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
成果物発表

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）

2025年3月14日

ワーキンググループの概要

●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

主な活動：検討会（毎月）／セミナー、ワークショップ等

成果物　：ハンドブック三部作
リスクアセスメント、リスク対策、BCP策定

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
- ●2025年　2月　サイバー攻撃疑似体験ワークショップ（NIRO/神戸市主催）
- ●2025年　3月　工場セキュリティハンドブック・BCP策定編（検討会11回）公開予定

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ハンドブック・リスクアセスメント編
https://www.jnsa.org/result/west/2022/index.html

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行います

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

ハンドブックの概要

取り組みハードルを下げる VS 対策効果が期待できる

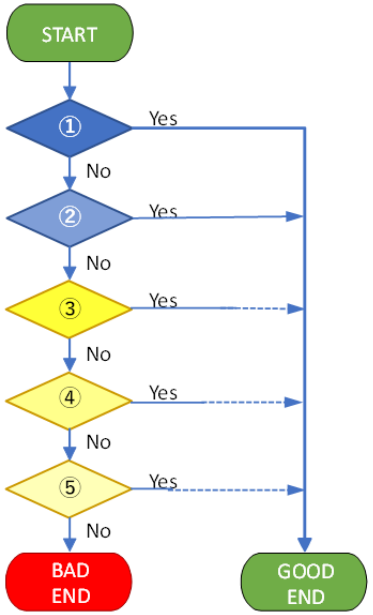
●一般的手法とは異なるユニークな手法で現場の担当者が簡単に実施できることを目指しています

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）

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ハンドブック・リスク対策編
https://www.jnsa.org/result/west/2023/index.html

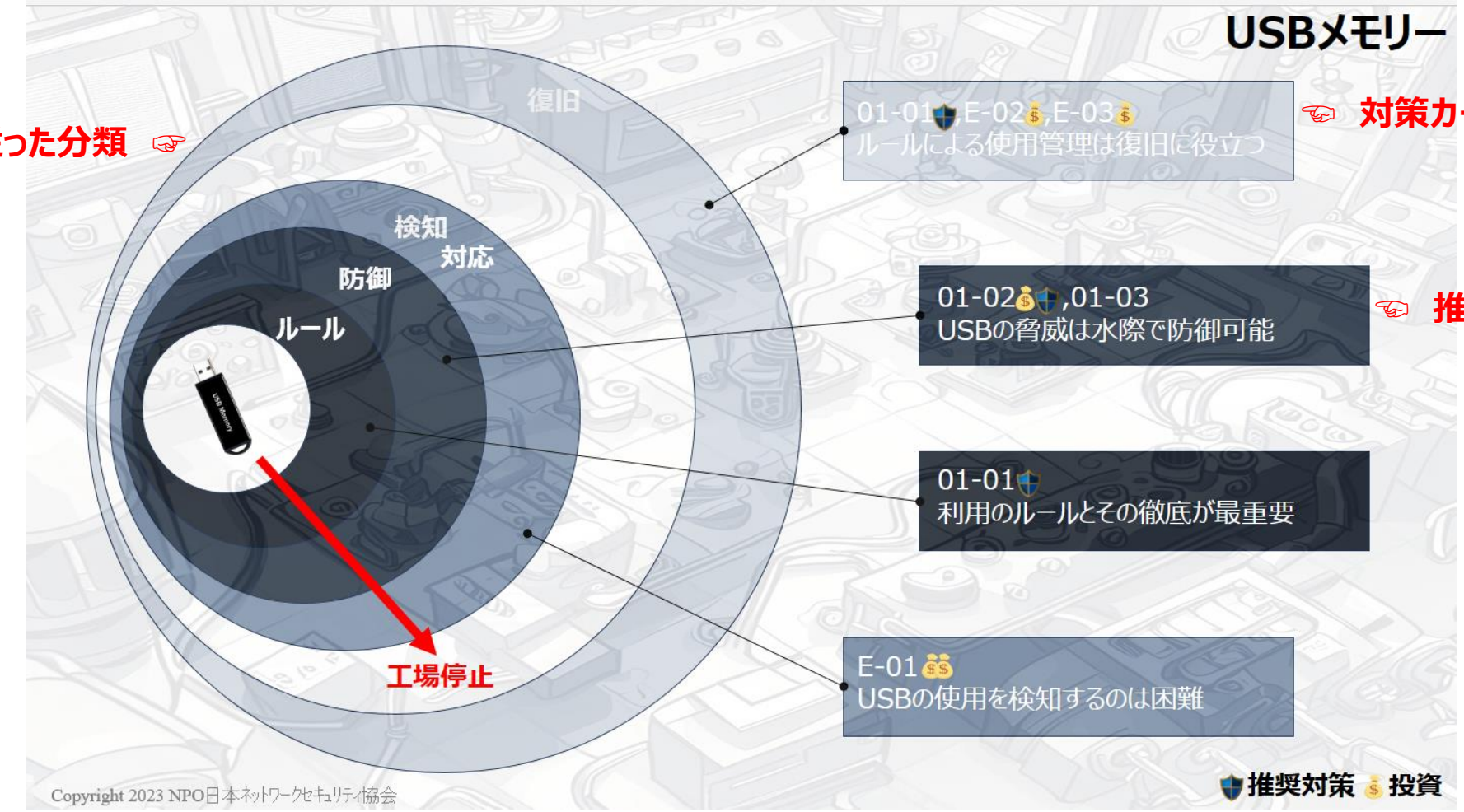
2nd STEP　リスク対策

● 13の脅威の入口に対応した対策と共通対策から必要なものを選択します

ハンドブック概要

● 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

ハンドブック概要

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）

ハンドブック・サイバーBCP策定編

3rd STEP　サイバーBCP策定

- リスクアセスメント、リスク対策を踏まえて、セキュリティ脅威に対するBCPを策定することが重要
- 災害等に対応したBCPとは別のIT-BCPの位置づけ。ひな形を活用して自社にあったBCPにカスタマイズする手段として、手動と生成AI利用の2種類を用意

	自然災害	サイバー攻撃
初動対応	・安全確認：従業員の安全を最優先し、避難を指示。 ・物理的被害の評価：建物や設備の損傷状況を確認。	・インシデントの特定：サイバー攻撃の種類を特定し、影響範囲を把握。 ・システムの隔離：影響を受けたシステムをネットワークから切り離す。
復旧手段	・修理・復旧作業：損傷した設備やインフラの修理。 ・外部業者の手配：建設業者や専門業者による復旧作業。	・データ復元：バックアップからデータを復元。 ・セキュリティ強化：攻撃を受けた原因を分析し、再発防止策を講じる。
フォロー	・代替資材の確保：自然災害で影響を受けた資材の調達計画を策定。	・情報伝達：従業員やステークホルダーに対して状況を説明し、透明性を確保。
業務再開	・段階的な業務再開：安全が確認された後、徐々に生産を再開。	・システムチェック：復旧後、システムの安全性を確認してから業務を再開。
レビューと改善	・災害後の教訓：自然災害に対する耐性を高めるための改善点を洗い出し、BCPを見直す。	・インシデント後の評価：攻撃の影響を評価し、サイバーセキュリティ対策を強化。BCPの見直しを行う。

ハンドブックの概要（予定）

目次

生成AIによるカスタマイズ

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するのは難しい

生成AIの活用

カスタマイズの準備

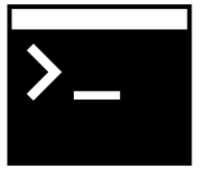
要件定義表

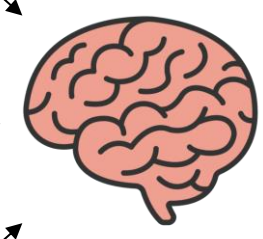
プロンプトの自動作成

AI用BCPひな形

カスタマイズ要素

プロンプト





生成AI

最終的に人がチェック

カスタマイズBCP

AIによるカスタマイズの実用性を検証

● 中小製造業24社様で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


JNSA