



工場セキュリティガイドライン啓発・連続セミナー

実践できる中小企業の工場セキュリティに 向けた活動のご紹介

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6月5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

- 1. セキュリティ対策の重要性**
- 2. 中小製造業のセキュリティ事情**
- 3. ハンドブックを活用した対策の紹介**

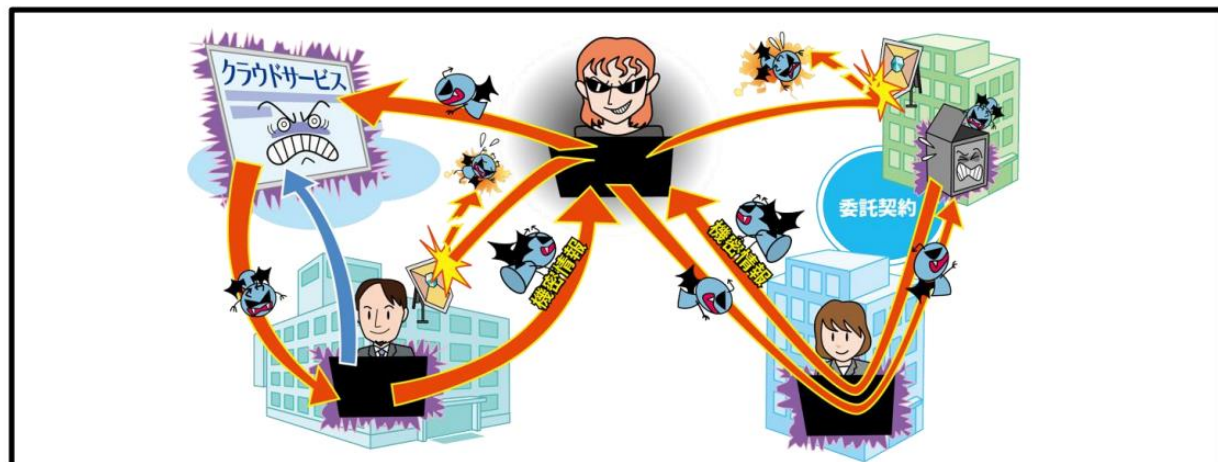
1. セキュリティ対策の重要性

本当に危ないのは誰？

【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～



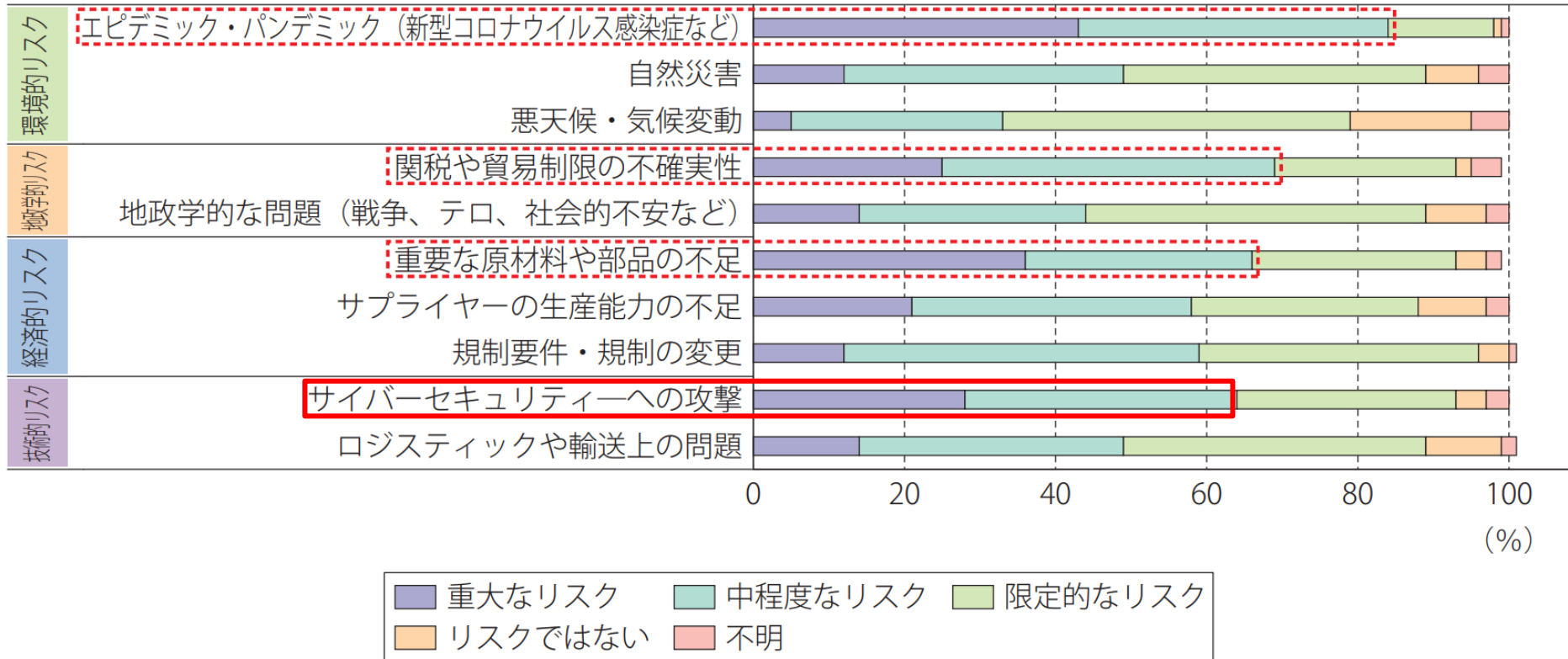
- 調達から販売、業務委託等一連の商流において、**セキュリティ対策が甘い組織が攻撃の足がかり**として攻撃される
- ソフトウェア開発のライフサイクルに関与するモノや人の繋がりを足掛かりとする(**ソフトウェアサプライチェーン**)攻撃も存在
- 取引先や業務を委託している**外部組織から情報漏えい**

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

IPA
情報セキュリティ10大脅威 2023 より抜粋

サプライチェーンリスク



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

参考（VPN装置への攻撃）

- ある食品製造業様での観測データより
 - データ期間：1月1日～2月29日
 - 採取対象：インターネット公開及び社外関連会社VPN接続口のFW/IPログ
- 1月10日、VPN装置の脆弱性情報が公開される
- VPN装置への最初の攻撃検知：1月17日（15件） ⇒ ブロック
- この期間の公開サイトへの攻撃数：8,352件
この中に、VPN装置を狙った攻撃はゼロ件 ⇒ **的確にVPN装置を把握して攻撃**

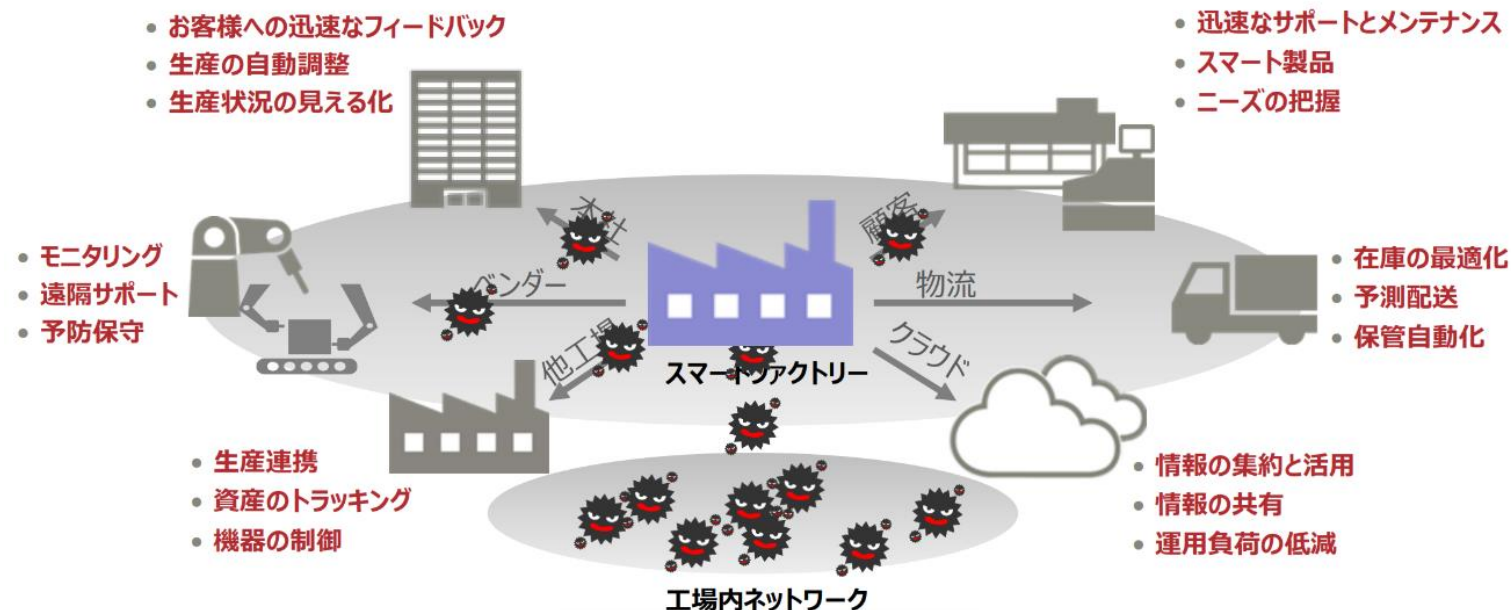
被害者から加害者へ

●生産停止の影響

基本的な対策を怠っているとセキュリティ侵害による生産停止の責任を問われる

●DXの推進で新たな脅威

安易なネットワーク化は新たな脅威を生むことになる。
知らずに飼っていたマルウェアを
まき散らす原因になるかも。



2. 中小製造業のセキュリティ事情

中小企業の生産現場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/L2スイッチ）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。

●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。

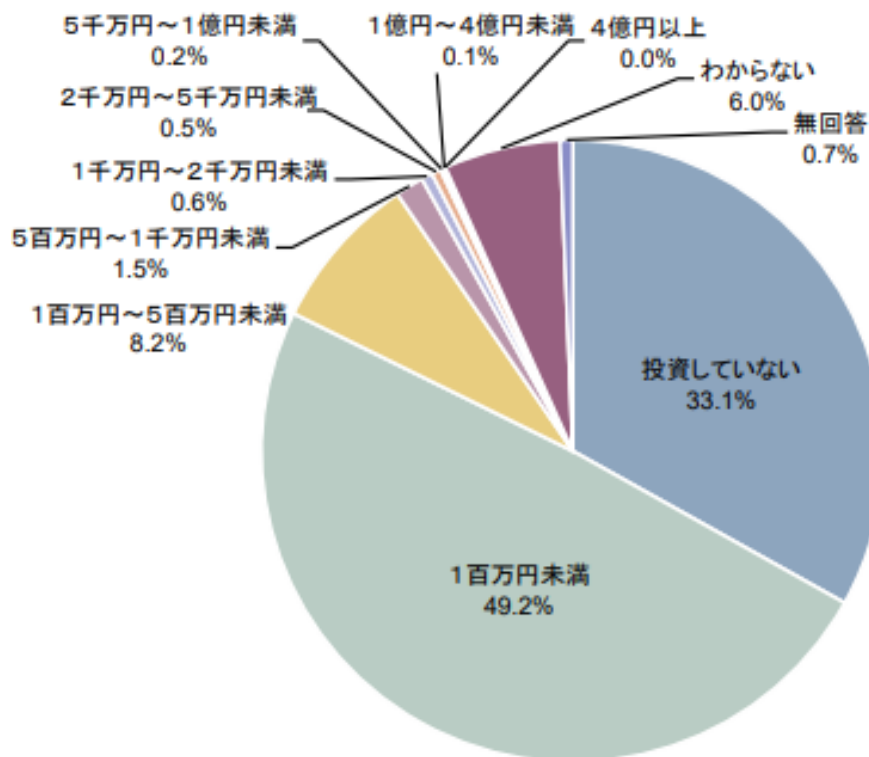
●セキュリティ侵害を受ける可能性

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。

中小企業の意識①

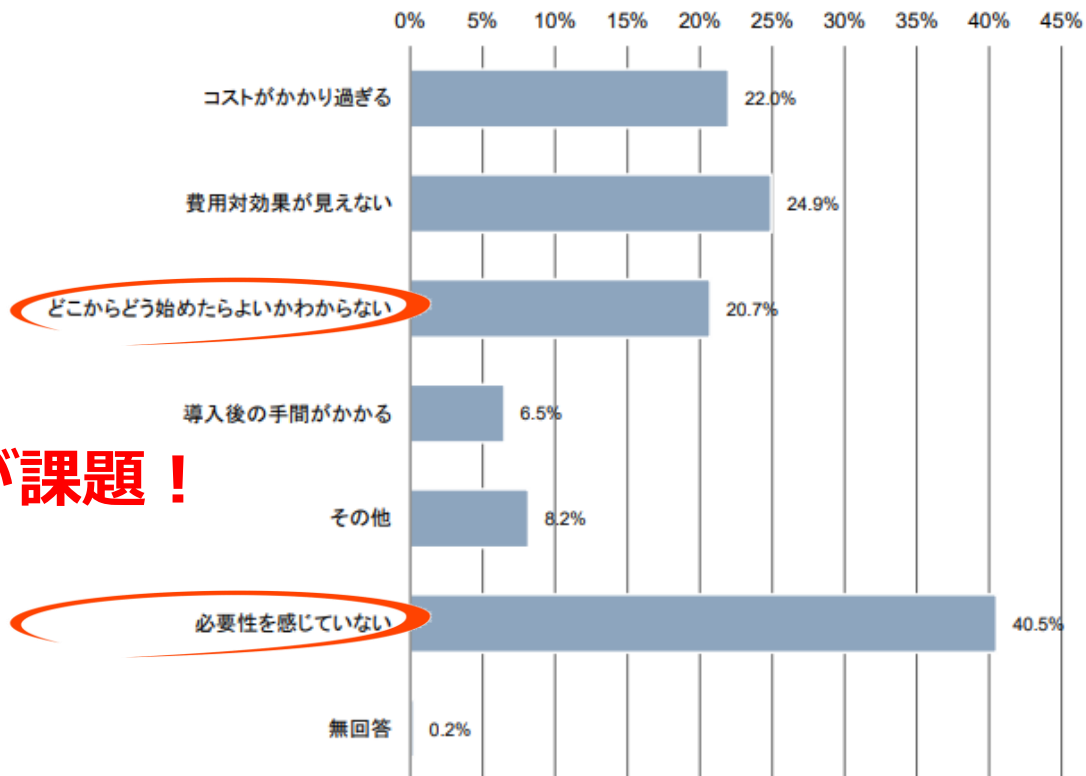
直近過去3期の情報セキュリティ対策投資額

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！

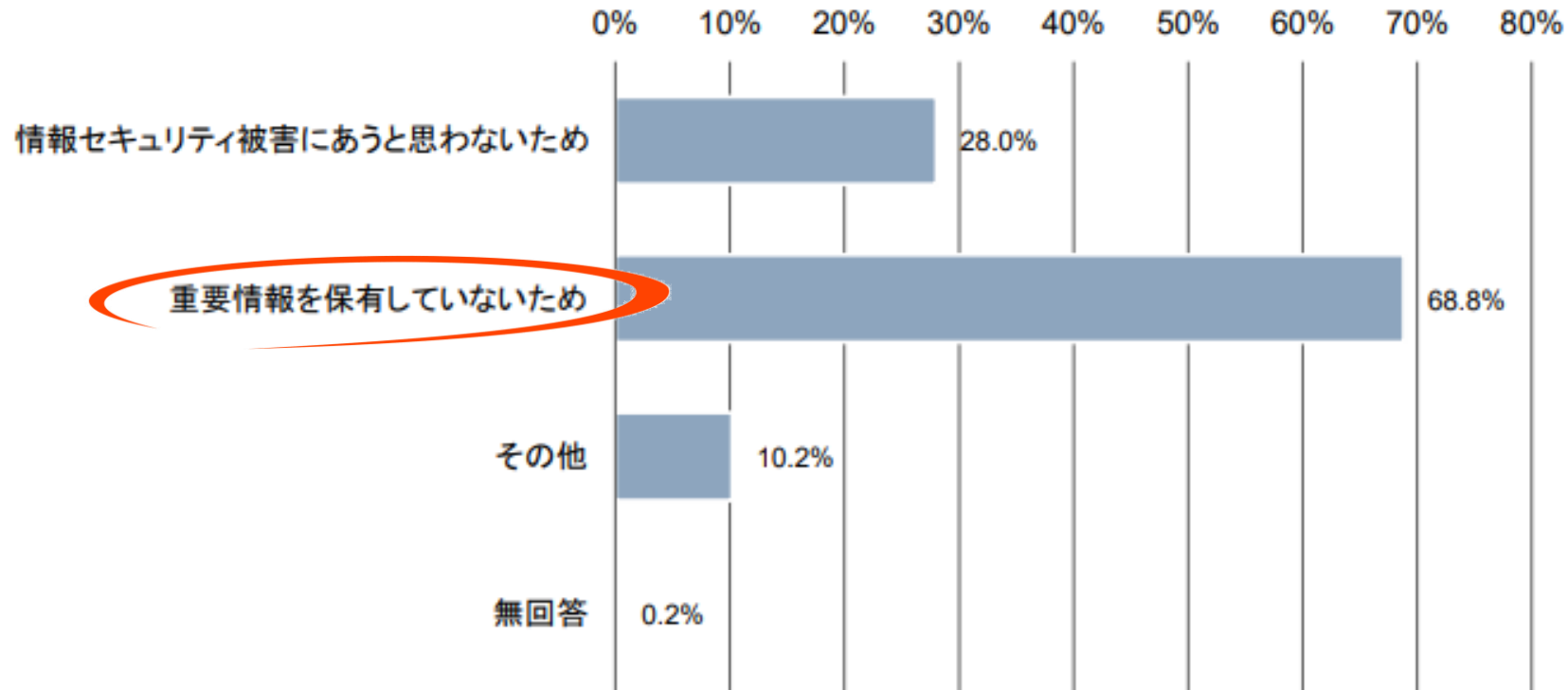
- ・製造現場にはセキュリティの専門家がいるわけではない
- ・迫っている脅威、リスクの大きさに気づいていない

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%）

中小企業の意識②

情報セキュリティ対策の必要性を感じない理由

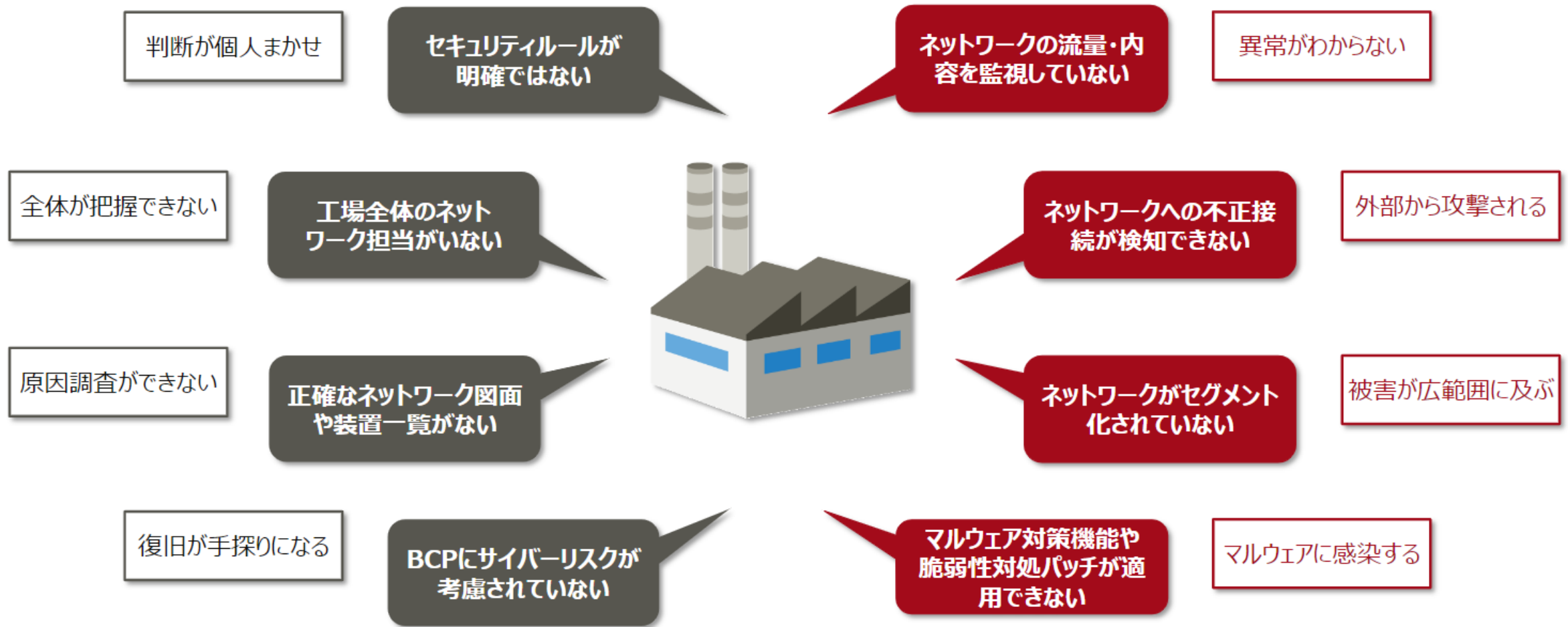
n=1,259



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

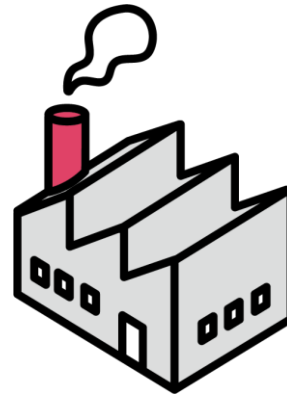


中小企業工場へのアプローチ

知識もノウハウもない

経済的な余裕はない

頼れる先もない



本当に取り組めるのか？

WGの重大テーマ

取り組みハードルを下げる



対策効果が期待できる

3.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実行できること～

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

- 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。

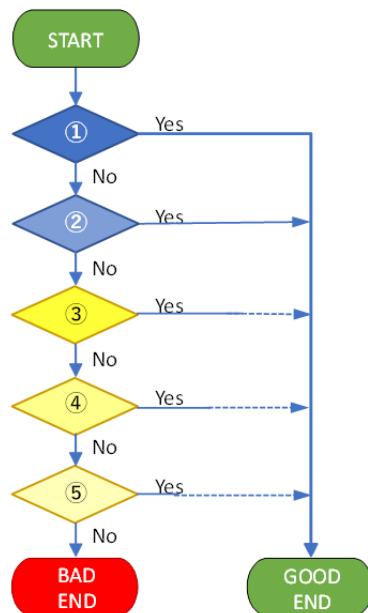
No.7 OAネットワーク

取り組みハードルを下げる 対策効果が期待できる

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



チェックポイント

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

※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

高度な共通対策 (E-01~03)

脅威の入口ごとの対策 (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)

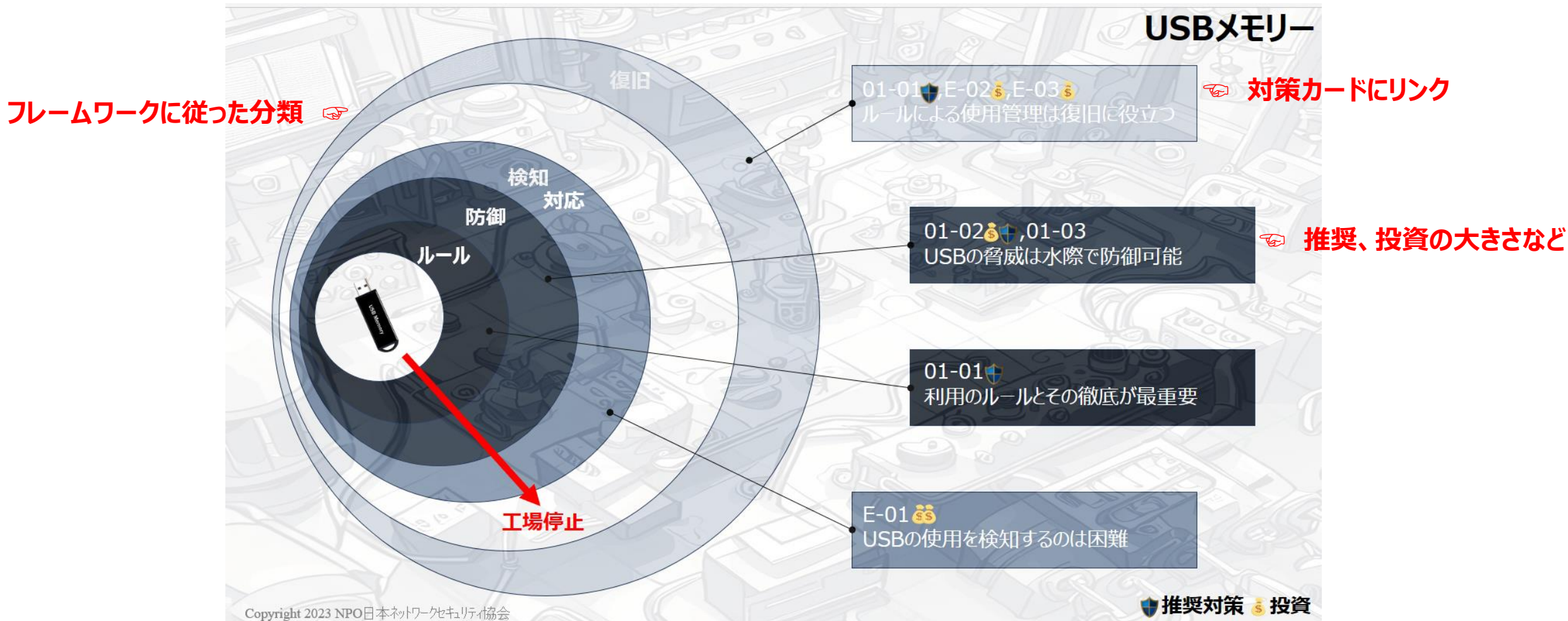
部品・原材料
(12-01~03)

新規購入機器
(13-01~02)

基礎的な共通対策 (C-01~05)

ハンドブック・リスク対策編

- 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。



●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。

取り組みハードルを下げる 対策効果が期待できる

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

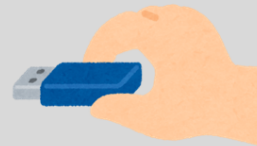
工場内で使用を許可するUSBメモリーとその取り扱い方法をルールとして明文化し周知徹底する。

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混入しないよう



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のため、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）

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

- 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）

- 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



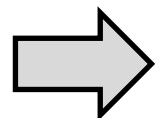
事業者自らがカスタマイズできるか？

取り組みハードルを下げる 対策効果が期待できる

適切な定義ができるか？



環境差分抽出表

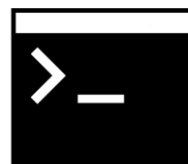


環境差分

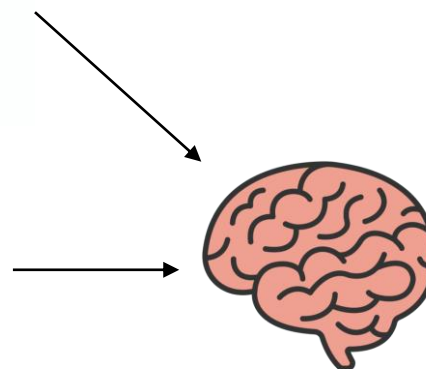
AI用BCPひな形
(カスタマイズ対象部分を##で囲む)



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)

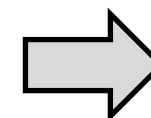


プロンプトの作成



生成AI

使い物になるか？



カスタマイズBCP

JNSA