JNSA2024年度活動報告会

中小製造業の工場セキュリティ対策を支援する取組みのご紹介

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7月17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30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の関するハンドブック

本日のお話

１．これまでの取り組み（振り返り）

２．成果物のご紹介

３．これからの取り組み

1.これまでの取り組み（振り返り）

このWGが目指すこと

そんな
有名ちゃうで

うちは
大丈夫や！

大事なもん
ないで

中小製造業が自らの手で工場セキュリティ対策を行えるように支援すること

助けて
くれるん？

お金かかるん
とちゃうの

そんなん
難しいわ

何が問題なのか（実態）

●問題意識がない

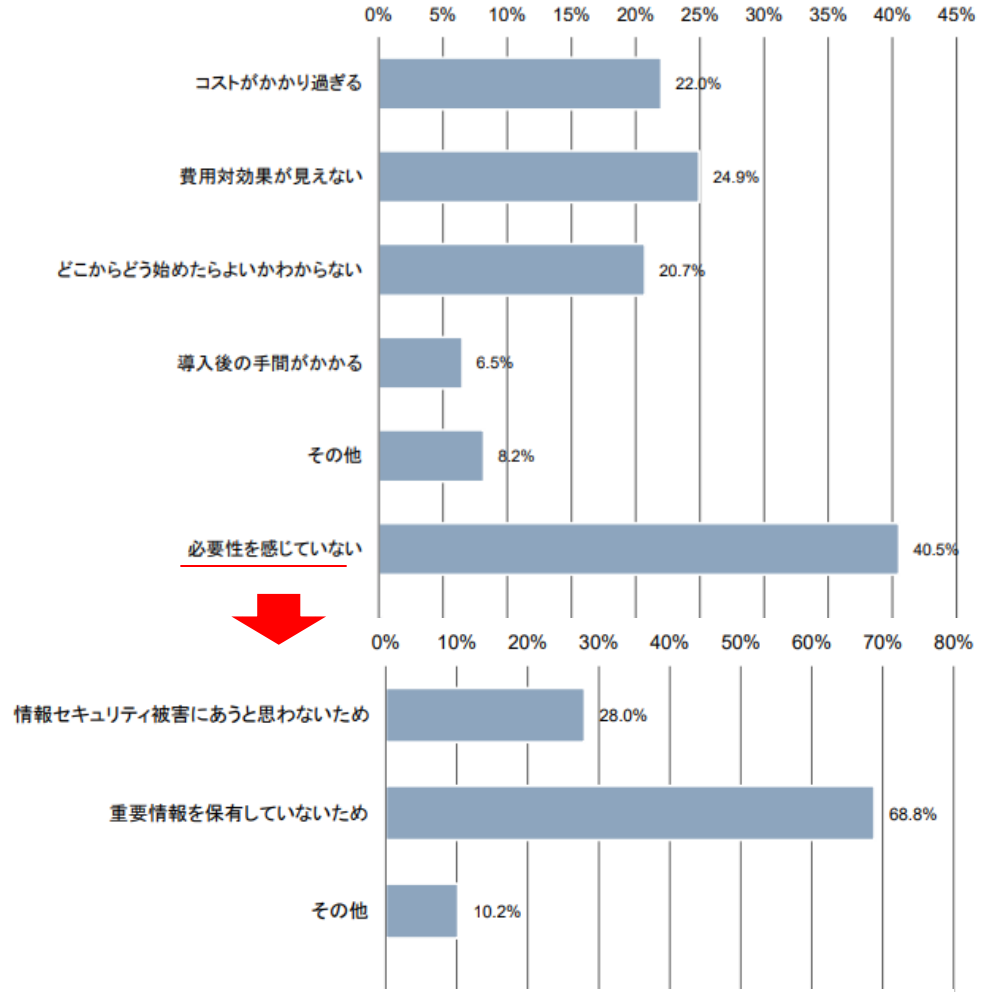
- 自然災害や火災ほど身近に感じられない
- 高度なITシステムは使っていない
- 日常業務や生産性向上が優先される

●根拠のない自信

- 狙われるのは大企業のみという思い込み
- 既存の対策で十分だと誤認している
- 他社の被害事例を他人事と捉えている

●知識がない

- 攻撃の手法や被害の実態に関する情報が不足
- 専門知識を持った人材が社内にいない
- 社内研修や外部セミナーに参加する余裕がない



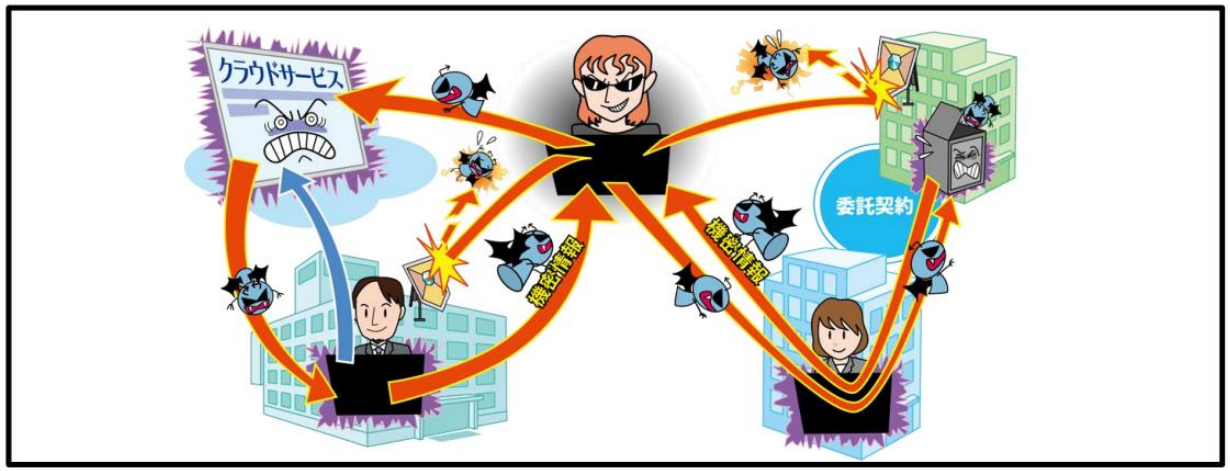
IPA「2021年度中小企業における
情報セキュリティ対策に関する実態調査」より抜粋
有効回答数4,074（製造業11.8%）

問題を放置できない中小製造業

【2位】サプライチェーンの弱点を悪用した攻撃

IPA

～自組織だけでなく、委託先や利用しているサービスも適切な管理を～



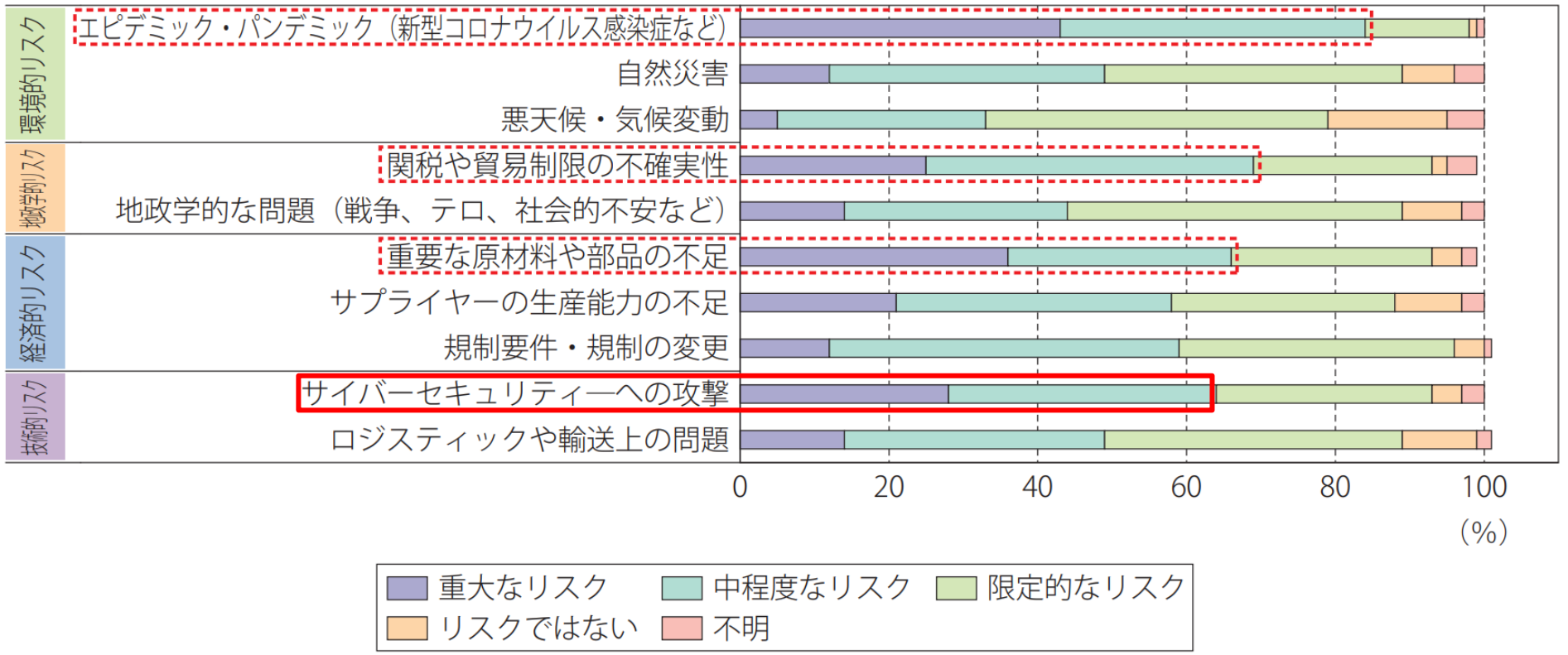
- 調達から販売、業務委託等一連の商流において、セキュリティ対策が甘い組織が攻撃の足がかりとして攻撃される
- ソフトウェア開発のライフサイクルに関与するモノや人の繋がりを足掛かりとする（ソフトウェアサプライチェーン）攻撃も存在
- 取引先や業務を委託している外部組織から情報漏えい

IPA
情報セキュリティ10大脅威 2023　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

サプライチェーンリスクの認識



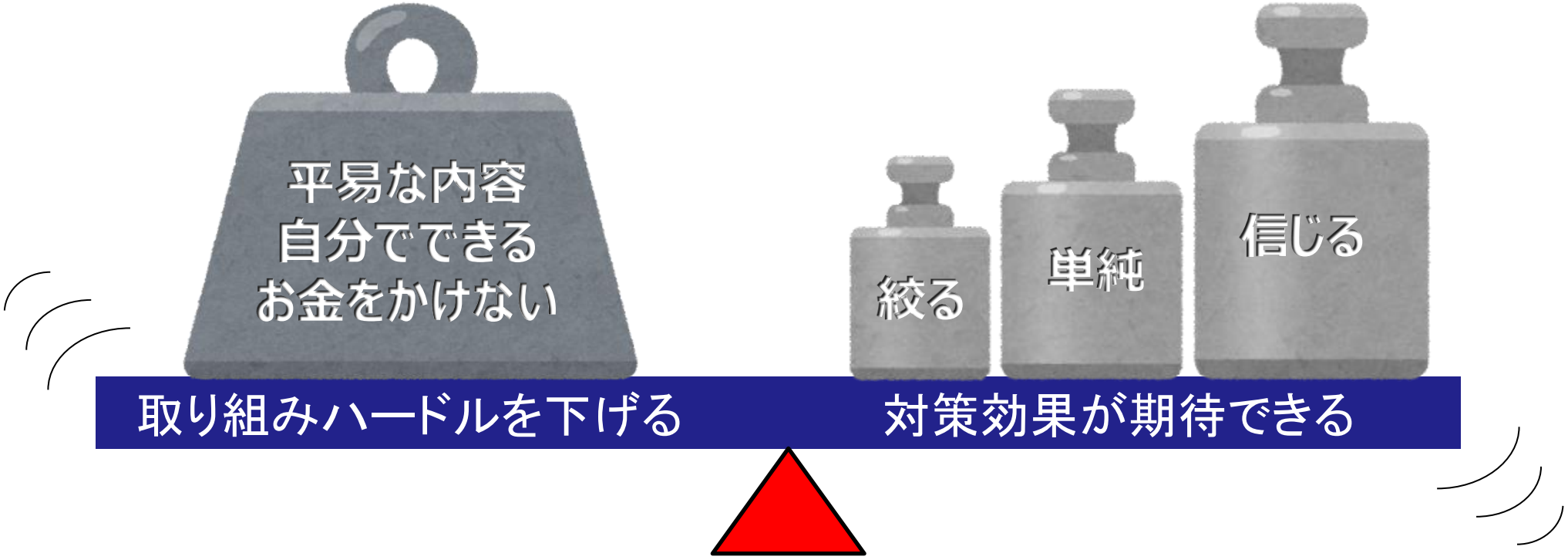
経済産業省
令和３年版　通商白書
第Ⅱ部第二節
第Ⅱ-1-2-3図
サプライチェーンリスクの認識（2020年）

ターゲットを絞って意図的に起こせる脅威

RaaS（Ransomware as a Service）の出現で攻撃は容易に実行可能

どのように支援するか

教科書ではなく参考書として気軽に扱える**ハンドブック**を作ろう！



主な取り組み実績

●2022年　5月　工場セキュリティハンドブック・リスクアセスメント編（検討会16回）公開
●2022年　5月　NSF2022 in Kansai 開催
●2023年　8月　関西情報セキュリティ合同セミナーで活動紹介
●2023年10月　NIRO主催セミナーで活動紹介
●2023年12月　NSF2023 in Kansai 開催
●2024年　2月　NSF2024で活動紹介＆2023年度JNSA賞受賞
●2024年　2月　経産省第7回工場SWGで活動紹介
●2024年　3月　工場セキュリティハンドブック・リスク対策編（検討会21回）公開
●2024年　6月　工場セキュリティガイドライン啓発・連続セミナーで活動紹介

2.成果物のご紹介

1st STEP　リスクアセスメント

● 13の脅威の入口とリスクシナリオに沿ったアセスメントを提唱

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ると考えています

ハンドブック・リスクアセスメント編

JNSA

取り組みハードルを下げる VS 対策効果が期待できる

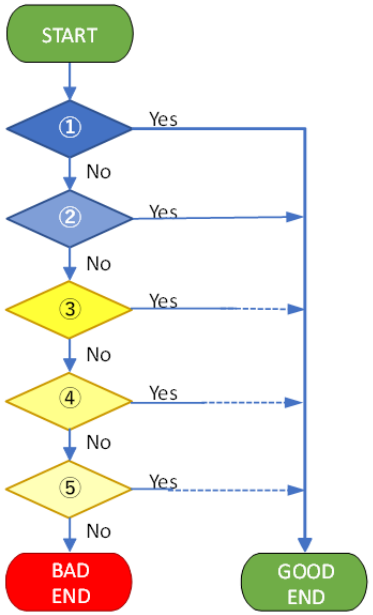
● 一般的手法とは異なるユニークな手法で現場の担当者が簡単に実施できることを目指しています。

No.7 OAネットワーク

リスクシナリオ ☞

リアルタイムな生産情報収集のために、新たに工場とOA 棟（一般オフィス棟）をネットワークで接続したところ、工場内の生産制御システムに異常が発生し、生産が停止した

アセスメントフロー ☞



現状の対策状況		対策の効果等
①	OAネットワーク（一般オフィスネットワーク）と工場ネットワーク（製造現場LAN）は物理的に繋がっていない	物理的に繋がっていないので、ネットワークを経由して脅威が侵入することはない
②	工場ネットワークには、OAネットワーク内の特定のPCやサーバー以外はつながらないように制限されている	工場ネットワークにつながる機器を制限することで、OAネットワークの影響を軽減することができる
③	工場ネットワーク内のPCや生産制御システム（サーバー）にはウイルス対策ソフトが導入されている	ウイルス対策ソフトの導入により、マルウェアの感染を防止できる。ただし、ウイルス対策ソフトが導入できない機器は感染する可能性がある
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

☞ チェックポイント

※ルールは徹底され、適切に運用されていることが前提

アセスメント結果の評価例

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	古い機種の入れ替え検討が必要
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

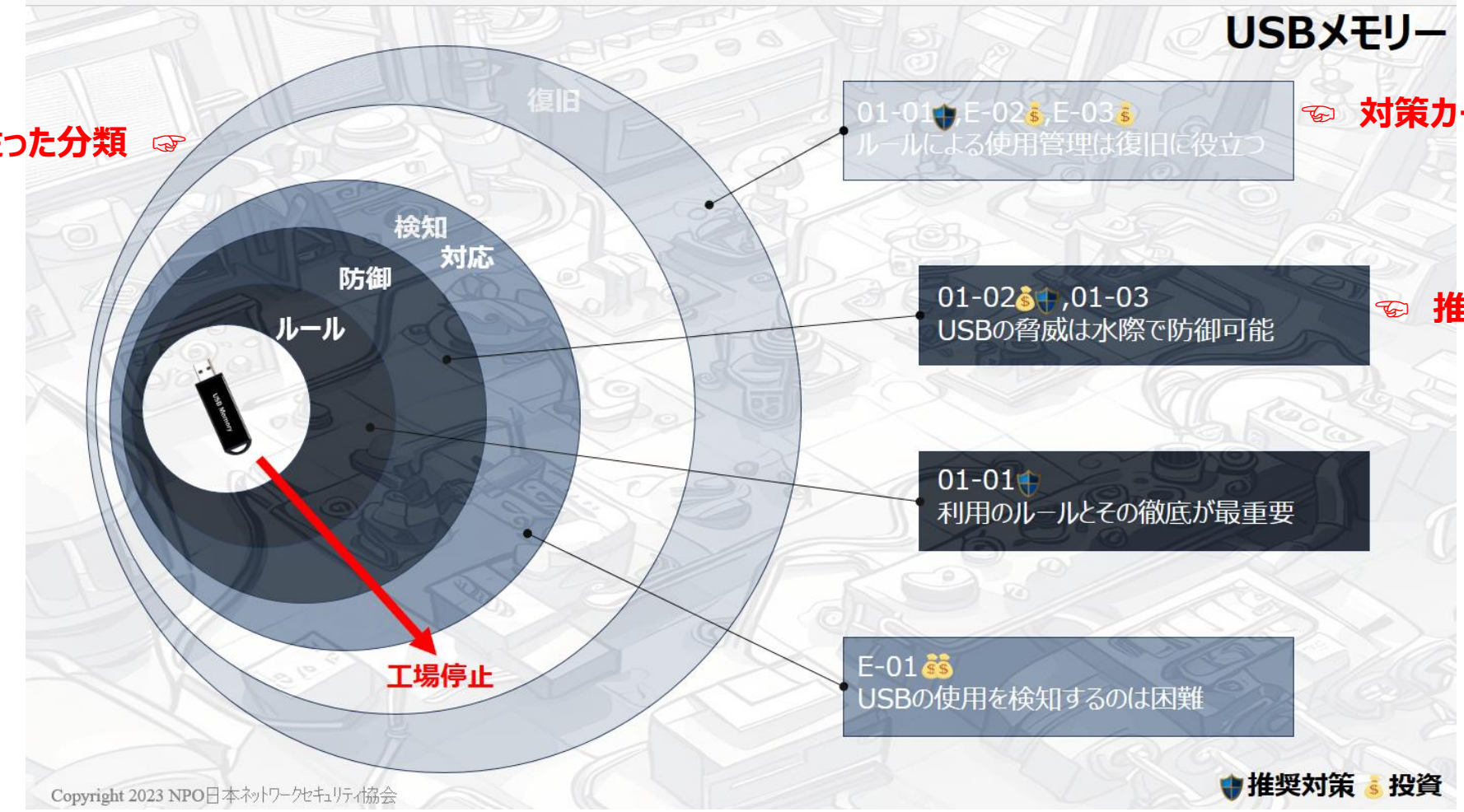
● 13の脅威の入口に対応した対策と共通対策を整理

ハンドブック・リスク対策編

JNSA

● 現場の担当者が選択しやすいように対策の分類や投資の有無なども記載しています。

フレームワークに従った分類 ☞



☞ 対策カードにリンク

☞ 推奨、投資の大きさなど

ハンドブック・リスク対策編

取り組みハードルを下げる VS 対策効果が期待できる

●現場の担当者が自らの手で実行できるように対策の要点を記載しています。

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

●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混入しないよ

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

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

ウイルスチェック機能付きのUSBメモリーを用意し、工場内ではこの使用のみを許可する。なお、対策No.01-01と併せて実施するとより効果的である。

●運用のポイント

USBメモリー内に組み込まれたウイルスチェックプログラムやウイルスパターンファイルは適宜アップデートが必要なため、インターネットに接続可能なパソコンにUSBメモリーを定期的に接続し、管理台帳に実施記録を残すこと。

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：対応製品は複数のメーカーが販売している。USBメモリーの容量が2GBの場合、6,500円～（2023.6時点）

3.これからの取り組み

ハンドブック・サイバーBCP策定編（検討中）

- リスクアセスメント編、リスク対策編を踏まえて、セキュリティ脅威に対するBCP策定を支援するハンドブックを検討中。（24年12月公開予定）

- 災害等に対応したBCPとは独立したIT-BCPの位置づけ。ただし、一連のハンドブックで想定しているセキュリティリスク（13の脅威の入口に関連）を対象とする。

- BCPを策定する手順やポイントの解説に加えて、ひな形を提供する予定。また、このひな形を環境に合わせてカスタマイズするポイントについても解説する。

生成AIの活用（実験）

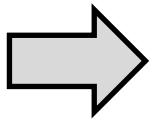
取り組みハードルを下げる VS 対策効果が期待できる

● 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？

適切な定義ができるか？

環境差分抽出表

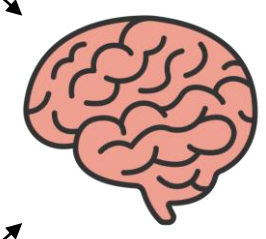


AI用BCPひな形
（カスタマイズ対象部分を＃＃で囲む）

環境差分

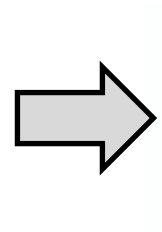
プロンプト
（BCPひな形の＃＃で囲まれた部分を環境差分に応じてカスタマイズせよ）

プロンプトの作成



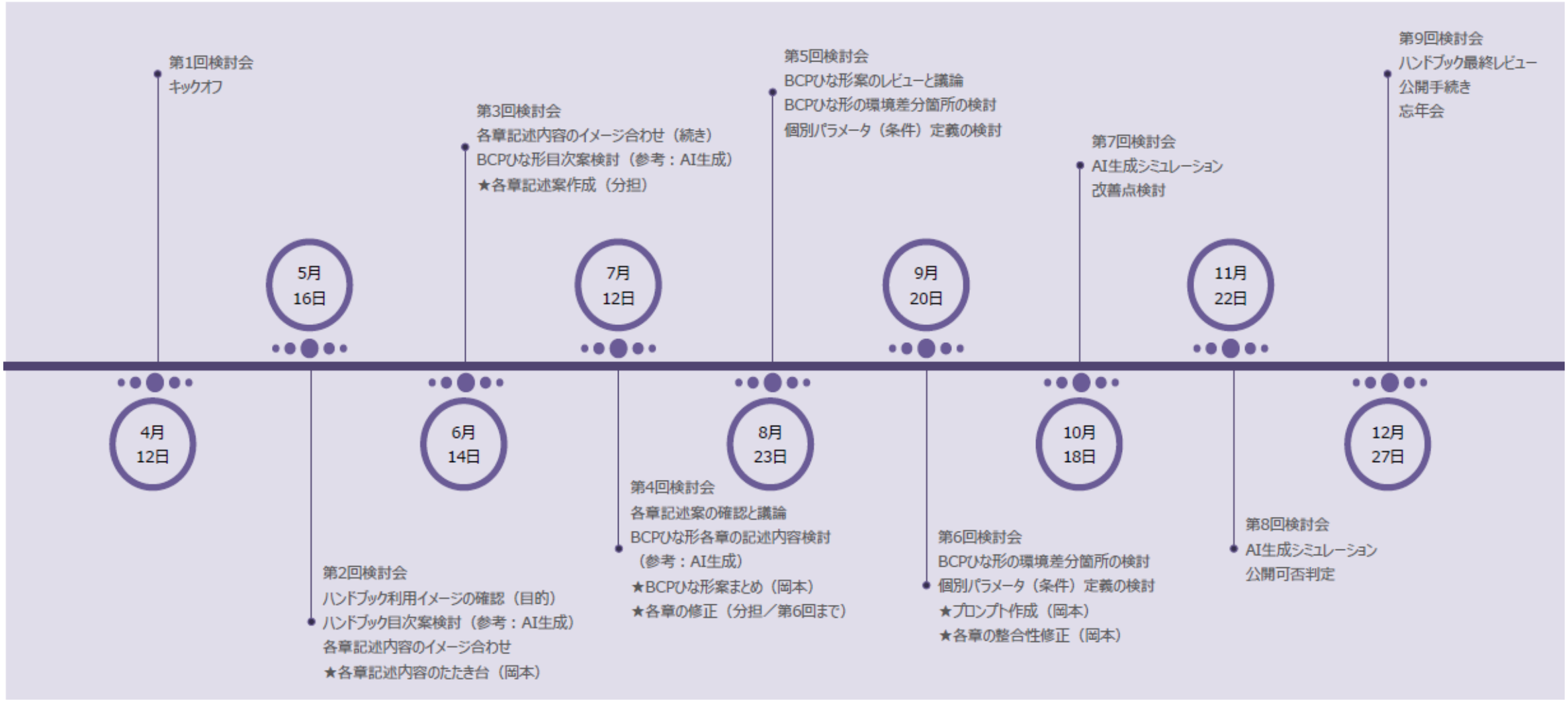
生成AI

使い物になるか？



カスタマイズBCP

スケジュール



ワークショップ（検討中）

NSF2023 in Kansaiで実施したワークショップをベースに、

「サイバー攻撃を受けたら」

を体験し、その後の対応をみなさんで考えるパッケージコンテンツを検討中。

中小製造業の方々が集まるセミナーや勉強会に西日本支部のメンバーが出張して対応します。（基本的に無償）

詳細は近日、JNSAホームページにて公開予定。


JNSA