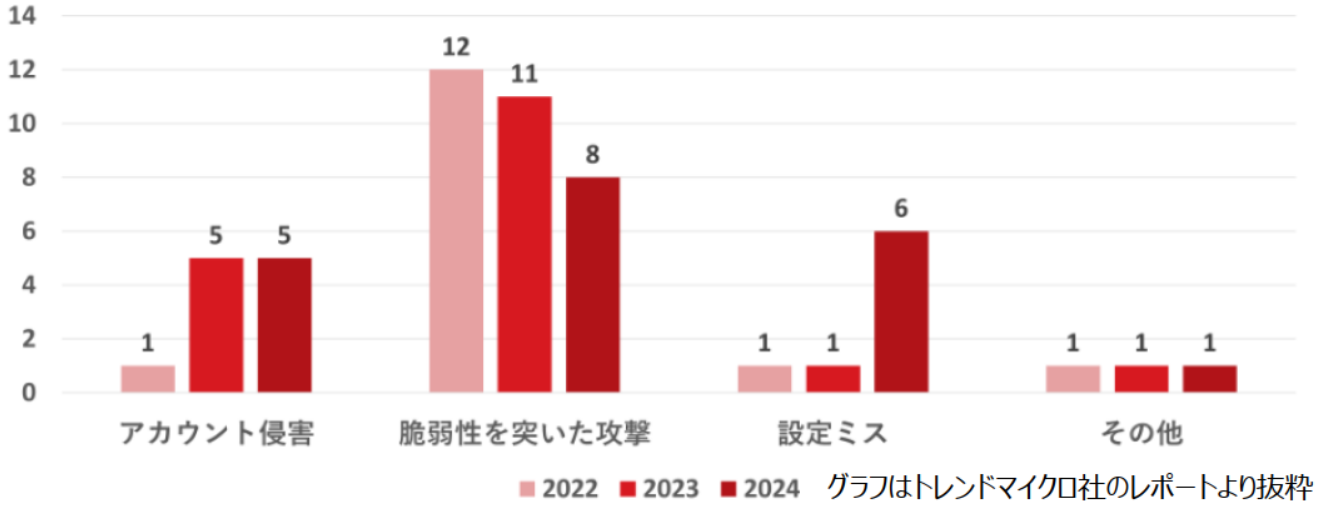
中小製造業が止まれば経済は止まる

ランサムウエアによる工場操業停止事例

公開資料では、事例は非公開でお願いします。

具体的なインシデントから学ぶ教訓

国内組織におけるランサムウェア被害の主な発生原因とその公表件数の推移



グラフはトレンドマイクロ社のレポートより抜粋

・設定ミス5/6はVPN機器設定
・脆弱性5/8はVPN機器

安全にリモートアクセスするための仕組みが、一番安全ではないという現状

適切にアップデート対応していれば**防げる問題**であることを認識すべき

サプライチェーン
= 社会全体の支え合い

崩れていかない仕組みを
考えないと！

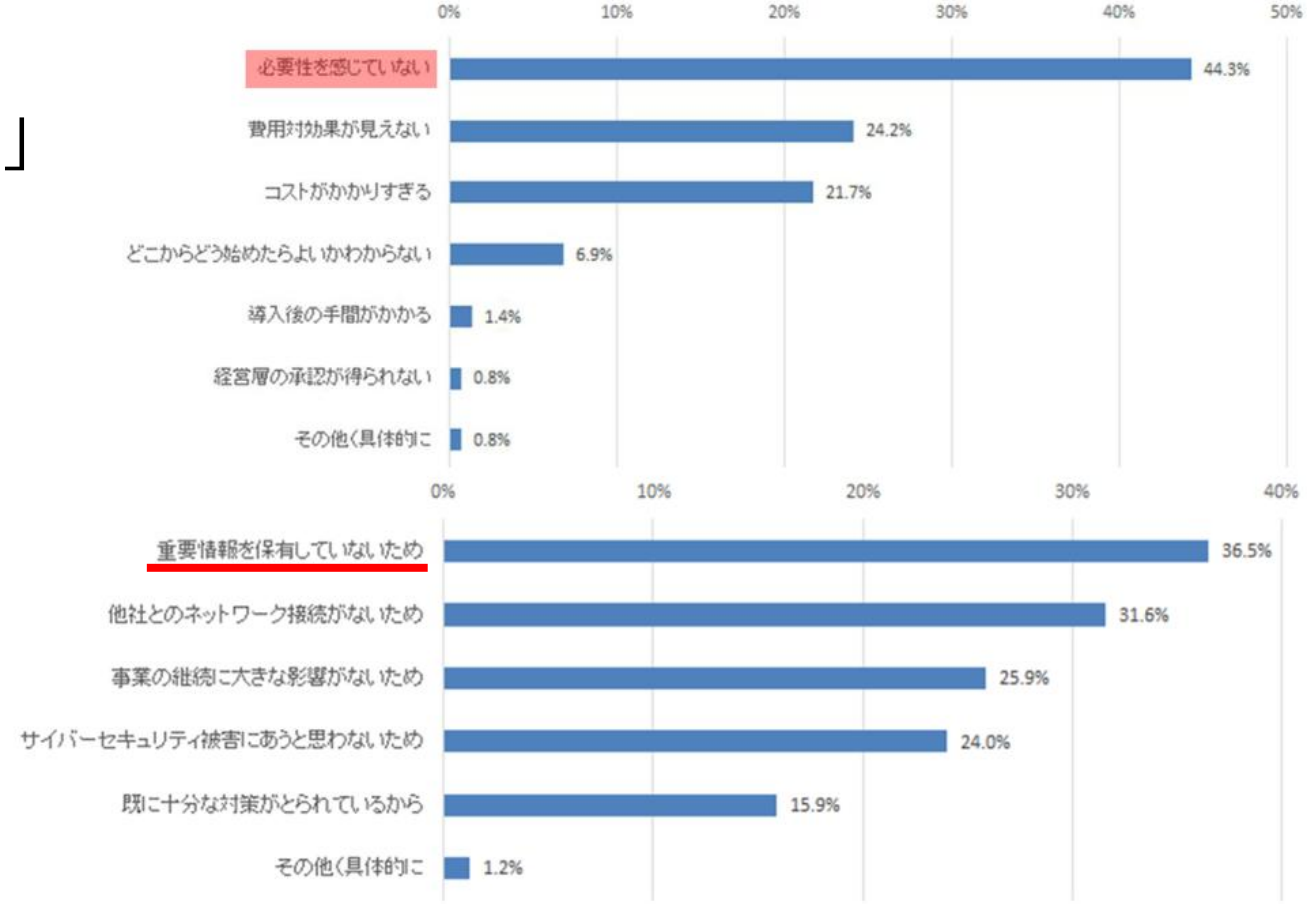
2. 中小製造業の現状

(1)自分たちが「日本の要」って思ってない

製造現場を見学させてもらった際のコメント

●**セキュリティインシデントへのイメージ**
「うちは、そんなすごい情報、もってませんから」

→ うちなんて 狙う人 いるんですか？
→ サイバー攻撃なんて、
　映画かドラマの中の出来事

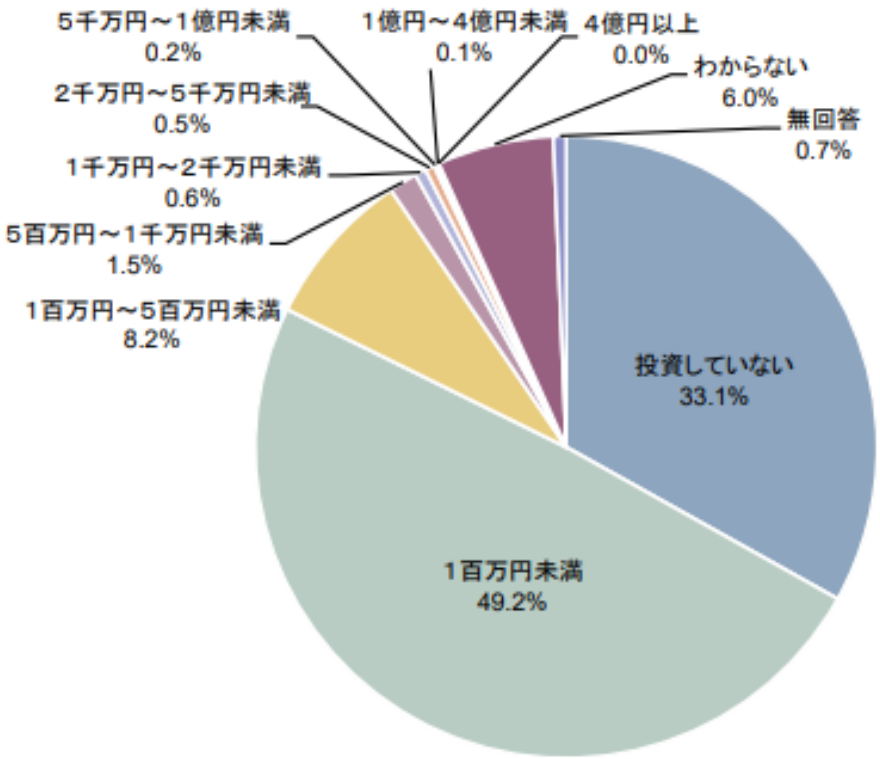


IPA「2024年度中小企業における
情報セキュリティ対策に関する実態調査」より抜粋

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

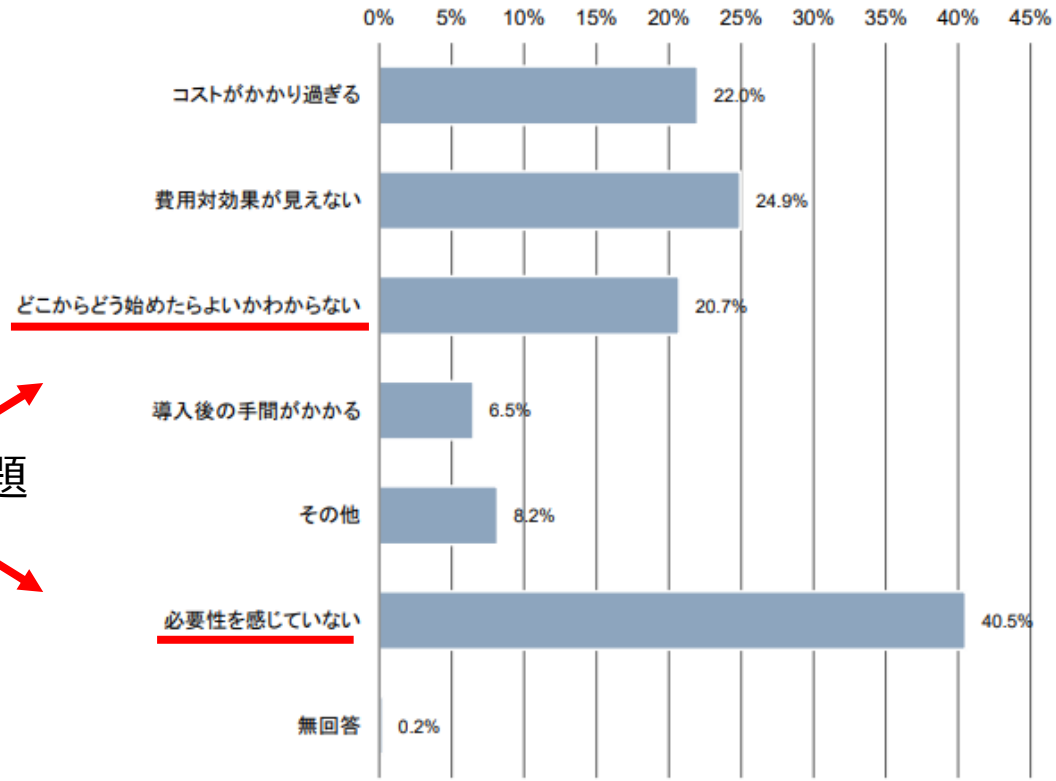
n=3,802



ここが課題

情報セキュリティ対策投資を行わなかった理由

n=1,259

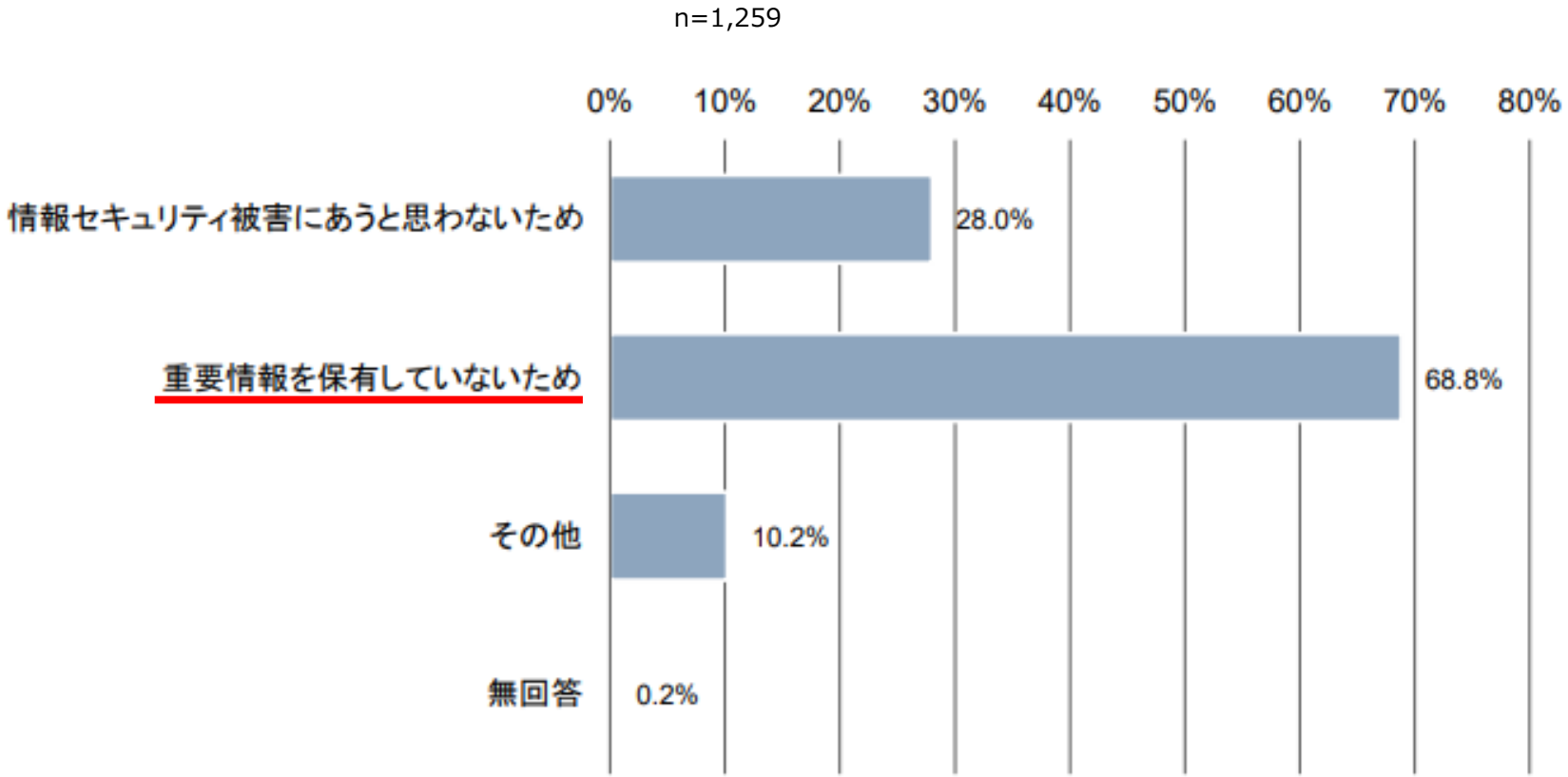


・製造現場にはセキュリティの専門家がいるわけではない。
・多くの工場はセキュリティ事故に遭遇していないか気が付いていない。

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



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！

(2) でも、やらないとあかんやろ？

● 事業継続計画（BCP）の策定状況

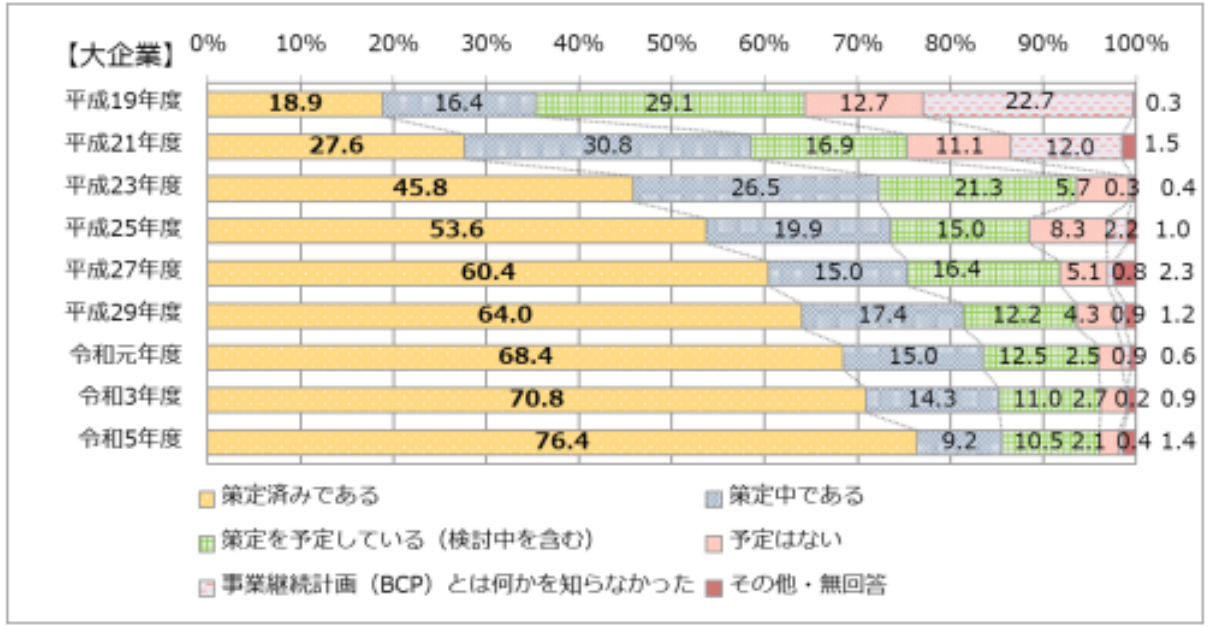
事業継続計画（BCP）の策定状況については、大企業では 76.4%が「策定済み」と回答している（令和 3 年度比 5.6 ポイント増）。
これに「策定中」（9.2%）を加えると、85.6%と 8 割を超え ている。
中堅企業では、45.5%が「策定済み」と回答している（同 5.3 ポイント増）。
これに「策定中」（12.1%）を加えると半数以上（57.6%）となっている。
以上のことから、大企業を中心に、BCP の策定は進んできている状況と言える。

「何か起きて、生産が止まってもいい」と思ってるわけではない。

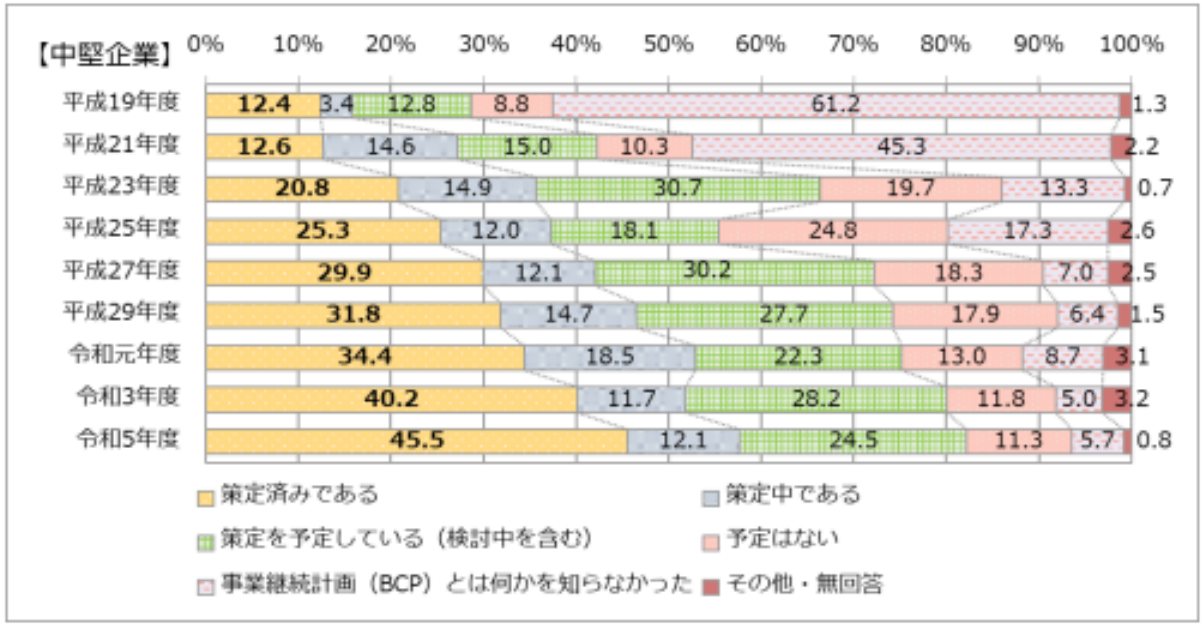
「止まるかも」の原因の中に
「セキュリティ侵害」という可能性が 視点として入っていないだけ。

「止まる原因」が、何であろうと止めてはいけない という意識はある。

【大企業】



【中堅企業】



出典：「令和5年度 企業の事業継続及び防災の取組に関する実態調査」内閣府(令和6年3月)

(3) 多くの中小工場が抱える課題

判断が個人まかせ

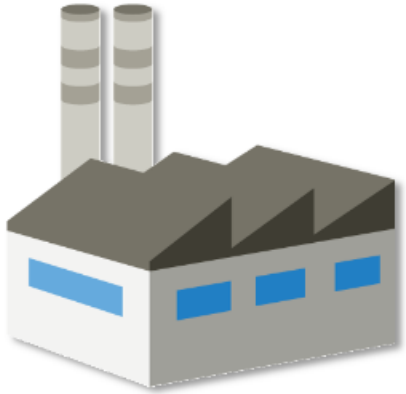
セキュリティルールが明確ではない

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

3.自分でできること、助けを求めること

(1) まず、自分でできる事ってなんだろう

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

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
2024.3 初版公開（ https://www.jnsa.org/result/west/2023/index.html ）

サイバーBCP策定編

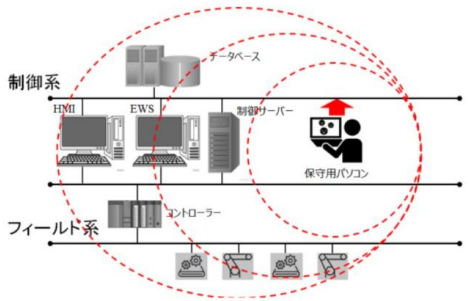
従来の災害対応BCPにセキュリティ観点を加えるための参考書
2025.5 初版公開(https://www.jnsa.org/result/west/smb/index.html)

コンセプト

- 中小企業の製造業を中心に工場セキュリティ対策を進めるための参考書
- 情報セキュリティに詳しくなくても、自社工場において、何をすべきか わかるもの
- 「何をすべき」という答えを載せた教科書 ではなく参考にしつつ、
  検討のベースになるハンドブック

リスクアセスメント編

1st STEP リスクアセスメント



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。

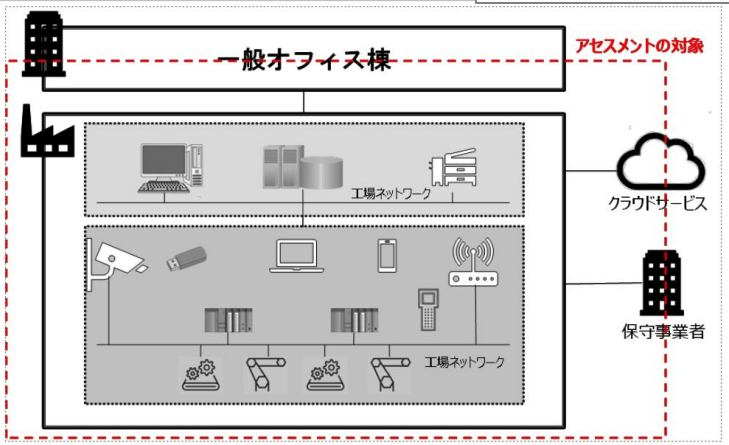
どこに弱点（脆弱性）があるかが分からなければ、有効な対策を行うことはできません
どの弱点からどんな脅威が侵入してくる可能性があるのか、その脅威は、工場にどのようなダメージを与えるのかをしっかり見極めることが重要です。

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の対象



リ ス ク 対 策 編

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 ➡ ファイヤ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
従業者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

水平方向の対策

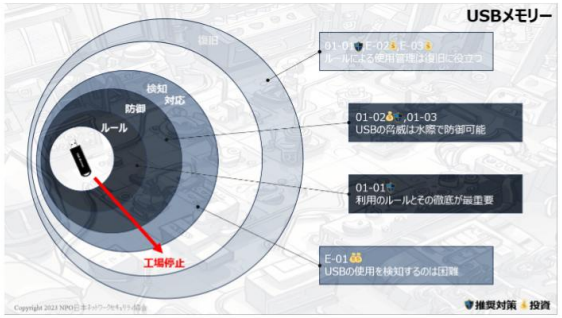
特定 → 防御 → 検知 → 対応 → 復旧

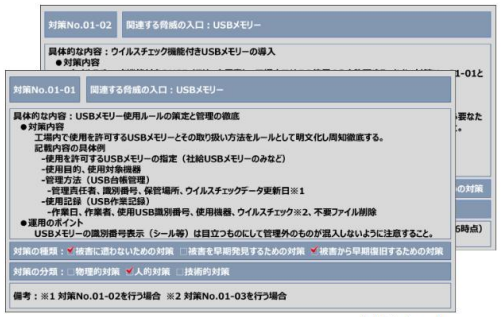
特定	防御	検知	対応	復旧
リスクを特定する	攻撃を防ぐ	異常を検知する	異常に対応する	被害を復旧する
13の脅威の入口の状況を把握し対策すべきリスクを特定する	被害に遭わないための対策を実施する	異常を早期に発見し被害が広がらない対応のための対策を実施する		被害から早期復旧するための対策を実施する

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





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。

垂直方向の対策

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）

サイバーBCP策定編

修正点
・リスク種別のタイトル修正（元：テロ、停電）
・システム障害のITシステム対策に冗長化追加

3. サイバー対応IT-BCPとこれまでのBCPの関係

これまで具体的なITシステムのBCPに取り組んでいなかった企業にとって、ITインフラのサービス継続だけでなく、サイバーセキュリティインシデントへの備えが重要な課題となっています。そのため、サイバーセキュリティインシデントに特化した対策や復旧計画を策定し、運用するためのガイドラインを「サイバー対応IT-BCP（以降、サイバーBCP）」として示します。

		リスク種別					
		自然災害	無差別攻撃や破壊攻撃	システム障害	サイバー攻撃	人的リスク	法的リスク
保護資産	ITシステム	データバックアップ、災害復旧計画	物理的セキュリティ強化	冗長化、UPS（無停電電源装置）、バックアップ電源	サイバーセキュリティ対策、データ暗号化	従業員教育、アクセス管理	法的コンプライアンス、契約管理
	データ・情報	データバックアップ、クラウドストレージ	データ保護、アクセス制限	データバックアップ	サイバーセキュリティ対策、データ暗号化	データ管理教育	データ保護法遵守、契約管理
	建物・設備	耐震補強、避難計画	セキュリティ強化、監視システム	非常用発電機	–	安全管理、避難訓練	保険、法的遵守
	人材	安全確保、避難訓練	安全確保、避難訓練	–	セキュリティ意識向上	健康管理、労働環境改善	労働法遵守、ハラスメント対策
	サプライチェーン	代替供給ルートの確保	供給元のセキュリティ強化	代替供給ルートの確保	サプライチェーンのセキュリティ強化	供給元のリスク評価	契約管理、法的

IT-BCP

サイバーBCP

土台となるBCP

企業の事業活動の継続計画(BCP)

中核事業の定義 | 避難計画、主要顧客、供給品目 | 投資計画対応手順

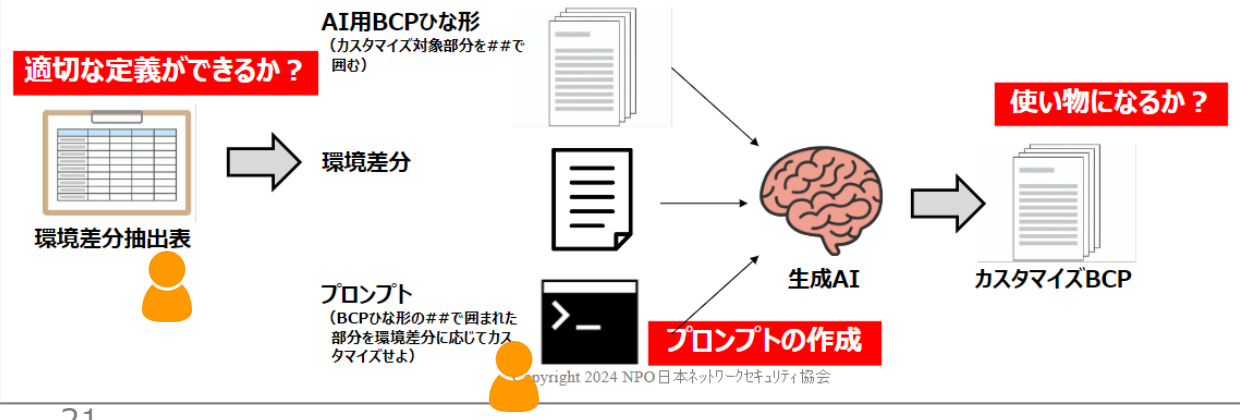
生成AIの活用（実験）

JNSA

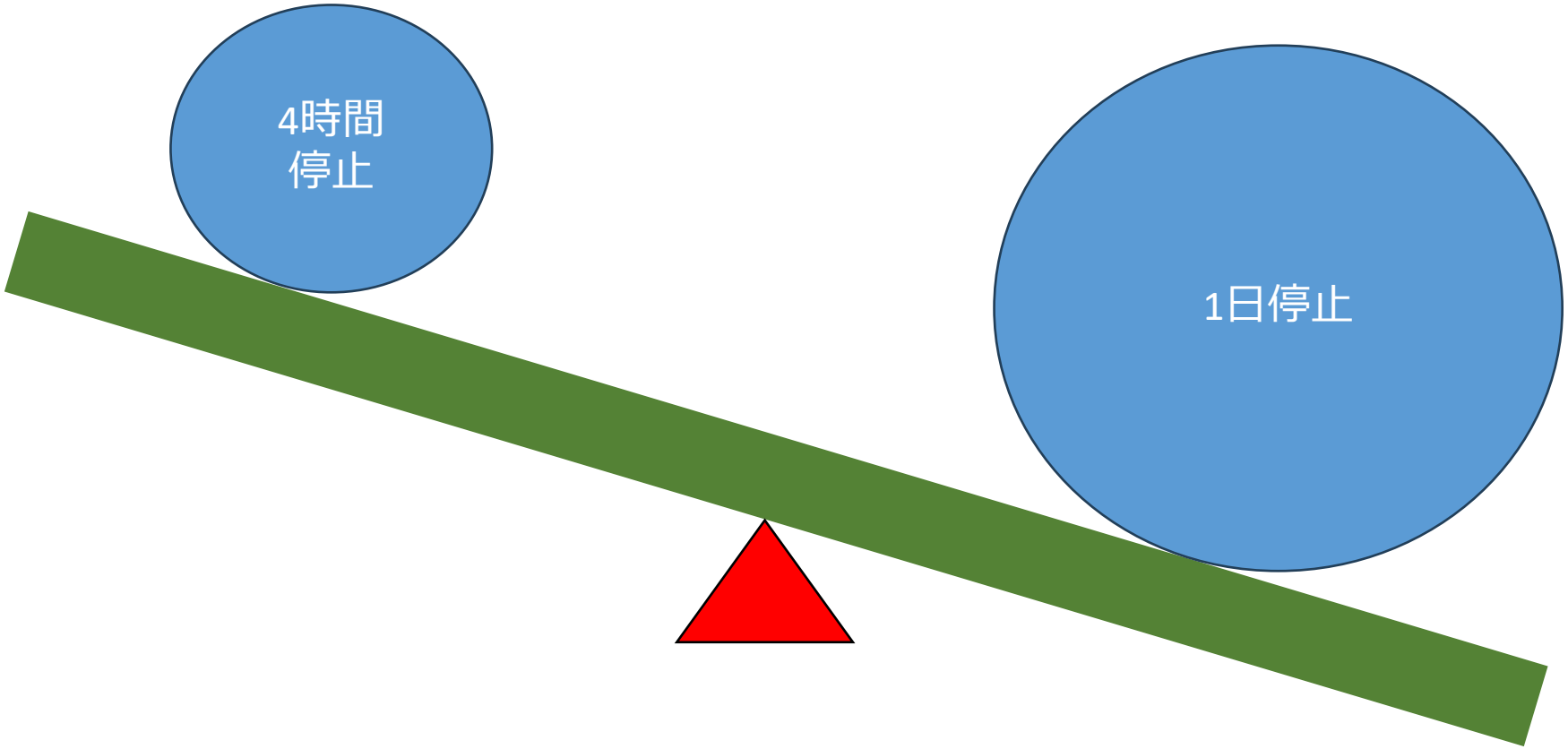
取り組みハードルを下げる ⇔ 対策効果が期待できる

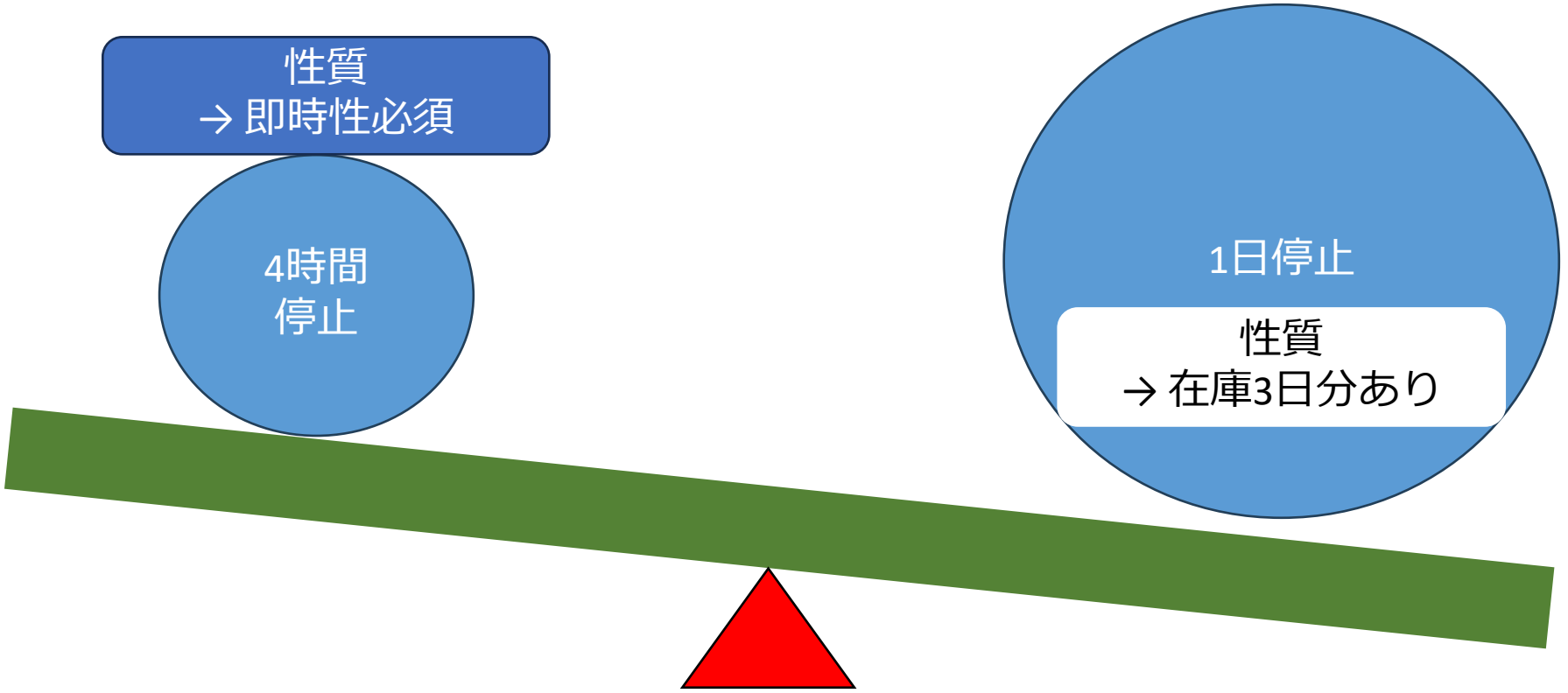
●中小事業者ごとに生産現場の環境は異なるためBCPはカスタマイズが必要

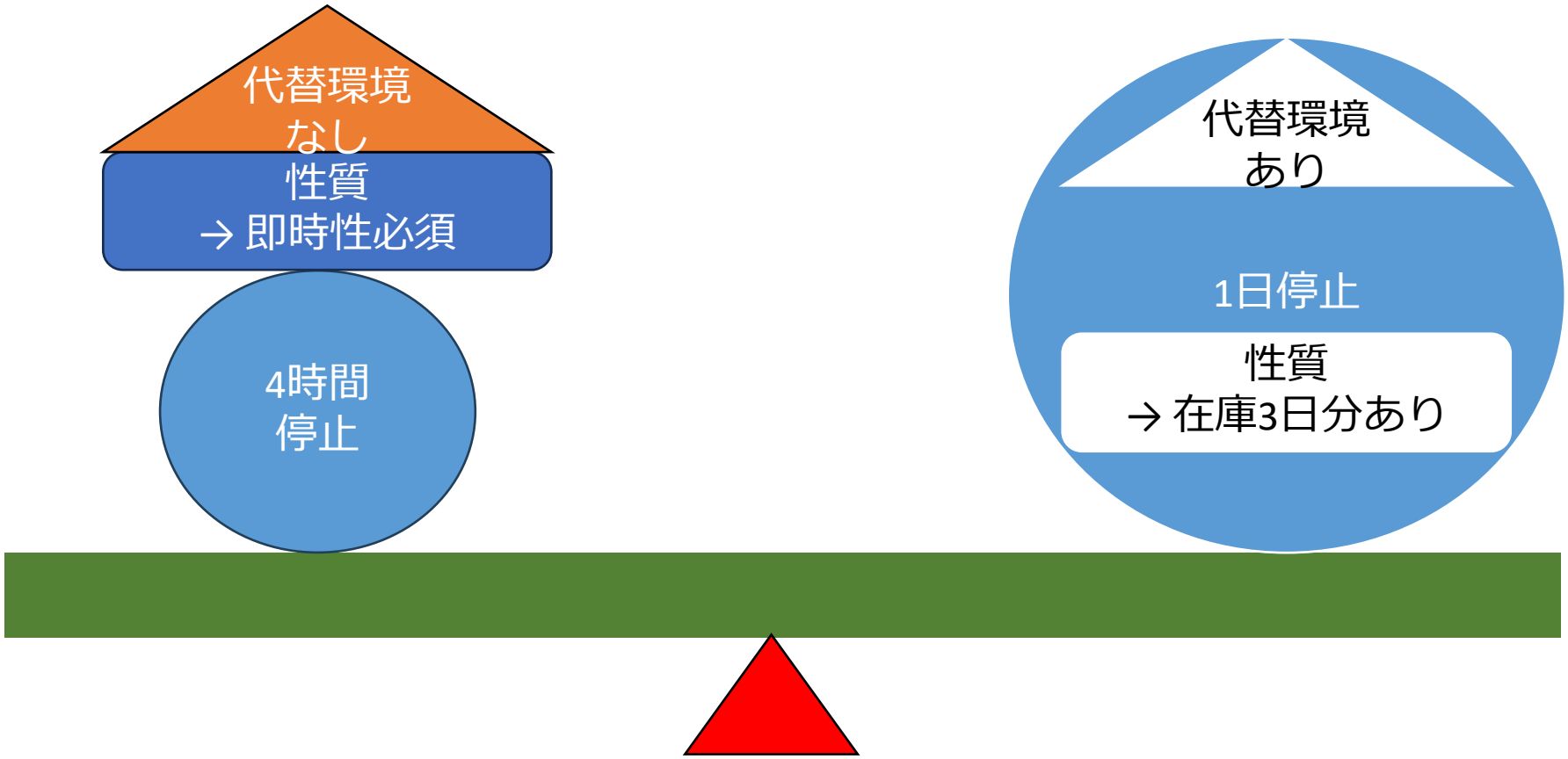
事業者自らがカスタマイズできるか？

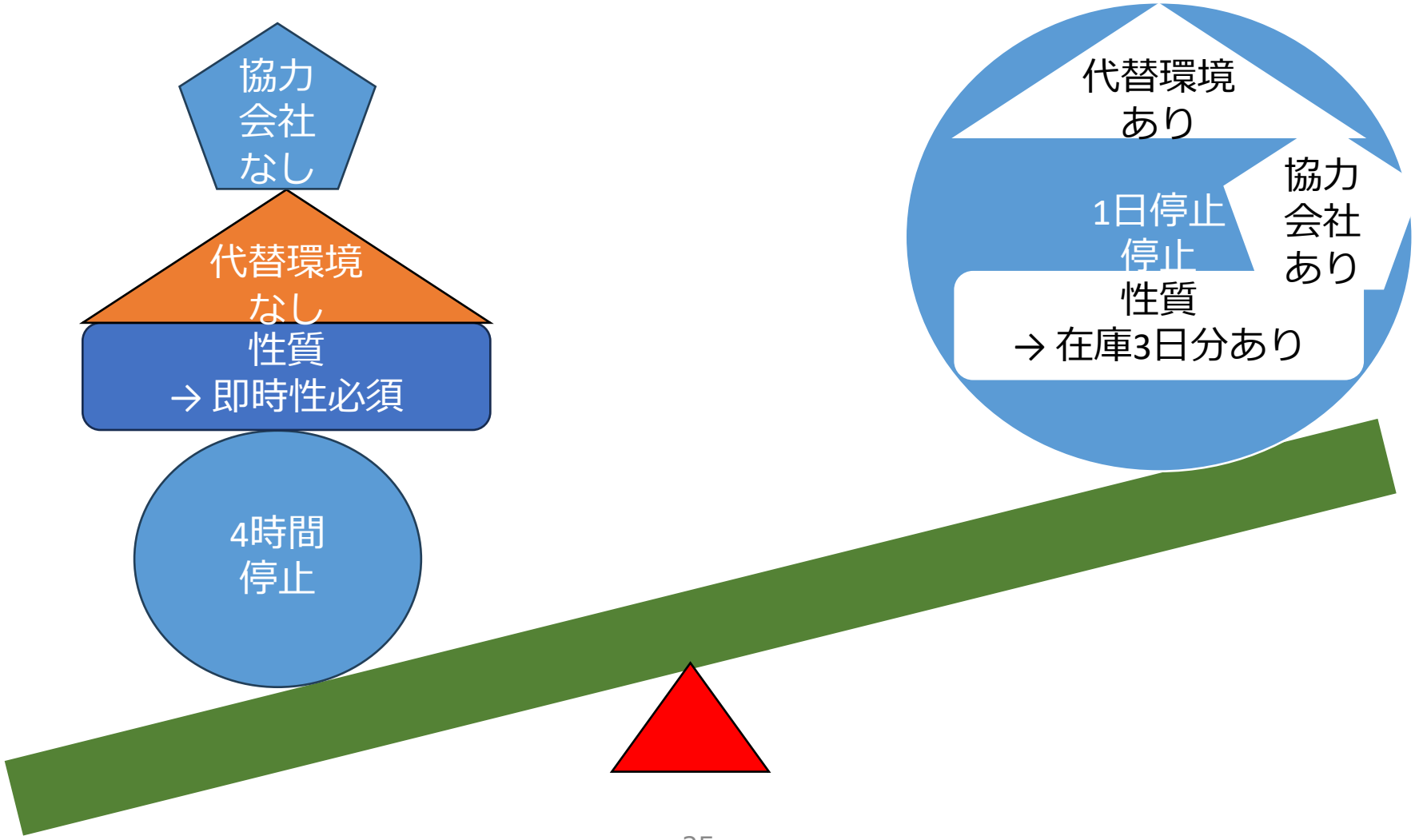


サービス停止時間の意味を考えてみよう



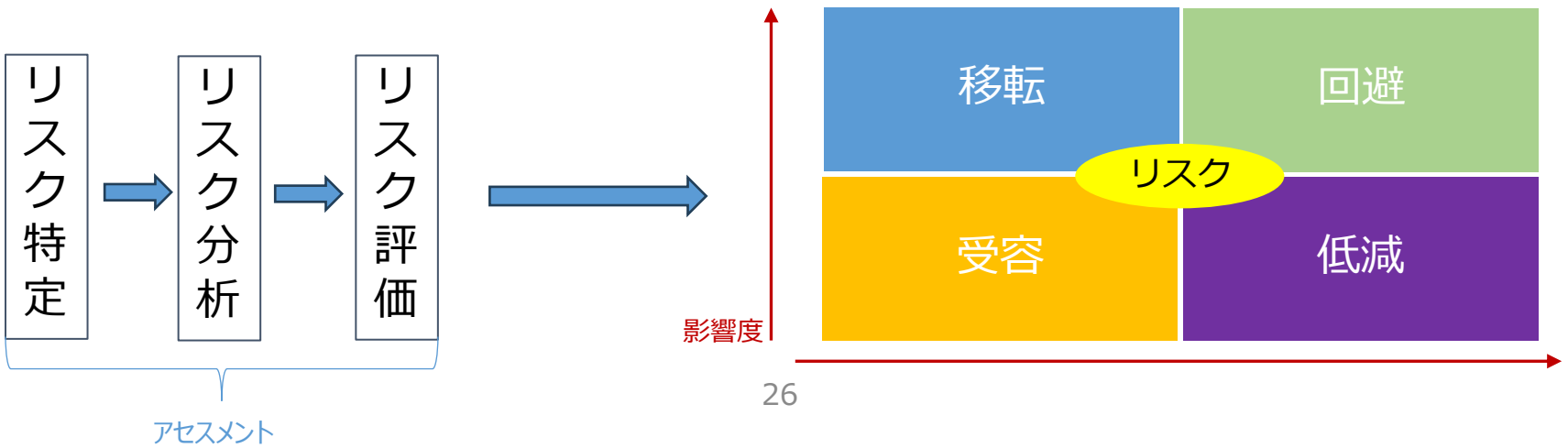

性質
→ 即時性必須
4時間
停止
1日停止
性質
→ 在庫3日分あり


代替環境
なし
性質
→ 即時性必須
4時間
停止
代替環境
あり
1日停止
性質
→ 在庫3日分あり


協力
会社
なし
代替環境
なし
性質
→ 即時性必須
4時間
停止
代替環境
あり
協力
会社
あり
1日停止
停止
性質
→ 在庫3日分あり

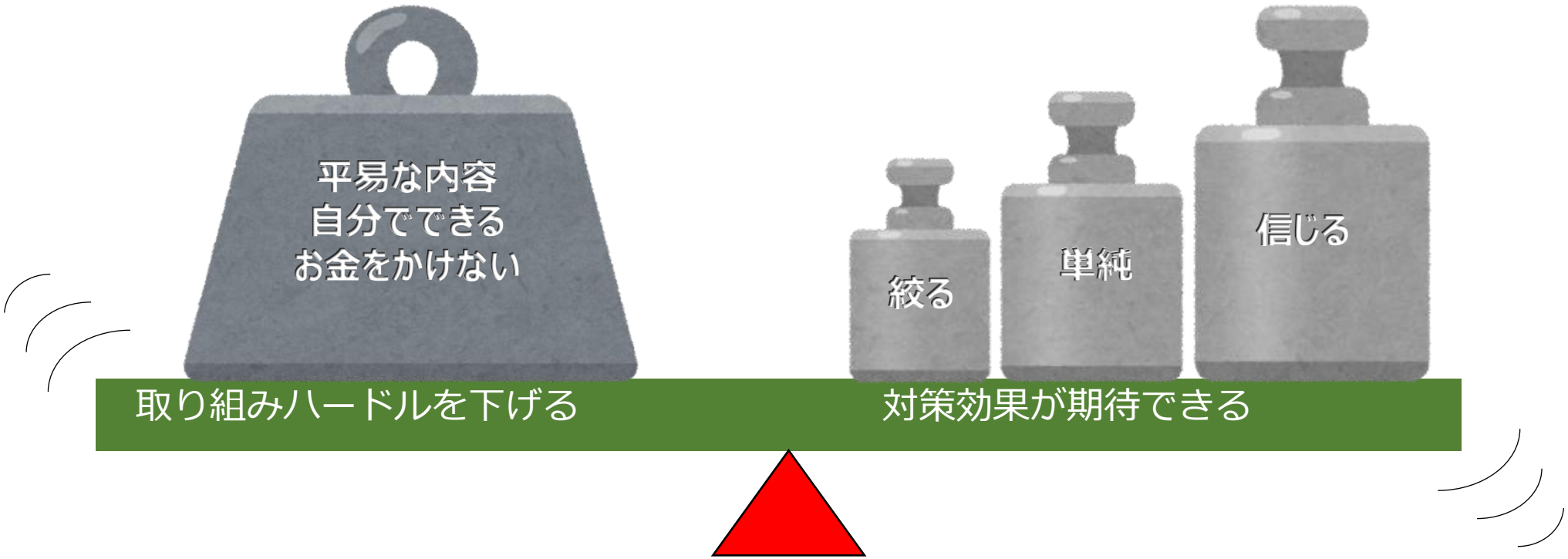
- システムが止まって、どのくらいの時間耐えられるか

→ 在庫の状況 や システムの性質に依存する
→ バックアップ や 代替環境 で 運営継続ができるのか
→ 協力会社に 一旦 変わりを頼める環境か？
　取引先が待ってくれるか？



考え方

教科書に書かれた正解を目指すのではなく、範囲を絞ってできる事を！



(2) 専門家 と 呼ばれる人たち

<JNSA会員企業>

https://www.jnsa.org/aboutus/03.html

2025年08月15日現在　302社

<サイバーインシデント緊急対応企業一覧>

https://www.jnsa.org/emergency_response/

※ 緊急で被害調査や被害切り分け、
復旧などの対応を請け負ってくれるJNSA所属企業

2025年06月現在　40社

<JNSAソリューションガイド>

https://sg.jnsa.org/

言いたかったのは、、、

- 「専門家」って言われる人は、割といっぱい いる

- 利用者は、「専門家」に、何を求めているか、**ちゃんと 言えないといけない**
  → **何が必要か、何をしてほしいか(導入範囲、作業範囲、保守要件等)**を伝える
  → 止まったら「電話したらなんとかしてくれる」と思うなかれ

- 「専門家」は、利用者のニーズに耳を傾けるべし
  → **サービス/製品の**押し付けは、ご法度。
  「何をどこまで」を聞かない、説明しない　は、
  できる事を できない と言って 売るのと同じ。

お互いのコミュニケーションで、市場は活性化する

(3) 意外と すっと入ってくる気もする

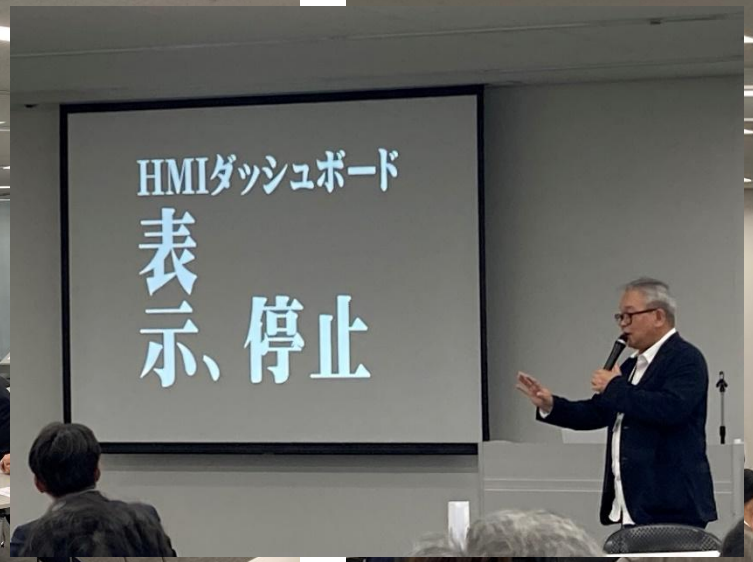
製造現場を見学させてもらった際の様子

- **とても、整理された工場内**
  - → ナンバリングされて 整頓された装置類
  - → 効率化された動線
  - → 実は、故障した時のために バックアップなんかも ちゃんとある・・・

日本の6割弱が ISO 9001(品質管理マネジメント)を取得している状況
ISO 14001(環境マネジメントシステム)も3割強が取得している。
その他、「5S活動」には積極的
→「マネジメント」する という素養はすでにある。
→ あとは、「セキュリティ」に取り組むと お得という何かが必要・・・

セキュリティ侵害・疑似体験ワークショップ

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



今後も、こういったワークショップをパッケージング化して開催予定
「利用者」「専門家」でコミュニケーションをとる場を大切に・・・

4. まとめ

- **中小製造業は、日本の「ものづくりの要」**
  ここが危険な状態は、土台がグラグラなのと同じ

- **中小製造業の方々が、ご自身で取り組むべき事**
  「難しい」「わからない」で見てみないフリしない。
  とりあえず、目に見える/できる所から初めてみて。
  ときには、専門家を頼ってください。

- **専門家と呼ばれる人**
  もっと、頑張らんとあかんよ。
  「市場が盛り上がる → 価値ある製品・サービスが登場し競争が起きる → 顧客の目がこえる」 が理想

「ガチガチのセキュリティ」「使い難くするためのセキュリティ」を
目指しているわけではなく、
より生産性を上げる/価値ある製造ためのIT利活用を目指して・・・