# 仮想企業で学ぶ！工場のサイバー・フィジカルセキュリティリスク【会場】(4126255)

工場DXやIoT化により、これまで閉域網だった工場が外部ネットワークと繋がる機会が増え、サイバー攻撃によって「生産ライン停止」などの物理的な被害を受けるリスクが急増しています。本セミナーでは、経産省の「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」の基本を座学で解説します。

| | |
|---|---|
| 開催日時 | 2026年12月10日(木) 10:00-17:00会場 |
| JUAS研修分類 | セキュリティ(情報セキュリティ)、セキュリティ(サイバーセキュリティ) |
| カテゴリー | IS戦略策定・IS戦略評価・IS企画・IS企画評価 専門スキル |
| DXリテラシー | How(データ・技術の活用):留意点 |
| 講師 | 佐々木弘志 氏<br>（フォーティネットジャパン合同会社　OTビジネス開発部　部長 ）<br>国内製造企業の制御システム機器の開発者として14年間従事した経験をもつ。<br>セキュリティ専門家として，産業サイバーセキュリティの文化醸成（ビジネス化）をめざし，国内外の講演，執筆などの啓発やソリューション提案などのビジネス活動を行っている。CISSP認定保持者。博士（工学）<br>2021年8月～現在：フォーティネットジャパン合同会社 OTビジネス開発部 部長<br>2022年5月～現在：名古屋工業大学 産学官金連携機構 ものづくりDX研究所 客員教授（非常勤）<br>2017年7月～現在：独立行政法人情報処理推進機構（IPA）産業サイバーセキュリティセンター（ICSCoE）専門委員（非常勤）<br>2016年5月～2020年12月，2021年7月～現在：経済産業省 情報セキュリティ対策専門官（非常勤） |
| 参加費 | JUAS会員企業/ITC：35,200円 一般：45,100円（１名様あたり　消費税込み、テキスト込み）【受講権利枚数1枚】 |
| 会場 | 一般社団法人日本情報システム・ユーザー協会（NBF東銀座スクエア２F） |
| 対象 | ・製造業IT部門セキュリティ担当者（中堅以上）　・OT部門のDX担当者、生産管理担当者（中堅以上）ほか 中級 |
| 開催形式 | 講義、グループ演習 |
| 定員 | 25名 |
| 取得ポイント | ※ITC実践力ポイント対象のセミナーです。（2時間1ポイント） |
| 特記 | ワークショップのパワーポイント資料作成用に、各自PCを持参してください |
| ITCA認定時間 | 6 |

## 主な内容

■受講形態
会場のみ（オンラインなし）
■テキスト
当日配布
■開催日までの課題事項
ワークショップのパワーポイント資料作成用に、各自PCを持参してください

---

仮想企業で学ぶ！「繋がる工場」のサイバー・フィジカルのセキュリティリスクをどう管理するか？
～経産省ガイドラインに基づくセキュリティ対策ワークショップ～

◆主な内容
１．はじめに
２．全社セキュリティの不可分領域：
IT/OTインテグレーション時代に情シスが修得すべき「OTセキュリティ」のグランドデザイン

３．ITセキュリティとはここが違う！ 工場DXに伴うOT特有のリスクと脅威
４．経産省ガイドラインを活用したアセスメントの進め方
工場システムにおける サイバー・フィジカル・セキュリティ対策
ガイドラインv1.1 https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html

５．事例ワークショップ
仮想企業紹介・課題説明
ワークショップ（１）実施
チーム発表（１）
ワークショップ（２）実施
チーム発表（２）
６．クロージング

◆特記
ワークショップのパワーポイント資料作成用に、各自PCを持参してください