西日本支部

ハンドブック3部作活用推進への取り組み

工場セキュリティWGリーダー　岡本　登

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

- 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)

Copyright 2026 JNSA

ハンドブック活用イメージ

自社の弱点を正確に把握する

潜在的な脅威を特定し、対策の基礎を築くための最初のステップです。

ハンドブックで簡単評価

「USBメモリ」など13の脅威の入口別に、チェックリスト形式で評価します。

弱点に応じた有効な対策を実施

アセスメント結果に基づき、脅威を軽減するための具体的な戦略を講じます。

ハンドブックで対策を選択

13の脅威ごとに対策が整理されており、優先順位付けを支援します。

事業継続計画を立てる

サイバー攻撃でシステムが停止した際の、事業継続と復旧の計画を策定します。

AI活用で計画をカスタマイズ

ひな形とヒアリング結果を基に、AIが自社に最適なBCP作成を支援します。

Copyright 2026 JNSA

リスクアセスメント編

JNSA

なぜ今、工場セキュリティ？

ランサムウェア等による工場停止が急増中

IoT化やDX推進で工場が外部ネットワークに接続され、リスクが高まっています。

工場を襲う3つの情報セキュリティリスク

可用性
(Availability)
制御システムや製造装置を停止させられ、生産が止まる。

出荷停止

完全性
(Integrity)
装置の設定が改ざんされ、製品の品質が低下する。

信用失墜

機密性
(Confidentiality)
製造情報やノウハウが流出し、ライバル企業に漏れる。

経営悪化

ハンドブックでかんたんリスク評価

専門家でなくても使える「自己診断ツール」

STEP 1: 脅威シナリオを選ぶ

具体的な13の脅威シナリオを元に、自社の弱点を発見できます。
「USBメモリーからマルウェア感染」など、自社に関係ありそうなシナリオを選択。


USBメモリー


持込パソコン


Wi-Fi


保守用ネットワーク


クラウドサービス

STEP 2: チェックポイントを確認

「USBメモリーの使用は禁止されているか？」などの質問にYes/Noで回答。

STEP 3: リスクを判断

回避可能
(Avoidable)
1つでもYesならリスクは回避可能。

BAD END
すべてNoなら対策が必要。

リスク対策編

JNSA

ハンドブック活用の3ステップ

ステップ1：リスクを特定する

まずは「13の脅威の入口」を参考に、自社工場にどんな危険があるか把握します。

ステップ2：対策を計画・実施する

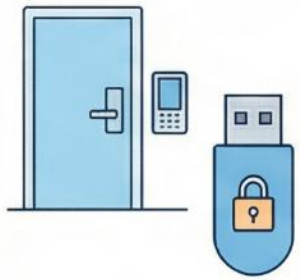
ハンドブックに掲載された「防御」「検知」「復旧」の3つの分類から対策を選びます。

ステップ3：基礎から始める

まずは全ての脅威に共通する「基礎的な共通対策」から取り組み、土台を固めます。

対策の3つの柱

① 防御 (Defense)



被害に遭わないための対策。部外者の立ち入り制限や、許可されたUSBメモリのみ使用するルールなどが含まれます。

② 検知 (Detection)

異常を早期発見するための対策。不審なパソコンの接続を検知する仕組みなどが含まれます。

③ 復旧 (Recovery)

被害から素早く復旧するための対策。セキュリティ事故が起きた際の報告・連絡体制の確立などが含まれます。

Copyright 2026 JNSA

サイバー対応IT-BCP編

このハンドブックで何ができる？

工場を守る「サイバーBCP」が作れる

サイバー攻撃時の被害を抑え、素早く復旧するための計画です。

なぜ中小工場にこそ必要？

サプライチェーンの弱点を狙った攻撃が増えているためです。

専門家でなくても大丈夫

ひな形とカスタマイズ手順で、自社に合った計画が作れます。

ハンドブックの簡単３ステップ活用法

1

ステップ1：準備

まず「カスタマイズ要件定義」シートに回答し、自社の状況を整理します。

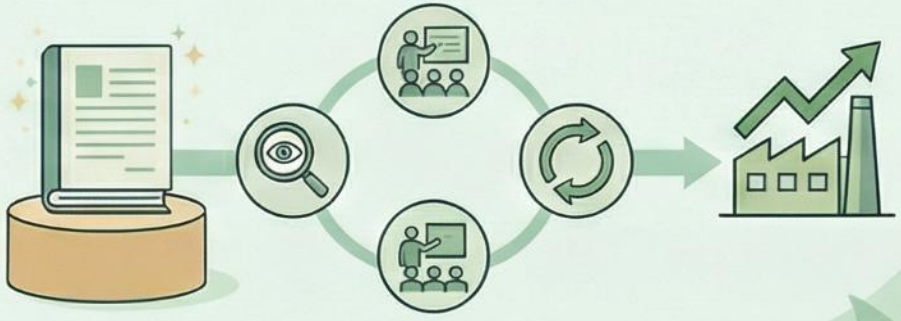
ステップ2：BCP作成

用意された「ひな形」を、手作業または生成AIを使って自社専用にカスタマイズします。

2

ステップ3：完成と改善

完成したBCPの内容を確認し、定期的な訓練と見直しで実効性を高めます。



Copyright 2026 JNSA

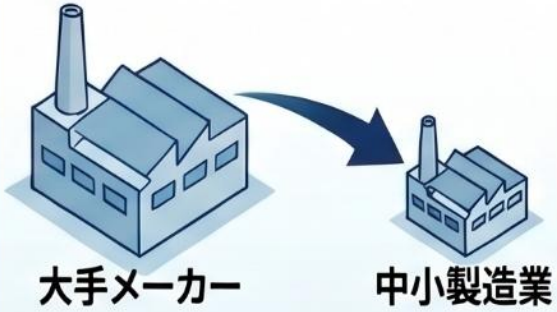
中小製造業支援の課題

JNSA

1. 遅れる防御対策

→ 多層防御的な対策が未着手

2. サプライチェーンにおける圧力と取引条件



- 一定のセキュリティ基準への適合
- SECURITY ACTION SECURITY ACTION宣言

→ 今後要求が増える

3. 経営課題としてのサイバーリスク

高額な復旧・損害賠償

コスト → 事業継続のためのリスク管理

4. 主な課題

遅れの理由

- 脆弱性の放置
- パッチ適用困難

当WGの認識： これらを踏まえて、ハンドブックの公開にとどまらず、実際に活用してセキュリティを向上していただくための取り組みが必要であると考えます。

Copyright 2026 JNSA

今後の活動方針

1. ハンドブック活用動画の公開

現状：工場セキュリティ必要性解説動画
公開中　YouTube

今後：各ハンドブック（アセスメント・
対策・BCP）の具体活用方法動画
作成・公開予定

2. 利用者アンケートによる実態調査

現状：JNSA HP（コンテンツダウンロードページ）
アンケートフォーム設置済

今後：蓄積データの分析・活用
ハンドブックのブラッシュアップ
支援方法の検討

3. ワークショップ形式の活用セミナー

内　容：3つのハンドブック（アセスメント，対策，
BCP）に合わせた体験型ワークショップ

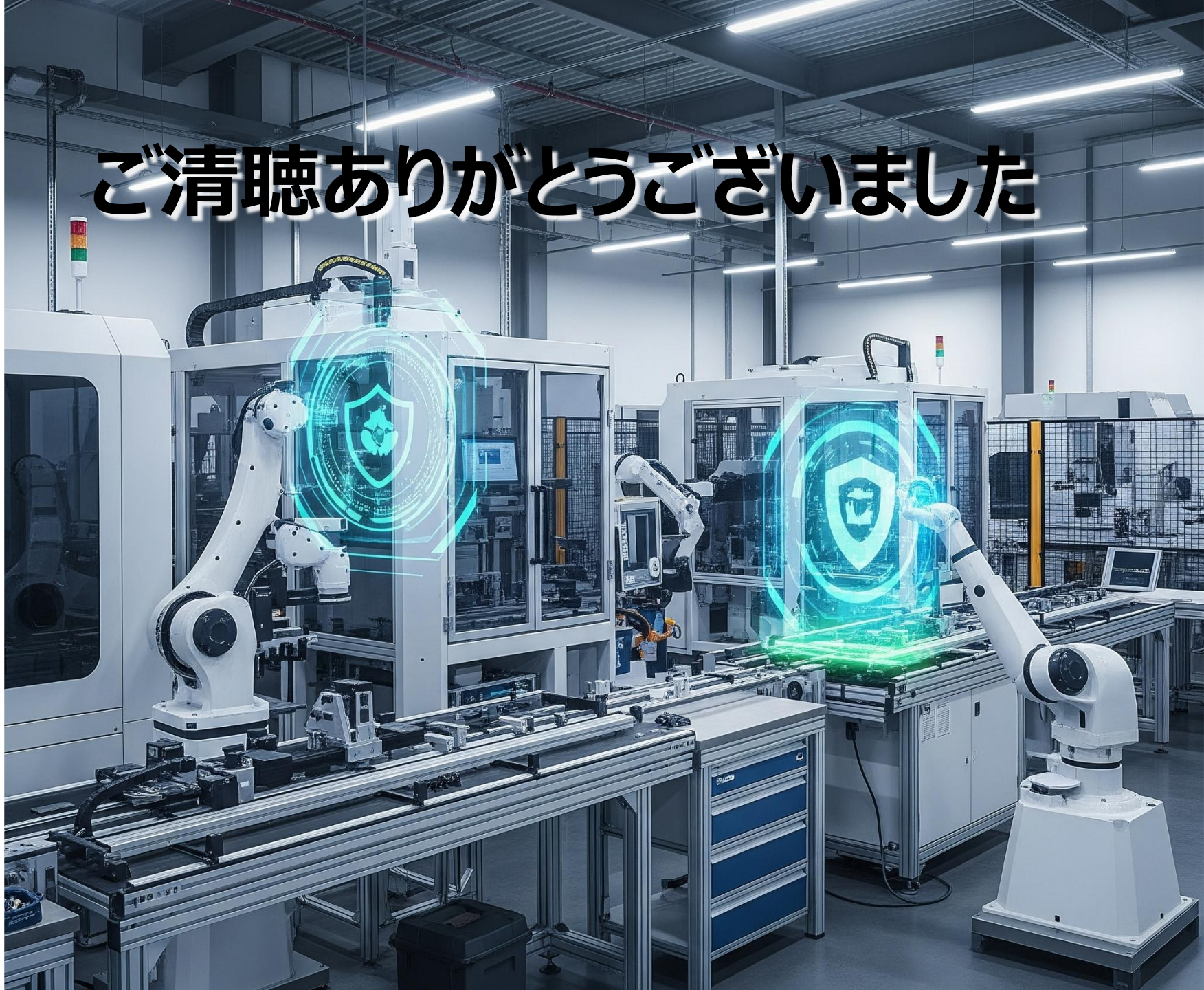
対象・展開：様々なチャネルによる募集
当面は近畿一円を対象
オンラインセミナーによる地域拡大検討

地域ワークショップ

オンライン配信

Copyright 2026 JNSA

ご清聴ありがとうございました



JNSA