西日本支部
工場セキュリティ対策ハンドブック完結のご報告

JNSA西日本支部
工場セキュリティWGリーダー

岡本　登

JNSA

はじめに

2020年11月 「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」 発足

- 関西を中心に参加メンバーは延べ約30人（西日本以外からも参加）

- テーマは「中小製造業の皆様が自らの手で実践できるセキュリティ対策」を考える

- 成果物：工場セキュリティハンドブック 3部作
  - ・リスクアセスメント編 (2022年5月公開)
  - ・リスク対策編 (2024年3月公開)
  - ・サイバー対応 IT-BCP策定編 (2025年4月公開)
- セミナー：・他団体のセミナー等で取り組みの紹介多数
  - ・インシデント発生を体験するワークショップ

WG活動の背景

●問題意識がない

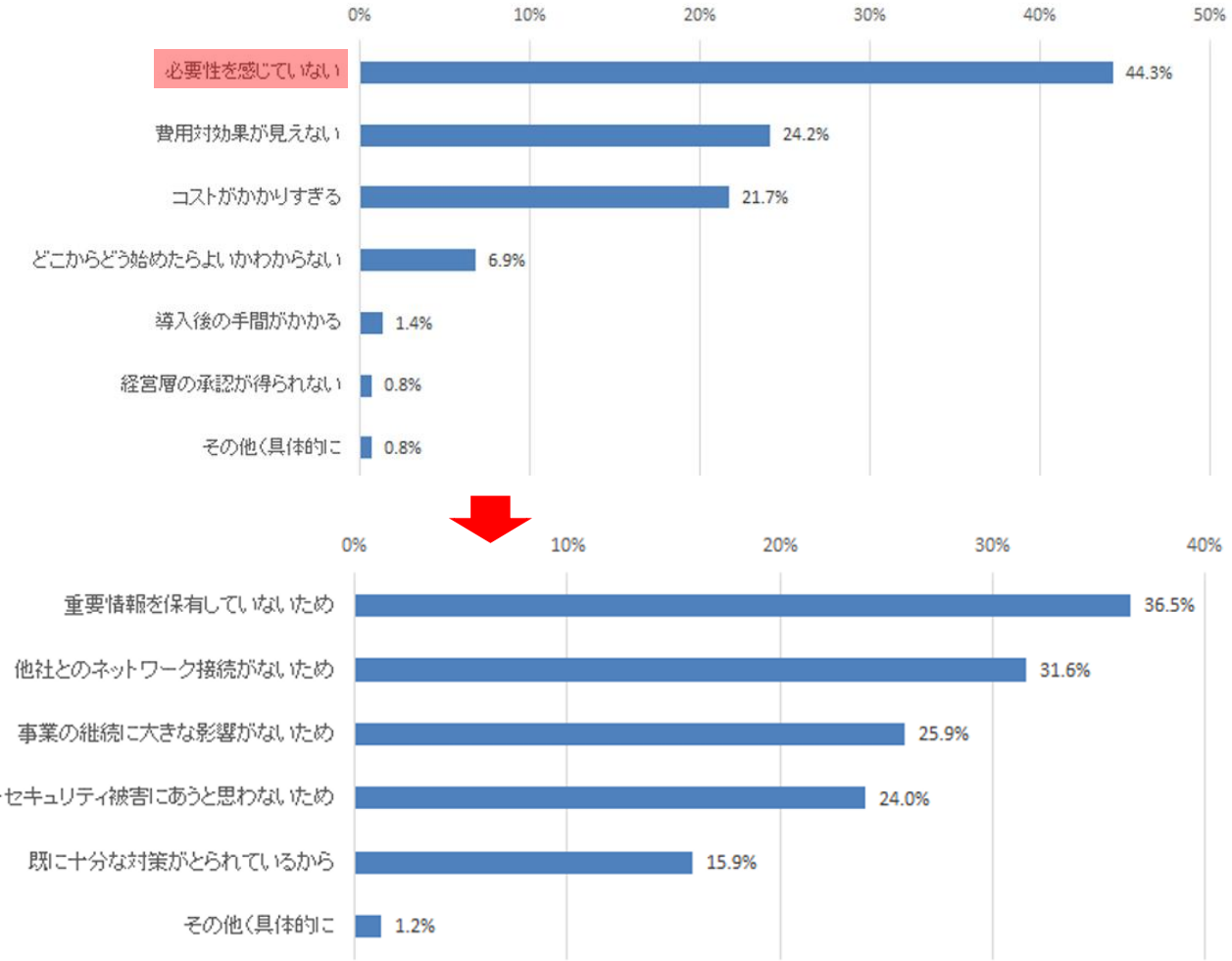
- 自然災害や火災ほど身近に感じられない
- 高度なITシステムは使っていない
- 日常業務や生産性向上が優先される

●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「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

WGが目指すコト

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

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

第1弾 リスクアセスメント編 - 脅威の可視化

ハンドブック概要

：製造現場におけるセキュリティリスクを理解し、自社の現状を把握するための参考書

● 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

第1弾 リスクアセスメント編 - 脅威の可視化

JNSA

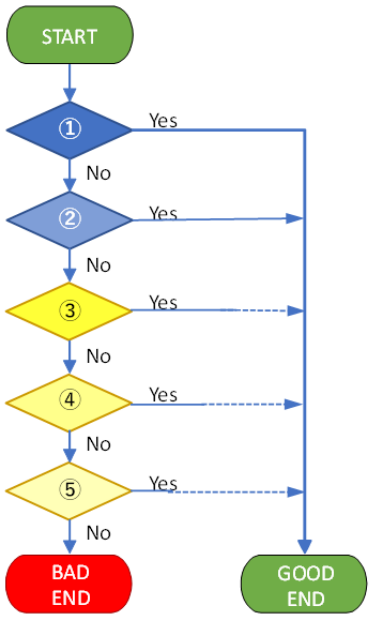
● 一般的手法とは異なるユニークな手法で現場の担当者が簡単に実施できることを目指しています。

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

第1弾 リスクアセスメント編 - 脅威の可視化

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）

第2弾 リスク対策編 - 具体的な対策の実践

● 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）	

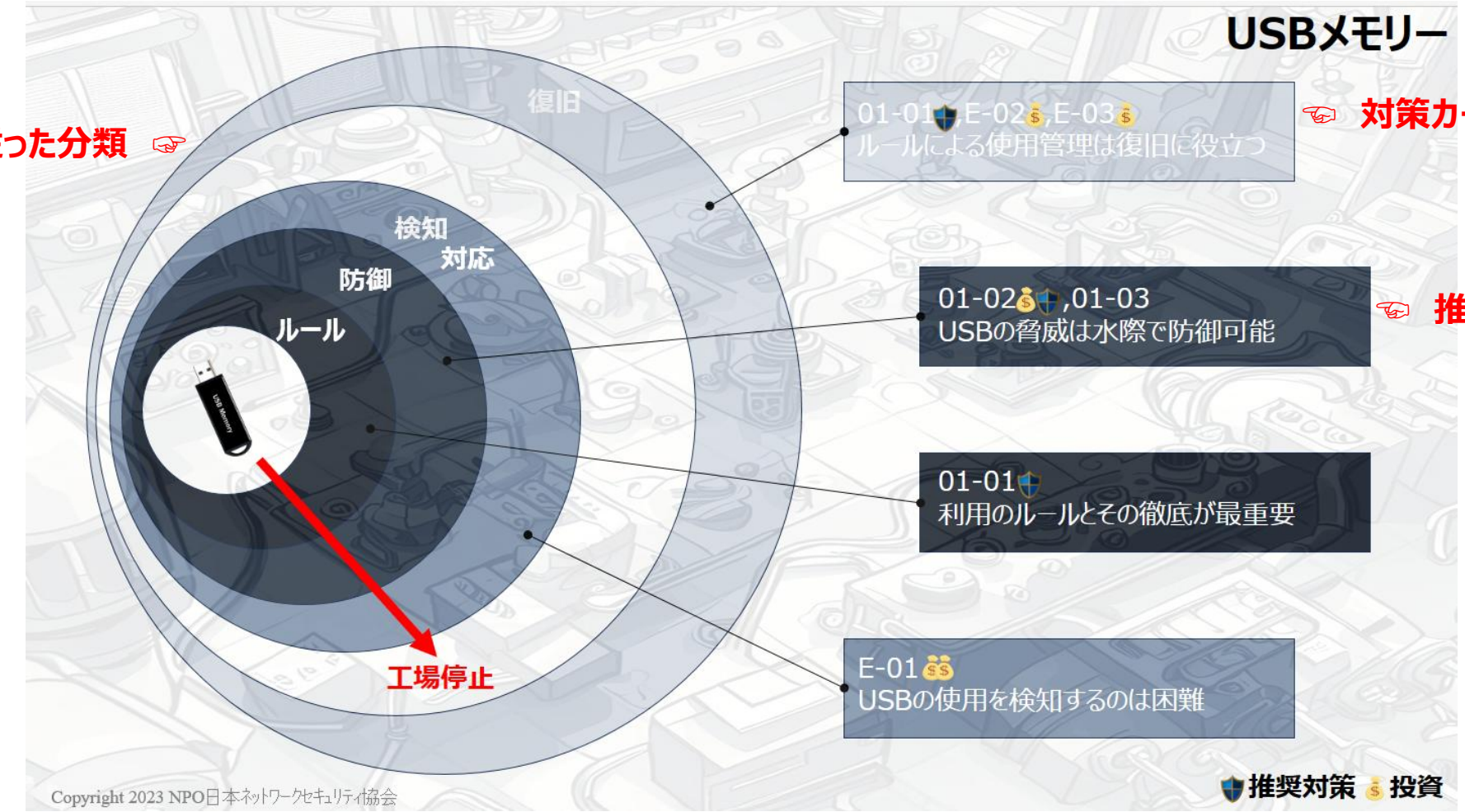
基礎的な共通対策（C-01~05）

第2弾 リスク対策編 - 具体的な対策の実践

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

第2弾 リスク対策編 - 具体的な対策の実践

JNSA

●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）

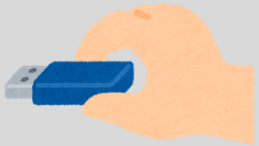
-管理責任者、識別番号、保管場所、ウイルスチェックデータ更新日※1

-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）

第3弾 サイバー対応 IT-BCP策定編 - 万が一への備え

JNSA

一般的なIT-BCPの記載項目例（赤破線枠）

BCP管理項目		リスク種別			
		自然災害・停電	システム障害	人的リスク	法的リスク
保護資産	ITシステム	・拠点被災時の代替システム確保 ・データセンターの選定 ・電力供給計画	・ハードウェア故障時の交換計画 ・ソフトウェア不具合時のロールバック計画 ・構成管理	・誤操作によるシステム停止対策 ・内部不正によるシステム破壊対策	・データ保護規制遵守 ・サービス停止による契約不履行対策
	データ・情報	・バックアップデータの保管場所分散 ・データ保全計画	・データ破損時の復旧手順 ・定期的なデータ整合性チェック	・誤削除対策 ・不適切な情報開示対策 ・機密情報の持ち出し対策	・個人情報保護法遵守 ・知的財産保護 ・データ保持期間の管理
	建物・設備	・代替オフィスの確保 ・免震・耐震構造 ・発電機・UPS設置	・空調・電源設備の故障対策 ・物理セキュリティ対策	・設備へのいたずら・破壊防止 ・不法侵入対策	・労働安全衛生法遵守 ・設備に関する契約遵守
	人材	・安否確認と参集計画 ・拠点分散勤務体制 ・災害時指揮命令系統	・システム操作担当者の複数化 ・業務継続のためのスキルマップ	・内部不正防止策 ・セキュリティ教育・訓練 ・ストレスマネジメント	・労働関連法規遵守 ・ハラスメント対策
	サプライチェーン	・複数サプライヤーの確保 ・物流ルートの多角化	・システム連携部分の障害対策 ・サービスレベルアグリーメント（SLA）確認	・委託先の情報漏えい対策 ・協力会社との連携強化	・契約内容の見直し ・秘密保持契約（NDA）の締結

サイバー対応IT-BCP

リスク種別
サイバー攻撃
・マルウェア感染からの復旧手順 ・ネットワーク遮断計画 ・バックアップとリカバリ戦略
・データ暗号化対策 ・データ窃取時の対処法 ・バックアップデータの保全
・物理的破壊からの防御（例：データセンターの物理的保護） ・監視カメラ設置
・サイバーセキュリティ訓練実施 ・緊急時連絡網の確保 ・セキュリティ意識向上教育
・委託先のセキュリティ対策状況確認 ・サプライチェーン全体のセキュリティ監査 ・緊急時協力体制の構築

一般的なIT-BCPではサイバー攻撃には対応できない

第3弾 サイバー対応 IT-BCP策定編 - 万が一への備え

事前対策を実施する
- リスクアセスメント
- リスク対策

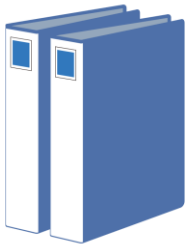
基本方針を決める
- 既存BCPとの整合性

判断基準を決める
- 何を以って侵害とするか

運用体制を決める
- 意思決定者
- 対応チーム
- 役割分担

緊急手順を決める
- 初動対応
- 被害拡大防止
- システム復旧
- 情報共有

サイバーインシデント訓練



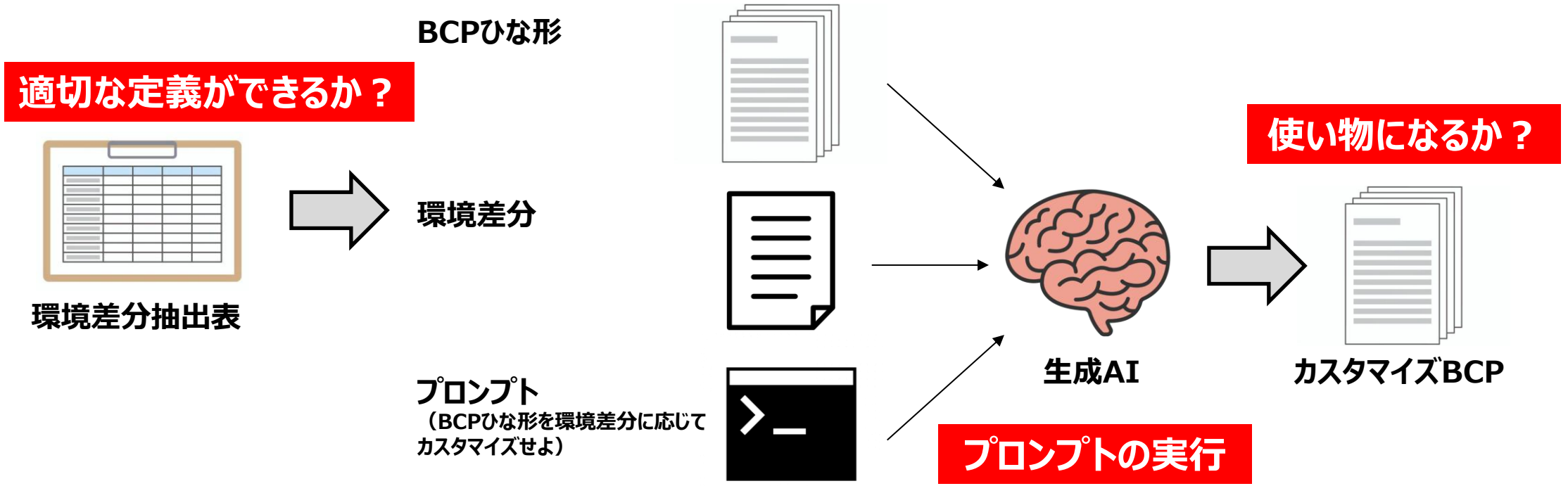
サイバー対応IT-BCP

第3弾 サイバー対応 IT-BCP策定編 - 万が一への備え

JNSA

●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

事業者自らでカスタマイズする方法



第3弾 サイバー対応 IT-BCP策定編 - 万が一への備え

JNSA

● 中小製造業24社でAIによるBCPカスタマイズ結果の満足度を検証

①BCPの各項目の過不足、記載内容のわかりやすさについて

②BCPの対策の具体性、実現可能性、自社への適用可能性について

③BCPの文章量、図表の活用、レイアウトについて

調査協力：公益財団法人 新産業創造研究機構（NIRO）

今後の展望

●ハンドブックを広めるパンフレット

●活用のためのワークショップ

インシデント体験型セミナーを企画中

JNSA西日本支部：中小工場向けセキュリティWSパッケージング企画案

【企画対象】
「**中小工場向けITセキュリティ対策ワーショップ**」パッケージ

【提供対象】
中小製造現場向けに啓発・教育セミナーを企画されている団体

【目的】
-製造現場に関わる多角的な方面の人々に、
「現場の安全」のもう1つの観点「ITセキュリティ」を伝える。
-パッケージング化する事で、提供対象の方が主催される
セミナーの1コマに入れていただきやすくなる。

【コンセプト】
地域で協力しあう、みんなで考える製造業のセキュリティ

【根拠・主旨 ～なぜ今】
『 中小製造業に、セキュリティ上の危機がある事は 認識している。
伝えなければ、気づかせなければ・・・』
は、共通認識。

[各団体様の課題]
-「伝える」ための、効果的なコンテンツづくりは難しい
ex)ナレッジ、ノウハウ、コスト etc....

[ＪＮＳＡ側の課題]
-検討してきた実績として知識やノウハウはあるが、
製造現場の方々との接点が薄い。集客力が弱い

⇒ワークショップをパッケージング化し、
団体様主催のセミナーに集まった現場の方々に体験していただく。

【参加者・Before】
参加者 ：製造現場の担当者、製造装置のメーカー担当者 等が対象
- 知識 ：製造現場もコンピュータ/ネットワークを利用していると
なんとなく知っている。
- メンタル ：普段、「現場の安全」「ラインを止めない」は意識している
「セキュリティ」という言葉にはピンとこない。
- 関係性 ：サイバーセキュリティの業界との関係を意識した事はない。
おそらく、ファンタジー/フィクションと感じている

【参加者・After】
- 知識 ：現場はセキュリティ侵害を受ける可能性があり、
それが、「現場の安全」「ラインを止めない」を
侵される可能性がある事を知っている状態
- メンタル ：「現場の安全」「ラインを止めない」のもう1つの観点が
「ITセキュリティ」であり、対策を講じる必要性を感じている
- 関係性 ：検討/対策は難しいと感じても「頼る先」として我々がいる。

【パッケージ内容】
1. イメージ：セキュリティ侵害 / 初体験を学ぶ!!!

2. 講義形態：グループディスカッション
1グループ約5名程度。
3～4グループを対象に進める

3. 進行 ：
-主催者であるＪＮＳＡ西日本支部の担当者1名が、
モデレータを務める。
-セキュリティ侵害を受けたシチュエーションストーリーを
時系列に進めながら、
「その時、あなたの工場なら？」を 考える。

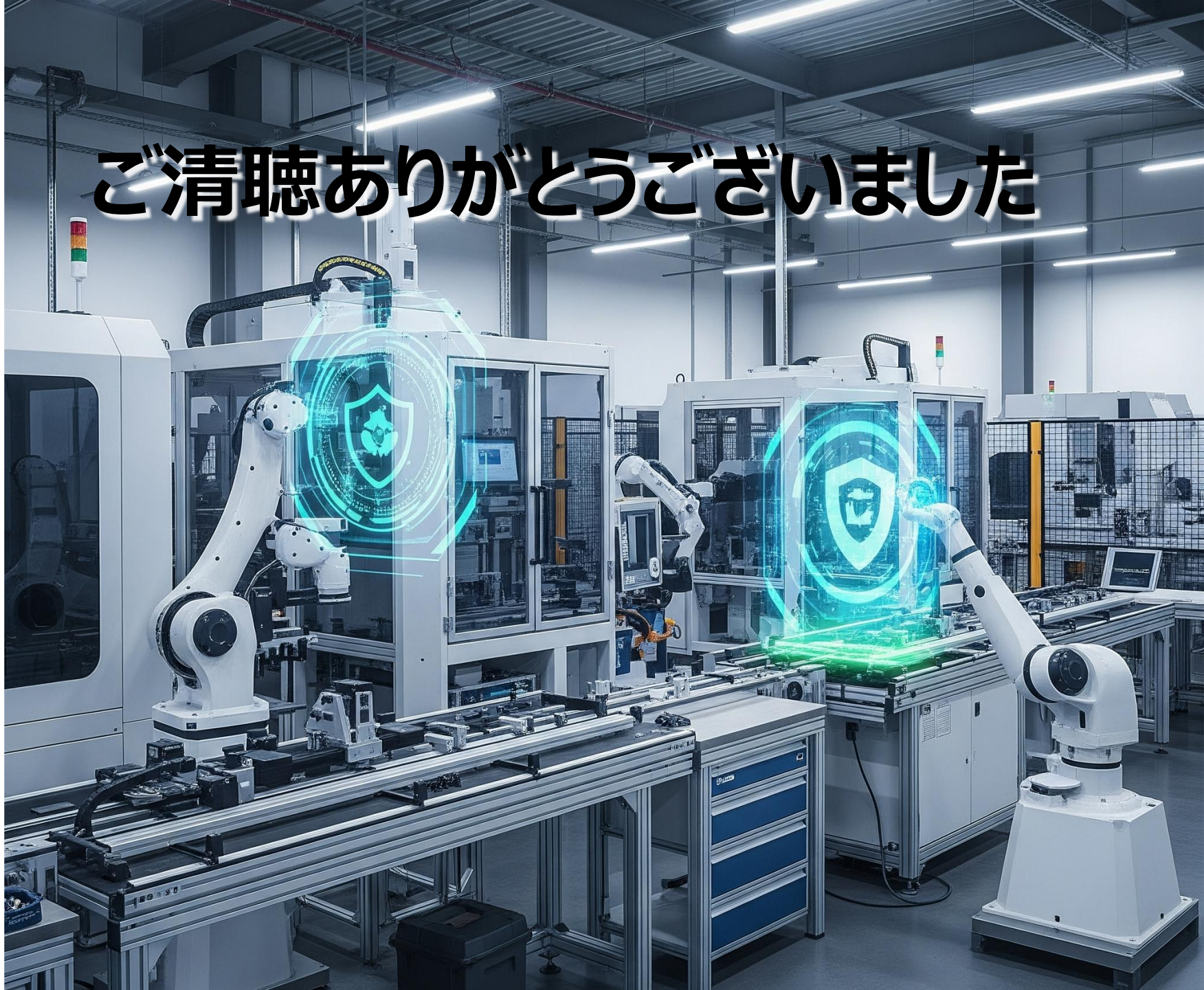
4. 3部作：アセスメント編、対策編、BCP編

5. その他：既作のハンドブックの抜粋等を用いた
講義テキスト等をお持ち帰りいただき
今後の自社の検討に役立てていただく

時間(約2時間)・募集定員(Min10名-Max30名)・費用(無償)
※ 会場/テキスト代はご負担お願いします)

・教科書に書いてある答えをゴールとしない。
・「自分の工場でできること」は何か？を考える事が目的

ご清聴ありがとうございました



JNSA