

## NIRO DXセミナー

中小ものづくり企業が自ら実践できる

## サイバーセキュリティ対策セミナー

サプライチェーンに深刻な影響をおよぼす重大セキュリティインシデントが相変わらず発生しています。これは日本だけでなく世界的な傾向であり、各国において対策が進められています。

日本においては、新たに2026年度中の運用開始を目指して「サプライチェーン強化に向けたセキュリティ対策評価制度」により中小を含めた企業の対策状況を可視化するしくみが政府により検討が進められており、対策状況が今後の企業間取引の参考情報となると考えられます。

セミナーでは最近の事例を交えてサイバーセキュリティの現状をお伝えするとともに、自社がサプライチェーンの弱点にならないために、日本ネットワークセキュリティ協会（JNSA）が公開したハンドブックのエッセンスを基盤とした「今すぐできること」をわかりやすく解説します。

■日程： 2026年2月27日(金)

■方法： リアル開催&amp;オンライン

■会場： 兵庫県立大学 新長田ランチ 5階 セミナー室

(神戸市長田区腕塚町5丁目2-1 : JR・地下鉄新長田駅徒歩7分)

■主催： 神戸市、(公財)新産業創造研究機構

■対象： 神戸市ならびに兵庫県下の中小ものづくり企業

優先順位 神戸市中小企業&gt; 兵庫県中小企業&gt; 兵庫県大企業&gt; その他

オンラインはこの限りではない

経営者、総務部門などのBCP（事業継続計画）担当の方、サイバーセキュリティ担当の方、ICT担当の方、サプライチェーン関連部門の方、サイバーセキュリティに関心のある方

■参加費： 無料 ■定員： リアル 25名程度（オンライン 制限なし）

※会場聴講の皆様にはJNSAのハンドブック3部作を配布します

■参加申込： NIROホームページよりお申込みください

<https://www.niro.or.jp/information/20260106/54550/>

■プログラム

**2026年2月27日（金） 14:00~16:30**

14:00-14:10 インタロダクション (公財)新産業創造研究機構

14:10-16:10 「3社に1社が被害に遭う時代を乗り切るために」

講演： 特定非営利活動法人 日本ネットワークセキュリティ協会(JNSA)

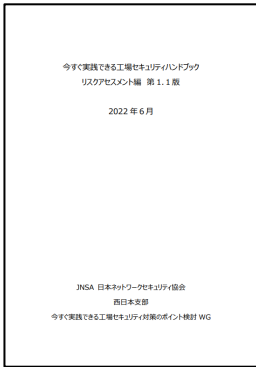
岡本 登 氏（所属：富士通株式会社）

(休憩10分)

16:20-16:30 神戸市・(公財)新産業創造研究機構からのご連絡

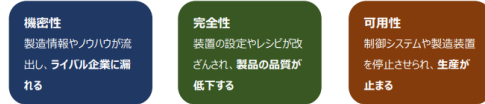
# 【セミナーで紹介するハンドブック】

## 1. 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



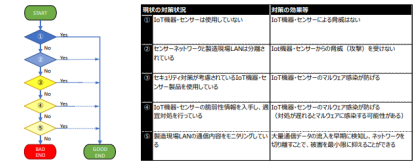
### 1. 1 ハンドブック・リスクアセスメント編活用の目的

製造装置の誤動作や停止、あるいは品質低下につながるような情報セキュリティリスクを理解し、自社の製造現場における現状を正しく把握するためには、脅威の存在と客観的なリスク評価が必要である。では、製造現場と情報セキュリティリスクにはどのような繋がりがあるのでしょうか。例えば、一般的なオフィス環境では、情報を適切に管理するために、「機密性」、「完全性」、「可用性」の3つの観点を用いながら情報セキュリティリスクを考えます。これに倣って、例えば、製造現場がコンピュータウイルス（脅威）に感染した場合、どのようなリスクがあるのか、3つの観点との関係性を考えてみます。



### (4)IoT 機器・センサー

直接インターネットに接続されていない製造装置が IoT 機器やセンサーから攻撃を受け、生産が停止した

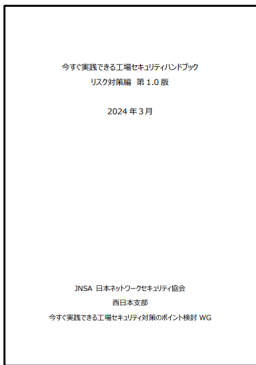


※ルールは徹底され、適切に運用されていることが前提

### 【補足】

- 製造装置への攻撃の原因は、マルウェアに感染した IoT 機器やセンサー（例えば監視用カメラや赤外線センサーなど）が遠隔で操作されることによるものです。
- IoT 機器・センサーにはセキュリティ対策が不十分なものも多く存在し、不正アクセスやマルウェア感染の脅威を受けやすいと考えられています。
- ③の「ネットワーク分離」とは、製造現場 LAN とは物理的に接続せずに、IoT 機器・センサー専用の LAN を作る方法や、物理的にはつながっていない、製造現場 LAN とは直接

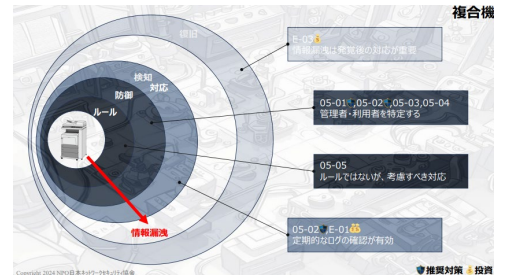
## 2. 今すぐ実践できる工場セキュリティハンドブックリスク対策編



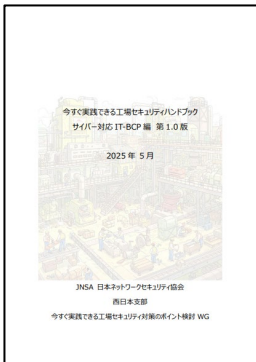
### 情報セキュリティ対策の考え方（一般的なフレームワーク）



※本ハンドブックでは、検知と対応を一体として取り扱います。



## 3. 工場セキュリティサイバー対応IT-BCP策定ハンドブック



### カスタマイズ要件定義

No.	質問	回答例1	回答例2	回答
1	ITは、30分以内で製造装置ですか？	電子部品・デバイス・電子回路製造業	食料品製造業	
2	製造している製品の応用が広がることは自社以外に大きな影響を与えますか？	大きな影響あり	若干影響あり	
3	サプライチェーンとして許容できる工場の稼働率・止期間は何パーセントですか？	3日	2週間	
4	自社経営計画で許容できる工場の稼働率・止期間は何パーセントですか？	1週間	1週間	
5	保存した情報が破られる脅威の入口はどこですか？	インターネット	保守用ネットワーク	
6	ITは、30分以内で製造装置ですか？	ファイアウォール、アンチウイルス、ネットワーク監視、Q7伝送	USBメモリ使用禁止	
7	システムのバックアップはありますか？	定期的に取得	なし	
8	サイバー攻撃を受けた際、自社内の要員で対応可能ですか？	可能	できません	
9	サイバー攻撃を受けた際、自社内で外部要員はベンダーに協力してもらえますか？	ベンダーに協力してもらえます	できません	
10	サイバー攻撃を受けた際、自社内で復旧は可能ですか？	ベンダーに協力してもらえます	できません	

### 中小製造業向けサイバー対応 IT-BCP サンプル Ver. 1.0

1. はじめに  
当社の製造現場において、サイバー攻撃は深刻な事業リスクとなり、工場の停止は社外へも大きな影響を及ぼす。本サイバー対応 IT-BCP は、当社が既に実施しているリスクアセスメントに基づき、サイバー攻撃発生時の対応を定めることで、速やかに情報セキュリティ脅威に対処し、結果として事業継続性を高めることを目的とする。
2. 基本方針  
サイバー攻撃による事業中断を最小限に抑え、迅速なシステム復旧を実現するため、以下の基本方針に基づき対策を実施する。
  - 統治：役割と責任を明確にし、緊急対応体制図を作成の上、組織的に対応する。
  - 特定：潜在するリスクとその影響範囲を特定する。
  - 防御：脅威の入口に対して必要な防御対策を行う。
  - 検知：異常な活動を早期に検知し、被害の拡大を防ぐ。
  - 対応：インシデント発生時には、サプライチェーンへの影響も考慮し、手順に従い迅速かつ適切な対応を行う。

会場：兵庫県立大学 新長田ランチ  
〒653-0036  
神戸市長田区腕塚町5丁目2-1  
(新長田キャンパスプラザ 5階)



### 公共交通機関

- JR・市営地下鉄（西神山手線）新長田駅から南へ徒歩7分
- JR大阪駅からJR新長田駅まで約34分  
(大阪方面からは、新快速にて神戸駅で普通に乗換えて2駅目)
- JR姫路駅からJR新長田駅まで約51分  
(姫路方面からは、新快速にて明石駅で普通に乗換えて8駅目)

新長田キャンパスプラザには駐車場はございません。  
車でお越しの方は、近隣の駐車場をご利用ください。